

CERTIFIED UPPER BOUNDS FOR TWO SUM-DIFFERENCE EXPONENTS

TEJASVI SINGH TOMAR

ABSTRACT. For finite sets A, B of real numbers and $G \subseteq A \times B$, Katz and Tao proved in 1999 that $\{a - b : (a, b) \in G\}$ has at most $N^{11/6}$ elements whenever A, B and $\{a + b : (a, b) \in G\}$ have at most N elements. We lower the exponent $11/6$ to 1.827297 . Without non-Shannon inequalities we obtain the exponent 1.829429 , but this exponent is valid in all abelian groups. We also prove $|X - Y| \leq |X + Y|^{1.422300}$ for all finite sets X, Y of integers. This improves the exponent 1.4543 of Kleinwaks, and through his transfer theorem it lowers the upper bound for the sum-difference constant of Gyarmati, Hennecart and Ruzsa from 1.3124 to 1.296914 . Both proofs establish entropy inequalities for a random pair. We construct several copies of the pair on a common probability space, glued by the copy lemma for the first problem and independent for the second, and use cross forms, which are integer combinations of coordinates of different copies. With rational weights found by linear programming, we combine Shannon inequalities among the joint entropies of these forms and, for the first problem, also non-Shannon inequalities that we prove from the copy lemma. For each bound, a checker recomputes the inequalities from their definitions and verifies the combination in exact rational arithmetic, and a second checker confirms the result. The proofs of the exponents 1.827297 and 1.422300 and of the bound 1.296914 have also been checked in the Lean 4 proof assistant.

1. INTRODUCTION

For finite subsets A, B of an abelian group and $G \subseteq A \times B$ we write

$$A \overset{G}{+} B = \{a + b : (a, b) \in G\}, \quad A \overset{G}{-} B = \{a - b : (a, b) \in G\}.$$

Bourgain [2] showed that bounds $|A \overset{G}{-} B| \leq N^{2-\varepsilon}$, valid whenever $|A|, |B|, |A \overset{G}{+} B| \leq N$, give lower bounds for the dimension of Kakeya sets, and he proved such a bound with $\varepsilon = 1/13$. Katz and Tao [14] proved it with $\varepsilon = 1/6$ in any abelian group. Following Tao's list of optimization constants [30, page 3b], let C_{3b} be the least exponent C such that

$$(1.1) \quad |A \overset{G}{-} B| \leq \max(|A|, |B|, |A \overset{G}{+} B|)^C$$

for all finite $A, B \subset \mathbb{R}$ and $G \subseteq A \times B$.¹ By [10] (see also [29, §1]), C_{3b} is also the least C such that

$$(1.2) \quad H(X - Y) \leq C \max(H(X), H(Y), H(X + Y))$$

for all real random variables X, Y with finitely many values, not necessarily independent, where H denotes Shannon entropy. We prove our bounds in both forms (Lemma 3.1). This is the constant $C_{6.30}(\{0, 1, \infty\}; -1)$ of Problem 6.30 in [9] and the sum-difference exponent $\text{SD}(\{0, 1, \infty\}; -1)$ of [29]. Its relation to the arithmetic Kakeya conjecture is discussed in [15, 10, 29]. The upper bound $11/6 = 1.8333\dots$ of [14] is the best one recorded in [9, 30],

2020 *Mathematics Subject Classification*. 11B13, 11B30; 94A17, 90C05, 68V05.

Key words and phrases. Sumsets, difference sets, sum-difference exponents, arithmetic Kakeya conjecture, Shannon entropy, copy lemma, non-Shannon inequalities, linear programming, computer-assisted proof.

¹The definition of $A \overset{G}{\pm} B$ on that page has $a \in A, b \in B$. The restriction to $(a, b) \in G$ is the intended one, as in [14, 10].

and the lower bounds recorded there are slightly above 1.7789 [17, 22, 30]. Farnamfar [6, 7] proves obstructions to improving 11/6 by combinatorial constructions that certify upper bounds through a score: literal ladders cannot improve it, and an improving construction must have dimension at least three and avoid several further families. The proof of Theorem 1.1 uses entropy inequalities instead of such constructions.

Theorem 1.1. *Let*

$$\begin{aligned}\lambda_X &= \frac{925\,252\,334\,339\,885\,103\,560\,423\,126\,733\,856\,553}{1\,309\,548\,008\,918\,246\,261\,431\,347\,658\,091\,038\,786}, \\ \lambda_Y &= \frac{424\,585\,766\,727\,935\,297\,449\,756\,583\,005\,066\,048}{654\,774\,004\,459\,123\,130\,715\,673\,829\,045\,519\,393}, \\ \lambda_S &= \frac{1\,237\,016\,505\,223\,052\,067\,896\,560\,048\,548\,494\,601}{2\,619\,096\,017\,836\,492\,522\,862\,695\,316\,182\,077\,572},\end{aligned}$$

so that

$$\lambda_X + \lambda_Y + \lambda_S = \frac{4\,785\,864\,240\,814\,563\,464\,816\,432\,634\,036\,471\,899}{2\,619\,096\,017\,836\,492\,522\,862\,695\,316\,182\,077\,572} < 1.8272963.$$

- (a) *If X, Y are random variables with finitely many values in a torsion-free abelian group, then $H(X - Y) \leq \lambda_X H(X) + \lambda_Y H(Y) + \lambda_S H(X + Y)$.*
- (b) *If A, B are finite subsets of a torsion-free abelian group and $G \subseteq A \times B$, then $|A \overset{G}{-} B| \leq |A|^{\lambda_X} |B|^{\lambda_Y} |A \overset{G}{+} B|^{\lambda_S}$.*

In particular $C_{3b} \leq 1.8272963$ in both formulations (1.1) and (1.2).

Theorem 1.2. *Statements (a) and (b) of Theorem 1.1 hold in all abelian groups with*

$$(\lambda_X, \lambda_Y, \lambda_S) = \left(\frac{882}{1\,259}, \frac{1\,609}{2\,518}, \frac{2\,467}{5\,036} \right),$$

whose sum is $9\,213/5\,036 < 1.8294282$.

Remark. A set A of n integers determines at most $n^{1.8272963}$ distinct positive common differences of three-term arithmetic progressions. This improves the exponent 11/6 recorded for Erdős problem #1097 [1], which asks how many such differences there can be; the problem page attributes to Chan the observation that this problem is “exactly equivalent” to the sums-differences question of Bourgain recalled above. For the proof, choose for each such difference $d > 0$ an a_d with $a_d, a_d + d, a_d + 2d \in A$, and let G consist of the pairs $(a_d + 2d, a_d)$. Their differences $2d$ are distinct, so $|A \overset{G}{-} A|$ is the number of such d , and their sums $2(a_d + d)$ lie in $\{2a : a \in A\}$, so $|A \overset{G}{+} A| \leq n$. Part (b) of Theorem 1.1 with $B = A$ gives $|A \overset{G}{-} A| \leq n^{\lambda_X + \lambda_Y + \lambda_S} \leq n^{1.8272963}$.

For finite subsets X, Y of an abelian group, Ruzsa’s triangle inequality and Plünnecke’s inequality give $|X - Y| \leq |X + Y|^{3/2}$ [11, §1]. Kleinwaks [16, Theorem 2.1] proved the exponent $\lambda_\infty = (9451e - 3286)/(5378e + 787) = 1.454277\dots$ for finite subsets of any abelian group. Taking $X = Y$ shows that such an exponent is at least the single-set exponent of [9, Problem 6.43], the least C with $|A - A| \leq |A + A|^C$ for all finite $A \subset \mathbb{Z}$, which lies between $\log(1 + \sqrt{2})/\log 2 = 1.2715\dots$ [12] and $4/3$ [8].

Kleinwaks also proved that an exponent λ valid for all finite $X, Y \subset \mathbb{Z}$ gives the bound $2 - 1/\lambda$ for the sum-difference constant C_{3a} of Gyarmati, Hennecart and Ruzsa [16, Theorem 2.2]. This constant is the supremum of the exponents t for which there are finite sets $A, B \subset \mathbb{Z}$ with $B \neq \emptyset$, $|A|$ arbitrarily large, $|A + B| \leq K|A|$ and $|A - B| \geq c|A + B|^t$ for some constants K and $c > 0$ [30, page 3a]. It is Problem 6.44 of [9]. The sources state its quantifiers differently, and Section 4.4 compares the readings. Gyarmati, Hennecart and Ruzsa proved $C_{3a} \leq 4/3$ [11, Corollary 3],

and Kleinwaks proved $C_{3a} \leq 2 - 1/\lambda_\infty = 1.312373\dots$ [16, Corollary 2.3]. The lower bounds recorded in [30, page 3a] reach 1.19102809 with an explicit construction and 1.19519192 as a limit of constructions.

Theorem 1.3. *For all finite subsets X, Y of a torsion-free abelian group,*

$$|X - Y| \leq |X + Y|^\lambda, \quad \lambda = \frac{7\,670\,057\,033}{5\,392\,715\,767} < 1.42229952.$$

Corollary 1.4.

$$C_{3a} \leq 2 - \frac{1}{\lambda} = \frac{9\,947\,398\,299}{7\,670\,057\,033} < 1.29691322.$$

The method. Both proofs are entropy arguments in the style of [16]; entropy methods in additive combinatorics are developed in [27, 28]. In both proofs the main new ingredient is a larger family of random variables: integer combinations of coordinates of different copies of a random pair for Theorems 1.1 and 1.2, and further independent variables for Theorem 1.3. For Theorems 1.1 and 1.2 we take a random pair (X, Y) such that $X - Y$ is injective on its support. Three applications of the copy lemma put six copies of the pair on one probability space. This configuration is a variant, in entropy form, of the one behind the bound $11/6$ of [14] (Proposition 3.2). Integer combinations of the coordinates of the copies are random variables, and Shannon inequalities hold for their joint entropies. We call the combinations that mix coordinates of different copies *cross forms*. For a fixed finite set of cross forms, a linear program finds a nonnegative combination that bounds $H(X, Y)$ by $\lambda_X H(X) + \lambda_Y H(Y) + \lambda_S H(X + Y)$. It combines Shannon inequalities, the identities given by the copy lemma and non-Shannon inequalities, each of them proved from the copy lemma. We call such a combination a *certificate*. Linear programs over linear forms of glued copies of a random pair, with copy-lemma variables, were used before in [21] for the Katz–Tao problem with many slopes. With 41 cross forms this gives Theorem 1.1, and without non-Shannon inequalities 20 cross forms give Theorem 1.2. Appendix A lists a certificate with five cross forms and 72 Shannon inequalities that proves the exponent $841/459 < 11/6$ in every abelian group.

For Theorem 1.3 we start from Kleinwaks’ coupling, a random pair (X_1, Y_1) uniform on a set $\Gamma \subseteq X \times Y$ with one pair for each element of $X - Y$. Kleinwaks uses two independent copies of this pair and the entropies $h(i, j)$ of sums of independent copies of its marginals. We add a variable with the law of X_1 and a variable with the law of Y_1 , independent of the two copies and of each other. Shannon inequalities among integer combinations of these coordinates give an inequality between $\log |X - Y|$, $\log |X + Y|$ and 8 values of h (Proposition 4.1). Finitely many of Kleinwaks’ inequalities for h eliminate these values (Lemma 4.2). In contrast to [16, Proposition 5.1], no non-Shannon inequality is needed.

Verification. The weights in the certificates are exact rational numbers, obtained from floating-point solutions of the linear programs. Section 5 describes how each certificate is verified in exact rational arithmetic and accepted by a second, independently written checker. For the inequalities proved inside the certificate of Theorem 1.1, the second checker follows the steps of the first, and the Lean proof checks them separately. Part (a) of Theorem 1.1 for real random variables, inequality (1.1) with its exponent for subsets of $\mathbb{R}$, Theorem 1.3 and Corollary 1.4 also have formal proofs in Lean 4, obtained by translating the certificates into Lean. Table 1 in Section 5 summarizes the checks.

Section 2 collects the entropy tools. Section 3 proves Theorems 1.1 and 1.2, and Section 4 proves Theorem 1.3 and Corollary 1.4, including a proof of Kleinwaks’ transfer theorem. Appendix A lists the short certificate, and Appendix B the cross forms and the non-Shannon inequalities of the certificate for Theorem 1.1.

2. ENTROPY TOOLS

All random variables below take finitely many values and are defined on a common probability space, which we enlarge when we construct new variables. We write H for Shannon entropy with the natural logarithm, treat a tuple of random variables as one random variable, and put

$$I(U; V | W) = H(U, W) + H(V, W) - H(U, V, W) - H(W), \quad I(U; V) = I(U; V | \emptyset).$$

We use Shannon's inequality $I(U; V | W) \geq 0$, the inequality $H(f(U)) \leq H(U)$ for any function f , with equality if f is injective on the range of U , and the identity $H(U, V) = H(U) + H(V)$ for independent U and V .

Lemma 2.1 (copy lemma [31, 5]). *Let A, B, C be random variables. On an enlarged probability space there is a random variable A' such that (A', B) has the law of (A, B) and A' is conditionally independent of (A, C) given B . In particular*

$$H(A', A, B, C) + H(B) = H(A, B, C) + H(A', B).$$

Proof. Put $P(A = a, B = b, C = c, A' = a') = P(A = a, B = b, C = c) P(A = a' | B = b)$ for all b with $P(B = b) > 0$. This law extends the law of (A, B, C) , the pair (A', B) has the law of (A, B) , and the conditional law of A' given (A, B, C) depends on B only. $\square$

Every relation that holds almost surely between A and B therefore holds between A' and B . For random variables a, b, c, d let

$$[abcd] = I(a; b | c) + I(a; b | d) + I(c; d) - I(a; b)$$

be the Ingleton expression.

Lemma 2.2. *Let $a_1, \dots, a_r$ be random variables and let $\psi = \sum_S c_S H(a_S)$, where S runs over the nonempty subsets of $\{1, \dots, r\}$ and $a_S = (a_i)_{i \in S}$. Suppose that random variables $b_1, \dots, b_q$ are obtained from $a_1, \dots, a_r$ by successive applications of Lemma 2.1, and that ψ is identically, as a linear combination of entropies, the sum of nonnegative multiples of Shannon inequalities and of inequalities that hold for all random variables, applied to joint variables made of the a_i and b_j , and of a linear combination of the identities given by these applications: the identity of Lemma 2.1 and the equalities of entropies that follow from the equality of the laws of (A', B) and (A, B) . Then $\psi \geq 0$ for all random variables $a_1, \dots, a_r$.*

Proof. The applications of Lemma 2.1 do not change the joint law of $a_1, \dots, a_r$. At the constructed variables the identities vanish and the remaining terms are nonnegative. $\square$

Dougherty, Freiling and Zeger prove the inequalities of their list [5, Section VIII] in this way. Matúš's inequality

$$M_s(a, b, c, d) = I(b; c | a) + s[abcd] + \binom{s+1}{2}(I(a; c | b) + I(a; b | c)) \geq 0$$

[20, Corollary 3, formula (4)] follows for each $s \geq 1$ from the case $s - 1$ by Lemma 2.2, with one copy of a over (b, c) [5, (80) and Rule [1]].

2.1. Linear forms and closures. Let $\mathbf{G}$ be an abelian group, let $Z = (Z_1, \dots, Z_m)$ be a random vector in $\mathbf{G}^m$, and let $\mathcal{R} \subseteq \mathbb{Z}^m$ be a set of integer vectors r with $\sum_i r_i Z_i = 0$ almost surely. A *form* is a vector $f \in \mathbb{Z}^m$, which defines the random variable $f(Z) = \sum_i f_i Z_i$. For a finite set F of forms, $H[F]$ denotes the entropy of the tuple $(f(Z))_{f \in F}$, and $\langle F \rangle$ denotes the subgroup of $\mathbb{Z}^m$ generated by F and $\mathcal{R}$.

Lemma 2.3. *Let F be a finite set of forms and let f be a form.*

(a) *If $f \in \langle F \rangle$, then $f(Z)$ is a function of $(g(Z))_{g \in F}$.*

- (b) If $cf \in \langle F \rangle$ for an integer $c \neq 0$ such that $u \mapsto cu$ is injective on $\mathbf{G}$, then $f(Z)$ is a function of $(g(Z))_{g \in F}$.
- (c) Let x, y be forms such that $(x(Z), y(Z))$ lies almost surely in a set on which $(u, v) \mapsto u - v$ is injective. If $(x - y)(Z)$ is a function of $(g(Z))_{g \in F}$, then so are $x(Z)$ and $y(Z)$.

Proof. For (a) write $f = \sum_{g \in F} a_g g + r$ with r in the subgroup generated by $\mathcal{R}$, so that $f(Z) = \sum_g a_g g(Z)$ almost surely. For (b), $cf(Z)$ is a function of $(g(Z))_{g \in F}$ by (a), and $u \mapsto cu$ is injective. Part (c) is immediate. $\square$

Fix a finite ground set E of forms and a list of pairs (x, y) as in (c). The *closure* $\text{cl } F$ of $F \subseteq E$ is the smallest subset of E that contains F and is closed under the rules (a)–(c), where (b) is used exactly for the integers $c \neq 0$ for which $u \mapsto cu$ is injective on $\mathbf{G}$, for example for all $c \neq 0$ if $\mathbf{G}$ is torsion-free. By Lemma 2.3, $H[\text{cl } F] = H[F]$. The checkers compute closures with rules (a) and (b) together, by linear algebra over $\mathbb{Q}$. A separate script determines which multipliers c in (b) a certificate uses (Table 1).

3. THE KAKEYA-TYPE EXPONENT

3.1. Reduction to injective pairs. A pair (X, Y) of random variables in an abelian group is *injective* if $(x, y) \mapsto x - y$ is injective on the support of (X, Y) . Then $H(X, Y) = H(X - Y)$.

Lemma 3.1. *Let $\mathbf{G}$ be an abelian group and $\lambda_X, \lambda_Y, \lambda_S \geq 0$. Suppose that*

$$(3.1) \quad H(X, Y) \leq \lambda_X H(X) + \lambda_Y H(Y) + \lambda_S H(X + Y)$$

for every injective pair (X, Y) in $\mathbf{G}$. Then

- (a) $H(X - Y) \leq \lambda_X H(X) + \lambda_Y H(Y) + \lambda_S H(X + Y)$ for all pairs (X, Y) in $\mathbf{G}$, and
- (b) $|A \stackrel{G}{-} B| \leq |A|^{\lambda_X} |B|^{\lambda_Y} |A \stackrel{G}{+} B|^{\lambda_S}$ for all finite $A, B \subseteq \mathbf{G}$ and $G \subseteq A \times B$.

Proof. (b) We may assume $G \neq \emptyset$. Choose $G' \subseteq G$ with exactly one pair (a, b) satisfying $a - b = z$ for each $z \in A \stackrel{G}{-} B$, and let (X, Y) be uniform on G' . This pair is injective, $H(X, Y) = \log |G'| = \log |A \stackrel{G}{-} B|$, and $X, Y, X + Y$ take values in $A, B, A \stackrel{G}{+} B$. Since a random variable with values in a finite set T has entropy at most $\log |T|$, (b) follows from (3.1).

(a) We use the construction in the proof of [29, Proposition 3.6]. Let $D = X - Y$. For each z in the range of D choose a random pair $\varphi(z)$ with the conditional law of (X, Y) given $D = z$, independently for different z and independently of (X, Y) , and put $(X', Y') = \varphi(D)$. Given $D = z$, both (X, Y) and (X', Y') have the conditional law of (X, Y) given $D = z$, so (X', Y') has the law of (X, Y) , and $X' - Y' = D$. For a value φ_0 of φ , the conditional law of (X', Y') given $\varphi = \varphi_0$ is the law of $\varphi_0(D)$, which is supported on points with distinct differences, so (3.1) applies to it. Averaging over φ_0 gives

$$\begin{aligned} H(X', Y' \mid \varphi) &\leq \lambda_X H(X' \mid \varphi) + \lambda_Y H(Y' \mid \varphi) + \lambda_S H(X' + Y' \mid \varphi) \\ &\leq \lambda_X H(X) + \lambda_Y H(Y) + \lambda_S H(X + Y), \end{aligned}$$

because conditioning does not increase entropy. Given φ , the pair $\varphi(D)$ and D determine each other, so $H(X', Y' \mid \varphi) = H(D \mid \varphi) = H(D)$, since φ is independent of D . $\square$

With $C = \lambda_X + \lambda_Y + \lambda_S$, Lemma 3.1 gives (1.1) and (1.2) with this C for subsets and random variables of $\mathbf{G}$.

3.2. The configuration. Let (X, Y) be an injective pair in an abelian group $\mathbf{G}$. We construct six pairs $g_v = (x_v, y_v)$, $0 \leq v \leq 5$, each with the law of (X, Y) , by three applications of Lemma 2.1, starting from $g_0 = (X, Y)$:

- (S1) g_1 is a copy of g_0 over x_0 ;
- (S2) (g_2, g_3) is a copy of (g_0, g_1) over (y_0, y_1) ;
- (S3) (g_4, g_5) is a copy of (g_0, g_1) over $(x_0 + y_0, y_1)$.

In each step, Lemma 2.1 is applied with A the tuple U of pairs to be copied, B the tuple V of variables it is copied over, and C the pairs constructed before. The new pairs satisfy the relations that U satisfies with V :

$$x_1 = x_0; \quad y_2 = y_0, \quad y_3 = y_1, \quad x_3 = x_2; \quad x_4 + y_4 = x_0 + y_0, \quad y_5 = y_1, \quad x_5 = x_4$$

almost surely. Hence all twelve coordinates are integer combinations of the five *free coordinates* x_0, y_0, y_1, x_2, x_4 :

$$(3.2) \quad \begin{aligned} g_0 &= (x_0, y_0), & g_1 &= (x_0, y_1), & g_2 &= (x_2, y_0), \\ g_3 &= (x_2, y_1), & g_4 &= (x_4, x_0 + y_0 - x_4), & g_5 &= (x_4, y_1). \end{aligned}$$

We apply Section 2.1 to the vector $Z \in \mathbf{G}^{12}$ of all coordinates, with $\mathcal{R}$ the seven relations above, so that forms are integer combinations of the free coordinates. The *standard forms* are $ax_v + by_v$ with $(a, b) \in \{(1, 0), (0, 1), (1, 1), (1, -1)\}$ and $0 \leq v \leq 5$. All other forms are *cross forms*. We write $s_v = x_v + y_v$ and $d_v = x_v - y_v$. The construction gives three further rules.

- (CI) For each step, with O the pairs constructed before it, U' the new pairs and V the variables copied over, $H(V, U') + H(O) = H(O, U') + H(V)$. This is the identity of Lemma 2.1.
- (EL) For each step and each set S of standard forms of the pairs in U and variables in V , $H[S] = H[\tau S]$, where τ replaces each pair of U by its copy and fixes V . This holds because (U', V) has the law of (U, V) .
- (INJ) Rule (c) of Lemma 2.3 applies to (x_v, y_v) for $0 \leq v \leq 5$, because g_v has the law of the injective pair (X, Y) .

Proposition 3.2. *Let $a = H(X)$, $b = H(Y)$ and $c = H(X + Y)$. In the configuration (3.2),*

$$6H(X, Y) = 4a + 4b + 3c - \Delta_{\text{KT}},$$

where

$$\Delta_{\text{KT}} = I(y_0; y_1) + I(s_0; y_1) + I(x_0; (s_3, s_5, y_4)) + I(s_3; y_4) + I(s_5; (s_3, y_4)) \geq 0.$$

In particular $H(X, Y) \leq \frac{2}{3}H(X) + \frac{2}{3}H(Y) + \frac{1}{2}H(X + Y)$ for all injective pairs in all abelian groups.

Proof. Let $L = H(X, Y)$ and $\Omega = (x_0, y_0, y_1, x_2, x_4)$. In step (S1), (CI) and $H(x_0, g_1) = H(g_1) = L$ give $H(g_0, g_1) = 2L - a$. In step (S2), $H(y_0, y_1, g_2, g_3) = H(g_2, g_3) = H(g_0, g_1)$ by the relations and (EL), so (CI) gives $H(g_0, \dots, g_3) = 2H(g_0, g_1) - H(y_0, y_1)$. In the same way step (S3) gives $H(\Omega) = H(g_0, \dots, g_3) + H(g_0, g_1) - H(s_0, y_1)$. Hence

$$H(\Omega) = 6L - 3a - H(y_0, y_1) - H(s_0, y_1).$$

On the other hand $(s_3 - s_5) + (x_0 - y_4) = x_2 - y_0 = d_2$, so by (INJ) the forms x_0, s_3, s_5, y_4 determine x_2 and y_0 , then $x_4 = x_2 - s_3 + s_5$ and $y_1 = s_5 - x_4$. Thus $H(\Omega) = H(x_0, s_3, s_5, y_4)$. The pairs g_1, g_3, g_4, g_5 have the law of (X, Y) , so $H(y_1) = H(y_4) = b$ and $H(s_3) = H(s_5) = c$, and expanding the five terms gives

$$\Delta_{\text{KT}} = (2b - H(y_0, y_1)) + (b + c - H(s_0, y_1)) + (a + b + 2c - H(x_0, s_3, s_5, y_4)).$$

Comparing the two expressions for $H(\Omega)$, we obtain the identity. No step uses rule (b), so the argument is valid in every abelian group. $\square$

Combined with Lemma 3.1, Proposition 3.2 yields the exponent $11/6$. It adapts the counting argument in [14, §3] to entropy. In this configuration an improvement of $11/6$ amounts to a lower bound for Δ_{KT} . Appendix A gives one: Shannon inequalities among five cross forms prove $153 \Delta_{\text{KT}} \geq 8H(Y) + 9H(X + Y) - 16H(X)$, and with Proposition 3.2 this gives $459H(X, Y) \leq 314H(X) + 302H(Y) + 225H(X + Y)$.

3.3. Certificates. Fix a finite set E of cross forms and take as ground set the standard forms together with E , with the pairs (x_v, y_v) in rule (c). Consider the linear program with one variable $h(F)$ for each closed set F and $h(\emptyset) = 0$, which maximizes $h(\text{cl}\{x_0, y_0\})$ subject to the following constraints, where K runs over closed sets and i, j over the ground set:

- (i) $h(\text{cl}(K \cup \{i\})) + h(\text{cl}(K \cup \{j\})) - h(\text{cl}(K \cup \{i, j\})) - h(K) \geq 0$ and $h(\text{cl}(K \cup \{i\})) - h(K) \geq 0$;
- (ii) the three identities (CI);
- (iii) $h(\text{cl} S) = h(\text{cl} \tau S)$ for the identifications (EL);
- (iv) instances of inequalities proved by Lemma 2.2 for joint variables made of closed sets, each with its proof, where the joint entropy of several closed sets is h of the closure of their union;
- (v) $h(\text{cl}\{x_0\}) \leq 1$, $h(\text{cl}\{y_0\}) \leq 1$ and $h(\text{cl}\{x_0 + y_0\}) \leq 1$.

For every injective pair with $\max(a, b, c) > 0$, the vector $F \mapsto H[F]/\max(a, b, c)$ is feasible. A *certificate* consists of a set E , the identifications (iii) that it uses, a finite list of rows R_k of types (i), (ii) and (iv) with rational multipliers μ_k , nonnegative except on rows of type (ii), and rational numbers $\lambda_X, \lambda_Y, \lambda_S \geq 0$, such that

$$(3.3) \quad h(\text{cl}\{x_0, y_0\}) + \sum_k \mu_k R_k = \lambda_X h(\text{cl}\{x_0\}) + \lambda_Y h(\text{cl}\{y_0\}) + \lambda_S h(\text{cl}\{x_0 + y_0\})$$

holds identically in the variables h after the identifications (iii). At the entropy vector of an injective pair the rows of types (i) and (iv) are nonnegative and the rows of type (ii) vanish, so (3.1) follows from (3.3). This conclusion does not depend on how the certificate was found.

We solve the linear programs with HiGHS [13] in floating point. Rows of type (iv) are added when the current optimum violates them. For the certificate we keep the rows whose floating-point multipliers exceed a tolerance and solve the dual equations on these rows exactly over $\mathbb{Q}$.

3.4. Proofs of Theorems 1.1 and 1.2.

Proof of Theorem 1.1. The certificate for Theorem 1.1, in the file `c3b_torsionfree.json`, uses the configuration (3.2), cross forms from Table 5 and identifications (EL). Its 293 rows are inequalities of both kinds in (i) (252 of the first kind and 3 of the second), the identities (CI) and applications of the inequalities that the certificate proves by Lemma 2.2, listed in Table 6; Table 1(a) gives the remaining counts. Its numbers $\lambda_X, \lambda_Y, \lambda_S$ are those of Theorem 1.1, and the checkers of Section 5 verify (3.3). The closures use rule (b) of Lemma 2.3, so (3.1) holds for injective pairs in torsion-free groups, and Lemma 3.1 gives (a) and (b). Since $\mathbb{R}$ is torsion-free, $C_{3b} \leq \lambda_X + \lambda_Y + \lambda_S$. The proved inequalities include Matúš's inequality for $s \leq 62$ and the inequalities numbered 5, 7, 8, 33, 35, 56, 60, 77, 107, 109 in [5, Section VIII], so the proof uses only Shannon inequalities and Lemma 2.1. $\square$

Remark 3.3. This certificate applies rule (b) with $c = 2^k$ only (Table 1), so Theorem 1.1 holds in all abelian groups without 2-torsion.

Proof of Theorem 1.2. The certificate for Theorem 1.2, in the file `c3b_allgroups.json`, combines inequalities of type (i) with the identities (CI), after identifications (EL), and uses no row of type (iv); Table 1(a) gives its counts. Its numbers λ are those of Theorem 1.2. For each set

of forms in it, the closure with rule (b) equals the closure without it (Table 1), and the relations of Section 3.2 have integer coefficients. Hence the rules it uses are valid in any abelian group, and Lemma 3.1 applies. $\square$

Remark 3.4. Cross forms are what make the improvement possible: on the configuration (3.2) with standard forms only, the floating-point optimum of the linear program with constraints (i), (ii), (iii) and (v) is $11/6$, the value of Proposition 3.2. Adding to the ground set any three of the 65 forms with coefficients ± 1 on at most three free coordinates does not lower this optimum, while the five cross forms of Appendix A lower it to $841/459$.

4. THE TWO-SET EXPONENT

4.1. Kleinwaks' setting. Let $X, Y \subset \mathbb{Z}$ be finite and nonempty. Choose $\Gamma \subseteq X \times Y$ with exactly one pair (x, y) satisfying $x - y = z$ for each $z \in X - Y$ [16, Lemma 4.1], let (X_1, Y_1) be uniform on Γ , and let μ and ν be the laws of X_1 and Y_1 . Put

$$L = \log |X - Y| = H(X_1, Y_1), \quad S = \log |X + Y|, \quad h(i, j) = H(\mu^{*i} * \nu^{*j}) \quad (i, j \geq 0),$$

where $\alpha * \beta$ is the law of $U + V$ for independent $U \sim \alpha$, $V \sim \beta$, and H of a law is the entropy of a random variable with that law. Kleinwaks proved [16, Lemmas 4.2 and 4.3] that for all $i, j \geq 0$

- (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) $h(1, 1) \leq S$.

Here (G1) is Madiman's inequality for sums of independent variables [18], and (G3) holds because $(X_1 + V, Y_1 + V)$ determines (X_1, Y_1, V) for V independent of (X_1, Y_1) , as $x - y$ determines (x, y) on Γ .

4.2. The configuration. Let $D_0 = (x_0, y_0)$ and $D_1 = (x_1, y_1)$ be independent copies of (X_1, Y_1) , and let w and v be random variables with laws μ and ν , such that D_0 , D_1 and the variables in $\mathcal{W} = \{w, v\}$ are mutually independent. Each variable in $\mathcal{W}$ carries a *type* (i, j) , given with the configuration, and has law $\mu^{*i} * \nu^{*j}$. We apply Section 2.1 to the vector Z of the coordinates x_0, y_0, x_1, y_1 and the variables in $\mathcal{W}$, with $\mathcal{R} = \emptyset$, so that forms are integer combinations of these coordinates. The following rules hold.

- (R1) Closure: rules (a)–(c) of Lemma 2.3, with (c) for the pairs (x_k, y_k) , $k = 0, 1$.
- (R2) Independence: the joint entropy of D_0, D_1 and the variables in $\mathcal{W}$ is the sum of their entropies.
- (R3) Symmetry: $H[F] = H[\tau F]$ for all sets F of forms and all permutations τ of the coordinates that map the pairs D_0, D_1 to D_0, D_1 (with x to x and y to y) and each variable in $\mathcal{W}$ to a variable in $\mathcal{W}$ of the same type.
- (R4) $H(x_k, y_k) = L$ for $k = 0, 1$.
- (R5) Grid identification: if $f = \sum_{k \in I} x_k + \sum_{k \in J} y_k + \sum_{u \in U} u$ with $I \cap J = \emptyset$ and $U \subseteq \mathcal{W}$, then $H(f) = h(i, j)$, where (i, j) is $(|I|, |J|)$ plus the sum of the types of the variables in U .
- (R6) Support: $H(a + b) \leq S$ if a is one of x_0, x_1 or a variable in $\mathcal{W}$ of type $(1, 0)$, and b is one of y_0, y_1 or a variable in $\mathcal{W}$ of type $(0, 1)$.

Rule (R1) holds because $\mathbb{Z}$ is torsion-free and $(x_k, y_k) \in \Gamma$. Rule (R3) holds since D_0 and D_1 are independent copies of one pair, variables in $\mathcal{W}$ of the same type are independent copies of one variable, and all of them are independent. Rule (R5) holds because f is a sum of independent variables, each with law μ or ν or one of the laws of the variables in $\mathcal{W}$. Differences such as $w - v$, however, are not identified with entries of h . Rule (R6) holds because x_k and variables

of type $(1, 0)$ take values in X , while y_l and variables of type $(0, 1)$ take values in Y . Without $\mathcal{W}$ and without rule (b), rules (R1)–(R6) correspond to the rules (R1)–(R7) of [16, §4.3].

- (R7) Reflection: $\Gamma' = \{(-y, -x) : (x, y) \in \Gamma\}$ is a subset of $(-Y) \times (-X)$ with distinct differences, $|\Gamma'| = |\Gamma|$ and $|(-Y) + (-X)| = |X + Y|$. Its marginals are the reflections of ν and μ , so the numbers attached to Γ' are L, S and $h'(i, j) = h(j, i)$ [16, proof of Corollary 5.3]. Hence (R1)–(R6) also hold for the configuration built from Γ' , in which a variable of type (i, j) has law $\mu'^{*i} * \nu'^{*j}$ for the marginals μ', ν' of Γ' , with $h(i, j)$ replaced by $h(j, i)$ in (R5).
- (R8) One probability space: $H'[F] = H[\sigma F]$ for each set F of forms of the configuration built from Γ' , where H' is entropy in that configuration and σ substitutes $x'_k \mapsto -y_k$, $y'_k \mapsto -x_k$ and $u' \mapsto -\pi(u')$ for the variables u' of the reflected configuration that occur in F . Here π is injective, and $\pi(u') \in \mathcal{W}$ has type (j, i) when u' has type (i, j) . The rule holds because $(-y_0, -x_0)$ and $(-y_1, -x_1)$ are independent copies of a pair uniform on Γ' , $-\pi(u')$ has the law of u' , since $\mu'^{*i} * \nu'^{*j}$ is the reflection of $\mu^{*j} * \nu^{*i}$, and all these variables are independent.

4.3. Proof of Theorem 1.3.

Proposition 4.1. *In the setting of Section 4.1,*

$$\begin{aligned}
 60\,559\,937\,823\,L &\leq 5\,975\,233\,166\,S \\
 &\quad + 5\,067\,604\,398\,h(0, 2) + 101\,405\,565\,296\,h(1, 1) \\
 &\quad + 1\,270\,254\,931\,h(1, 2) + 3\,241\,242\,225\,h(2, 0) \\
 &\quad + 4\,922\,979\,277\,h(2, 1) \\
 &\quad - 218\,001\,042\,h(1, 3) - 29\,004\,161\,662\,h(2, 2) \\
 &\quad - 218\,001\,042\,h(3, 1).
 \end{aligned}$$

Proof. The certificate for Theorem 1.3, in the file `pair_exponent.json`, lists 1306 instances of the rules of Section 4.2 with rational multipliers, each for the configuration of Γ or of Γ' . Besides Shannon inequalities among joint entropies of forms and one support inequality (R6), they are identities (R2)–(R5) and (R8); Table 1(b) gives the number of each kind. The multipliers of the inequalities are nonnegative. In the weighted sum, after each $H[F]$ is replaced by $H[\text{cl } F]$, the coefficients of all joint entropies cancel, and what remains is the stated inequality. $\square$

Lemma 4.2. *Let $L, S \in \mathbb{R}$ and $h: \{0, \dots, 12\}^2 \rightarrow \mathbb{R}$ satisfy (G1)–(G4) whenever all indices involved are at most 12. Then*

$$\begin{aligned}
 14\,938\,082\,915\,L + 5\,067\,604\,398\,h(0, 2) \\
 &\quad + 101\,405\,565\,296\,h(1, 1) + 1\,270\,254\,931\,h(1, 2) \\
 &\quad + 3\,241\,242\,225\,h(2, 0) + 4\,922\,979\,277\,h(2, 1) \\
 &\quad \leq 101\,405\,565\,296\,S + 218\,001\,042\,h(1, 3) \\
 &\quad + 29\,004\,161\,662\,h(2, 2) + 218\,001\,042\,h(3, 1).
 \end{aligned}$$

Proof. The inequality is a sum of 163 instances of (G1)–(G4) with nonnegative rational multipliers, listed in the certificate: 69 and 68 instances of the two concavity inequalities, 23 of (G3), 2 of the monotonicity inequalities in (G2) and 1 of (G4). $\square$

Proof of Theorem 1.3. If X or Y is empty, both sides vanish. For nonempty $X, Y \subset \mathbb{Z}$, the sum of Proposition 4.1 and Lemma 4.2 is $75\,498\,020\,738\,L \leq 107\,380\,798\,462\,S$, that is, $L \leq \lambda S$. Finite subsets X, Y of a torsion-free abelian group lie in a subgroup isomorphic to $\mathbb{Z}^d$ for some

d. A homomorphism $\phi: \mathbb{Z}^d \rightarrow \mathbb{Z}$ that is injective on the finite sets $X + Y$ and $X - Y$ exists, because only finitely many hyperplanes must be avoided. Since $\phi(X) \pm \phi(Y) = \phi(X \pm Y)$, the integer case applied to $\phi(X), \phi(Y)$ gives the general case. $\square$

Remark 4.3. The certificate uses only Shannon inequalities, while the two-copy inequality of [16, Proposition 5.1] uses ten instances of the non-Shannon families of Matúš [20] and of Csirmaz and Csirmaz [4]. The gain over [16] comes from the variables in $\mathcal{W}$: for the configuration of D_0 and D_1 alone, with all forms whose coefficients lie in $\{-1, 0, 1\}$, the floating-point optimum of the Shannon linear program is 1.4621, the optimum of (G1)–(G4) alone at depth 12.

4.4. The transfer theorem. In [30, page 3a] and [9, Problem 6.44], C_{3a} is the supremum of the t for which there exist arbitrarily large finite $A, B \subset \mathbb{Z}$ with $|A+B| \ll |A|$ and $|A-B| \gg |A+B|^t$ (in [9], $|A-B| \gg |A|^t$), the implied constants being independent of A and B . Gyarmati, Hennecart and Ruzsa [11, (5)] and Kleinwaks [16, §2.2] ask for such sets for every $K > 1$ in $|A+B| \leq K|A|$, which can only give a smaller supremum. If $|A+B| \leq K|A|$ and $t \geq 0$, then $|A-B| \geq c|A|^t$ implies $|A-B| \geq cK^{-t}|A+B|^t$, so the next theorem, stated with $|A-B| \geq c|A+B|^t$, bounds C_{3a} in each of these readings. Although Kleinwaks formalized it in Lean for his reading [16], we include the proof, which follows [16, §3]. Its main estimate, [16, Proposition 3.5], holds for every K .

Theorem 4.4 (Kleinwaks). *Let $\lambda \geq 1$ be such that $|X-Y| \leq |X+Y|^\lambda$ for all finite $X, Y \subset \mathbb{Z}$. Let $K \geq 1$, $c > 0$ and $t \in \mathbb{R}$, and suppose that there are finite nonempty $A, B \subset \mathbb{Z}$ with $|A|$ arbitrarily large, $|A+B| \leq K|A|$ and $|A-B| \geq c|A+B|^t$. Then $t \leq 2 - 1/\lambda$.*

Proof. Let $A, B \subset \mathbb{Z}$ be finite and nonempty, and write $M_h = |hB - hB|$, where hB is the h -fold sumset.

Packing. For a finite nonempty D , a set $T \subseteq A$ of maximal size such that the translates $t + D$, $t \in T$, are pairwise disjoint satisfies: for each $a \in A$ there is $t \in T$ with $a - t \in D - D$. Otherwise $a \notin T$ and $a + D$ is disjoint from all the translates $t + D$, which contradicts the maximality of T . This is Ruzsa's covering argument [26].

Localization. We show that

$$(4.1) \quad |A - B| |D| \leq |D - D - B|^{1-1/\lambda} |A + B| |D - D + D - B|.$$

Assign each $a \in A$ to one $t \in T$ with $a - t \in D - D$, and let A_t be the set of elements assigned to t . Then $A_t - B \subseteq t + (D - D - B)$, so $x = |A_t - B|$ satisfies $x \leq U := |D - D - B|$ and, by hypothesis, $x \leq |A_t + B|^\lambda$. Hence $x = x^{1-1/\lambda} x^{1/\lambda} \leq U^{1-1/\lambda} |A_t + B|$, and $|A - B| \leq \sum_t |A_t - B| \leq U^{1-1/\lambda} \sum_t |A_t + B|$. If $u \in A_t + B$, say $u = a + b$ with $a \in A_t$ and $a - t = d_1 - d_2$ with $d_1, d_2 \in D$, then $t + D = u - b - d_1 + d_2 + D \subseteq u + (D - D + D - B)$. The translates $t + D$ with $u \in A_t + B$ are disjoint, so there are at most $|D - D + D - B|/|D|$ of them, and $\sum_t |A_t + B| \leq |A + B| |D - D + D - B|/|D|$.

One scale. Take $D = hB - hB$ with $h \geq 1$. Then $D - D - B = 2hB - (2h + 1)B$ and $D - D + D - B = 3hB - (3h + 1)B$. Since $B \neq \emptyset$, $|mB - nB|$ does not decrease in m or n , so both sets have at most M_{4h} elements, and (4.1) gives $|A - B| M_h \leq M_{4h}^{2-1/\lambda} |A + B|$.

Several scales. Let $d = |A - B|$, $s = |A + B|$ and $m_j = M_{4^j}$. By induction on j , $d^j m_0 \leq s^j m_j^{1+j(1-1/\lambda)}$: the case $j = 0$ is an equality, and the step multiplies by $d m_j \leq m_{j+1}^{2-1/\lambda} s$ and uses $m_j \leq m_{j+1}$. Now $m_0 \geq 1$, and if $|A + B| \leq K|A|$, the Plünnecke–Ruzsa inequality $|kB - lB| \leq K^{k+l}|A|$ [25, Theorem 1.2] gives $m_J \leq K^{2 \cdot 4^J} |A| \leq K^{2 \cdot 4^J} s$. Hence, for every $J \geq 1$,

$$d \leq s (K^{2 \cdot 4^J} s)^{(1+J(1-1/\lambda))/J} = C_{K,J} s^{2-1/\lambda+1/J}.$$

For the sets of the theorem $s \geq |A|$ is arbitrarily large and $d \geq cs^t$, so $t \leq 2 - 1/\lambda + 1/J$. Letting $J \rightarrow \infty$, we conclude that $t \leq 2 - 1/\lambda$. $\square$

Proof of Corollary 1.4. The number $\lambda \geq 1$ of Theorem 1.3 satisfies the hypothesis of Theorem 4.4, so all exponents t in the definition of C_{3a} satisfy $t \leq 2 - 1/\lambda$. $\square$

5. VERIFICATION

The checkers `check630.py` (for the certificates of Section 3 and Appendix A) and `check3.py` (for that of Section 4) use only the Python standard library and do not import the programs that produce the certificates.

The checker `check630.py` reads the copy steps, the cross forms, the identifications, the rows and λ . It recomputes the relations of each copy step from Lemma 2.1 and computes closures by exact elimination over $\mathbb{Q}$ together with rule (INJ). It then rebuilds each row from its definition, merges the closed sets identified by (EL), and compares the two sides of (3.3) coefficient by coefficient. For each inequality proved in the certificate it also checks the proof, including the absence of cycles among the earlier proved inequalities that the proof applies.

The checker `check3.py` rebuilds the closures with (R1) and checks the following:

- (i) each permutation in (R3) maps pairs to pairs and variables in $\mathcal{W}$ to variables of the same type;
- (ii) the indices (i, j) of each identification (R5) are those of its form, transposed for Γ' ;
- (iii) each support row involves a form $x + y$ with x taking values in X and y in Y ;
- (iv) the map π of each row (R8) is injective and pairs variables of transposed types;
- (v) the grid indices are at most 12.

It then verifies that the weighted rows sum to $\lambda S - L$. Both checkers reject negative multipliers on inequality rows.

The second checkers `indep_check.py` and `indep3.py` were written independently from the mathematical definitions. They represent the configuration by an explicit parametrization and store closed sets as reduced row echelon bases computed with `python-flint`. A further script re-implements the lemma check of `check630.py`, following the same steps, for the inequalities proved inside the certificate of Theorem 1.1. The inequalities of the list of Dougherty, Freiling and Zeger among them are also re-derived from their copy steps by an exact linear program, all of them are compared with the published formulas, and the Lean proof below proves each of them from its copy steps. For the certificates of Section 3, a comparison script confirms that the two checkers compute the same relations and the same closures.

Table 1 also records three further checks. A negative test alters one item of a certificate. Both checkers reject each altered certificate, except a few that are again valid certificates, and the second checker also fails when rule (INJ) is switched off. On explicit joint laws of the glued variables, built from random laws of (X, Y) with up to 15 support points and from the 13-point law of [22] behind the record lower bound for C_{3b} , all rows hold, all identifications are equalities of laws, all closures are functions of their generators, and (3.3) holds with the true entropies up to rounding errors of order 10^{-14} . For the two-set certificate the same is done with explicit sets X, Y , including pairs with $|X - Y| > |X + Y|$, and random choices of Γ . A third script compares, for each set of forms in a certificate, the closures over $\mathbb{Q}$ with those over $\mathbb{Z}$ and over $\mathbb{Z}[1/m]$ for small m .

Formal verification. Some of the results are also proved in Lean 4 [23] with Mathlib [19]. The proofs build on Kleinwaks' Lean library [16], which we ported to a newer version of Lean and Mathlib without changing its statements. For the certificates of Theorems 1.1 and 1.3, a Python program translates the certificate into Lean source. Each row becomes a lemma proved from general facts, two sets of forms with the same closure are shown to determine each other by explicit derivations with the rules (a)–(c) of Lemma 2.3, which the kernel checks by evaluation, and the tactic `linear_combination` checks the weighted sum of the rows. The theorems of

Table 2 do not mention the certificates, so the translation program need not be trusted. Their statements use definitions from Mathlib, from Kleinwaks' library and from our hand-written files, except that the injectivity of $(x, y) \mapsto x - y$ on a finite set is abbreviated in one line of a generated file. They depend only on the three standard axioms of Lean. In an independent replay, the exported proofs of all theorems of Table 2 except `admissibleK_le_value` were also accepted by `leanchecker` and by two further kernel implementations, `nanoda` [24] and `lean4lean` [3].

In the formalization of the certificate of Theorem 1.1, the copy steps of Section 3.2 are built with Kleinwaks' formal construction behind Lemma 2.1, and the relations of each step, the identifications (EL) and rule (INJ) are proved for this construction. Each inequality that the certificate proves by Lemma 2.2 becomes a Lean theorem about arbitrary random variables, proved from its own copy steps and, where the certificate does so, from earlier such inequalities applied to joint variables. The Lean files for this certificate prove the first four theorems of Table 2. The proof of `entropy_ineq_general` formalizes part (a) of Lemma 3.1. The Lean files of this release do not cover groups other than $\mathbb{R}$ or the product form in part (b) of Theorem 1.1.

In the formalization for Theorem 1.3, a row for the configuration of Γ' is the same lemma applied to Γ' , and a variable of type (i, j) is realized as the sum of i first coordinates and j second coordinates of further independent copies of (X_1, Y_1) , which does not change the joint law of the configuration. Rows (R8) are proved by realizing the configuration of Γ' from the copies of (X_1, Y_1) as in the justification of (R8). The Lean files for this certificate prove the last five theorems of Table 2. The theorem `pair_ceiling_torsionFree` follows from `pair_ceiling` by a formal version of the reduction to $\mathbb{Z}$ in the proof of Theorem 1.3 (`card_sub_le_of_int`). The step from `pair_ceiling` to `theta_le` is Kleinwaks' formal proof for his reading. For `thetaK_le` and `admissibleK_le_value` we adapt its last step to a fixed K , and the main estimate [16, Proposition 3.5] is again taken from his library.

TABLE 1. The certificates and their checks. A certificate NAME is the file `certs/NAME.json` of the repository. Times are wall-clock seconds on one core. Negative tests: the number of certificates altered in one item (a multiplier, a λ , a row, a copy step, a cross form, an identification, a proved inequality or its proof, a permutation, a grid index or a type), and in parentheses the number that the checkers accept. The last six rows of each part identify the certificate file and record the checks made on it; they are not steps of the proofs.

(a) The Kakeya-type exponent; checker <code>check630.py</code>			
	Theorem 1.1	Theorem 1.2	Appendix A
Certificate	c3b_torsionfree	c3b_allgroups	c3b_short
Checked bound	1.8272963	1.8294282	1.8322441
Cross forms used	41 of 43	20 of 21	5 of 5
Shannon rows	255	139	82 (72 grouped)
Proved inequalities	72 (35 rows)	none	none
Identities (CI)	3	3	3
Identifications (EL)	21	21 (19 needed)	16
Closed sets used	331	172	103
Rule (b) used	$c = 2^k$	no	no
Valid in	groups without 2-torsion	all abelian groups	all abelian groups
SHA-256 (prefix)	2f553651	a7d47d40	244f0ff7
Checker time	9	3	1
Second checker	accepts	accepts	accepts
Negative tests	64 (4)*	41 (2)*	36 (0)
Joint laws checked	321	321	321
Lean 4 proof	CL3B6SC	none	none
(b) The two-set exponent; checker <code>check3.py</code> ; variables D_0, D_1, w, v for Γ and for Γ'			
	Theorem 1.3		
Certificate	pair_exponent		
Checked bound	$\lambda < 1.42229952$		
Forms (with $\mathcal{W}$)	62 (42)		
Shannon rows	799		
Identities (R2)	5		
Identities (R4)	2		
Identities (R5)	29		
Identities (R3)	328		
Identities (R8)	142		
Support rows (R6)	1		
Grid rows (depth 12)	163		
Closed sets used	1332 (Γ), 195 (Γ')		
Rule (b) used	yes		
SHA-256 (prefix)	d0cf73dc		
Checker time	2		
Second checker	accepts		
Negative tests	45 (0)		
Triples (X, Y, Γ)	55		
Lean 4 proof	Y0		

*The accepted modifications drop an identification (EL) that the identity does not use (two in **c3b_allgroups**) or replace a cross form by its negative or by twice it (four in **c3b_torsionfree**), which leaves the closures unchanged in the groups of the row *Valid in*. They are again valid certificates.

TABLE 2. The theorems of the Lean proofs. The numbers $\lambda_X, \lambda_Y, \lambda_S$ and λ are those of the certificates.

Lean theorem	Statement
Theorem 1.1; namespace EntropyBounds.Glue.Certs.CL3B6SC	
entropy_ineq	(3.1) for every pair (X, Y) of real random variables whose law is supported on a finite set on which $(x, y) \mapsto x - y$ is injective
entropy_ineq_general	part (a) of Theorem 1.1 for all real random variables X, Y with finitely many values
entropy_max	(1.2) with $C = \lambda_X + \lambda_Y + \lambda_S$
set_ineq'	(1.1) with the same C for all finite $A, B \subset \mathbb{R}$ and $G \subseteq A \times B$
Theorem 1.3 and Corollary 1.4; namespace EntropyBounds.TwoSet.Certs.Y0	
pair_ceiling	$ X - Y \leq X + Y ^\lambda$ for all finite $X, Y \subset \mathbb{Z}$
pair_ceiling_torsionFree	$ X - Y \leq X + Y ^\lambda$ for all finite subsets X, Y of a torsion-free abelian group
thetaK_le	$C_{3a} \leq 2 - 1/\lambda$: the supremum of the admissible exponents is at most $2 - 1/\lambda$ in the reading with fixed K and c (Section 4.4)
admissibleK_le_value	every exponent admissible in the reading with fixed K and c is at most $2 - 1/\lambda$
theta_le	the same bound for the supremum in Kleinwaks' reading, with every $K > 1$

6. CONCLUDING REMARKS

The lower bounds recorded in [30] leave gaps of about 0.05 for C_{3b} and about 0.1 for C_{3a} . In floating point, the Shannon linear programs on the configurations of Sections 3 and 4 do not improve the earlier bounds without the new variables: with standard forms only, the optimum for C_{3b} is 11/6 (Remark 3.4), and with D_0 and D_1 alone and the forms with coefficients in $\{-1, 0, 1\}$, the optimum for λ is 1.4621, above the exponent 1.4543 of [16] (Remark 4.3). We do not know how far larger configurations, more cross forms or further non-Shannon inequalities can lower the two exponents.

APPENDIX A. A SHORT CERTIFICATE

The certificate `c3b_short.json` proves $H(X, Y) \leq \frac{314}{459}H(X) + \frac{302}{459}H(Y) + \frac{225}{459}H(X + Y)$ for injective pairs in any abelian group. By Lemma 3.1 it gives the exponent $841/459 < 1.8322441$ in all abelian groups. It uses the configuration (3.2) and the five cross forms

$$y_0 - x_4, \quad x_0 + y_0 + x_2, \quad x_0 + y_1 + x_2, \quad x_0 + y_1 - x_4, \quad y_0 + y_1 + x_2.$$

Let $\text{CI}_t = H(V, U') + H(O) - H(O, U') - H(V)$ be the expression of (CI) for step (St), and let I_k be the 72 mutual informations of Table 4 with weights w_k . Then

$$(A.1) \quad 459 H(X, Y) + \sum_k w_k I_k - 220 \text{CI}_1 - 79 \text{CI}_2 - 69 \text{CI}_3 = 314 H(X) + 302 H(Y) + 225 H(X + Y)$$

holds after each joint entropy is replaced by the entropy of the closure of its forms, which uses only rules (a) and (c), and after the identifications of Table 3 are applied. Since $I_k \geq 0$ and $\text{CI}_t = 0$, (A.1) gives the stated inequality. In the certificate file each I_k is expanded by the chain rule into inequalities of the first kind in (i), all with the weight $w_k/459$. Comparing (A.1) with 76.5 times the identity of Proposition 3.2 gives

$$153 \Delta_{\text{KT}} = 2 \sum_k w_k I_k + 8H(Y) + 9H(X + Y) - 16H(X) \geq 8H(Y) + 9H(X + Y) - 16H(X).$$

TABLE 3. The identifications (EL) of the short certificate, by copy step.

Step	Identification	Step	Identification
1	$H[y_0] = H[y_1]$	2	$H[(x_0 + y_1, x_0 + y_0)] = H[(y_1 + x_2, y_0 + x_2)]$
1	$H[x_0 + y_0] = H[x_0 + y_1]$	2	$H[(y_1, x_0 + y_0)] = H[(y_1, y_0 + x_2)]$
1	$H[x_0 - y_0] = H[x_0 - y_1]$	3	$H[x_0] = H[x_4]$
2	$H[x_0] = H[x_2]$	3	$H[y_0] = H[x_0 + y_0 - x_4]$
2	$H[x_0 + y_0] = H[y_0 + x_2]$	3	$H[x_0 - y_0] = H[x_0 + y_0 - 2x_4]$
2	$H[x_0 + y_1] = H[y_1 + x_2]$	3	$H[x_0 - y_1] = H[y_1 - x_4]$
2	$H[(x_0 - y_1, y_0)] = H[(y_1 - x_2, y_0)]$	3	$H[(x_0 - y_1, y_0)] = H[(y_1 - x_4, x_0 + y_0 - x_4)]$
2	$H[(x_0 + y_1, y_0)] = H[(y_1 + x_2, y_0)]$	3	$H[(x_0 + y_1, y_0)] = H[(y_1 + x_4, x_0 + y_0 - x_4)]$

APPENDIX B. THE CERTIFICATE FOR THEOREM 1.1

Table 5 lists the cross forms of `c3b_torsionfree.json` and Table 6 its applications of the inequalities proved in the certificate. The exact multipliers are in the certificate.

TABLE 4. The 72 Shannon inequalities $I_k \geq 0$ of the short certificate with their weights w_k . A tuple in parentheses is one random variable, and a list after the bar is the conditioning tuple.

w_k	I_k	w_k	I_k
81	$I(y_0; y_1)$	2	$I(y_0; x_4 x_0 + y_1 + x_2)$
68	$I(x_0 + y_0; y_1)$	2	$I(x_0 + y_1; x_4 y_0 + x_2)$
38	$I(y_0; x_0 + y_1)$	2	$I(y_0 - x_4; x_0 + y_0 + x_2 x_0 + y_1 + x_2)$
22	$I(x_0 + y_0; x_0 + y_1)$	1	$I(y_1; y_0 + x_2 x_4)$
20	$I(x_0; y_0 + x_2)$	10	$I(y_0; y_1 x_0, x_2)$
19	$I(x_0 + y_0; x_2)$	7	$I(x_0; x_4 y_1, x_0 + y_0)$
17	$I(x_0 + y_0 + x_2; (y_1 + x_4, x_0 + y_0 - x_4))$	5	$I(y_1; x_2 x_0, y_1 + x_4)$
14	$I(x_0 + y_1 + x_2; (y_1 + x_4, x_0 + y_0 - x_4))$	5	$I(x_2; x_0 y_1 - x_4, x_0 + y_0 + x_2)$
13	$I(x_0; x_0 + y_0 - x_4)$	5	$I(x_0; x_0 + y_0 - x_4 x_2, y_1 + x_4)$
12	$I(x_0; y_1 + x_2)$	5	$I(y_0 - x_4; y_1 + x_4 x_0, y_0 + x_2)$
12	$I(x_0 + y_1; x_2)$	5	$I(x_0 + y_1; y_0 - x_4 x_2, y_1 + x_4)$
11	$I(y_0; x_4)$	4	$I(x_0; y_0 + x_2 x_0 + y_1, x_0 + y_0 - 2x_4)$
11	$I(y_0 - x_4; (y_0 + x_2, y_1 + x_2))$	4	$I(x_0; y_1 x_2, x_0 + y_0 - 2x_4)$
9	$I(x_0 + y_0 - x_4; (y_0 + x_2, y_1 + x_2))$	3	$I(x_0; x_2 y_0, y_1 - x_4)$
7	$I(x_0; x_0 + y_1 - x_4)$	3	$I(x_0; y_1 + x_2 x_4, y_0 + x_2)$
7	$I(x_0 + y_1; x_4)$	3	$I(y_0; y_1 + x_2 x_4, x_0 + y_0 + x_2)$
5	$I(y_0 + x_2; (x_0, y_1 + x_4))$	2	$I(x_0; x_4 y_1, x_0 + y_0 + x_2)$
5	$I(x_0 + y_0 + x_2; y_0 + y_1 + x_2)$	2	$I(x_0; x_0 + y_0 - x_4 x_0 + y_1, y_0 + x_2)$
3	$I(x_0 + y_0 - x_4; (x_0, y_0 + x_2))$	2	$I(x_0 + y_0; y_1 x_4, x_0 + y_1 + x_2)$
2	$I(x_0; (y_0 + x_2, y_1 + x_2))$	2	$I(x_0; y_0 y_1 - x_4, x_0 + y_1 + x_2)$
2	$I(x_0; (y_0 + x_2, x_0 + y_1 - x_4))$	2	$I(x_0; x_0 + y_0 - x_4 x_0 + y_0 + x_2, x_0 + y_1 + x_2)$
2	$I(y_1 + x_2; (x_0, y_0 - x_4))$	2	$I(x_0; y_0 y_0 - x_4, x_0 + y_1 + x_2)$
2	$I(x_0 + y_1 + x_2; y_0 + y_1 + x_2)$	2	$I(x_0; x_2 x_0 + y_1 + x_2, x_0 + y_0 - 2x_4)$
19	$I(x_0; x_2 x_0 + y_0 + x_2)$	2	$I(y_1; x_0 + y_0 - x_4 y_0, x_0 + y_1 + x_2)$
12	$I(x_0; x_2 x_0 + y_1 + x_2)$	2	$I(x_4; y_1 + x_2 y_0 + x_2, x_0 + y_1 - x_4)$
11	$I(x_0; y_0 y_0 - x_4)$	1	$I(x_0; x_4 y_1, y_0 + x_2)$
10	$I(x_0; y_1 + x_4 x_2)$	5	$I(y_0; x_0 x_2, y_1 + x_4, y_0 - x_4)$
9	$I(x_2; x_4 x_0 - y_0)$	5	$I(y_1; y_0 x_2, y_1 + x_4, x_0 + y_0 - x_4)$
7	$I(y_0; y_1 y_0 + y_1 + x_2)$	5	$I(x_0; y_0 x_2, x_0 + y_1, y_1 + x_4)$
7	$I(x_4; (y_0 + x_2, y_1 + x_2) x_0 + y_1 - x_4)$	3	$I(x_0; y_1 y_0, x_4, x_0 + y_0 + x_2)$
4	$I(x_0 + y_1; x_2 x_0 + y_0 - 2x_4)$	3	$I(y_0; x_0 + y_0 x_4, y_0 + x_2, y_1 + x_2)$
3	$I(x_0; x_4 x_0 + y_0 + x_2)$	3	$I(y_1; x_0 x_4, y_1 + x_2, x_0 + y_0 + x_2)$
3	$I(y_0; x_0 + y_0 + x_2 y_1 - x_4)$	2	$I(y_0; y_1 x_0, y_0 + x_2, y_0 - x_4)$
2	$I(x_2; x_4 x_0 - y_1)$	2	$I(x_0; x_2 y_0, x_0 + y_0 - x_4, x_0 + y_1 + x_2)$
2	$I(x_4; y_1 + x_2 x_0 - y_0)$	2	$I(x_2; y_0 x_0 + y_0 - x_4, x_0 + y_0 + x_2, x_0 + y_1 + x_2)$
2	$I(y_0; x_0 + y_0 + x_2 y_1)$	2	$I(x_4; y_0 x_0 + y_1, y_0 + x_2, x_0 + y_0 - x_4)$

TABLE 5. The 43 cross forms of `c3b_torsionfree.json`, in the free coordinates of (3.2). The forms marked with an asterisk occur in no row.

$x_0 - x_2, x_0 + x_2, x_0 - x_4, x_0 + x_4, y_0 - y_1, y_0 + y_1, y_0 - x_4, x_2 - x_4, x_2 + x_4, x_0 - y_0 + y_1,$
 $x_0 + y_0 - y_1, x_0 + y_0 + y_1, x_0 - y_0 - x_2, x_0 + y_0 - x_2, x_0 + y_0 + x_2, x_0 - y_0 - x_4, x_0 + y_1 - x_2,$
 $x_0 + y_1 + x_2, x_0 - y_1 - x_4, x_0 - y_1 + x_4, x_0 + y_1 - x_4, x_0 + y_1 + x_4, x_0 - x_2 - x_4, x_0 + x_2 - x_4,$
 $y_0 - y_1 + x_2, y_0 + y_1 + x_2, y_0 - y_1 - x_4, y_0 + y_1 - x_4^*, y_0 + x_2 - x_4, y_1 + x_2 + x_4,$
 $x_0 - y_0 + y_1 + x_2^*, x_0 + y_0 + y_1 + x_2, x_0 + y_0 - y_1 - x_4, x_0 + y_0 + y_1 - x_4, x_0 + y_0 - x_2 - x_4,$
 $x_0 + y_0 + x_2 - x_4, x_0 + y_1 - x_2 + x_4, y_0 - y_1 - x_2 - x_4, y_0 - y_1 + x_2 - x_4, x_0 + y_0 + y_1 + x_2 - x_4,$
 $x_0 + y_0 - y_1 - x_2 - x_4, x_0 - y_1 - x_2, y_0 + y_1 + x_2 - x_4.$

TABLE 6. The 35 applications of inequalities proved in `c3b_torsionfree.json`: Matuš's inequality M_s and entries of the list [5, Section VIII], applied to joint variables a, b, c, d , with their multipliers μ_k in (3.3) rounded to three significant digits. Forms are shown up to sign.

Inequality	μ_k	a	b	c	d
M_7	$6.94 \cdot 10^{-6}$	x_2	$x_0+y_0-y_1-x_2-x_4$	y_1+x_2	$x_0-x_2-x_4$
M_7	$5.94 \cdot 10^{-6}$	x_2	$x_0+y_0-y_1-x_2-x_4$	y_1+x_2	$x_0+y_0-x_2-x_4$
M_{10}	$3.34 \cdot 10^{-6}$	$(y_0, x_0+y_0-y_1-x_2-x_4)$	$(x_2, x_0+y_0-y_1-x_4)$	$(y_1, x_0+y_0-x_2-x_4)$	x_0-x_4
M_{11}	$1.76 \cdot 10^{-5}$	$(x_0+y_0-x_4, y_1+x_2+x_4)$	$(y_0+x_2, y_0-y_1-x_4)$	$(y_0, y_1+x_2+x_4)$	$(y_1+x_2, x_0+y_0-y_1-x_4)$
M_{15}	$3.43 \cdot 10^{-6}$	(y_1+x_2, x_0-x_4)	$(x_0+y_0-x_4, y_0+y_1+x_2)$	$(y_1, x_0-x_2-x_4)$	$y_0+x_2-x_4$
M_{16}	$1.76 \cdot 10^{-6}$	$(y_0+x_2, y_0-y_1-x_4)$	$(x_0+y_1, x_0+y_0-x_4)$	(y_1, y_0-x_4)	x_0-x_4
M_{17}	$6.13 \cdot 10^{-6}$	$(y_1+x_2, y_0-y_1-x_4)$	$(x_0+y_1, x_0+y_0-x_4)$	$(x_0-x_4, x_0-y_0+y_1)$	y_1
M_{57}	$2.57 \cdot 10^{-7}$	(y_0+x_2, y_0-x_4)	(x_0-x_2, x_0+x_4)	(x_0, x_2+x_4)	$y_0+x_2-x_4$
M_{62}	$5.09 \cdot 10^{-9}$	(y_0+x_2, y_0-x_4)	(x_0-x_2, x_0+x_4)	(x_0, x_2+x_4)	$y_0+x_2-x_4$
DFZ 5	$6.48 \cdot 10^{-4}$	$y_0+y_1+x_2$	$y_0+x_2-x_4$	y_0+x_2	$y_0+y_1+x_2-x_4$
DFZ 5	$1.52 \cdot 10^{-4}$	x_0-x_4	$y_0+x_2-x_4$	x_2	x_4
DFZ 7	$3.04 \cdot 10^{-3}$	(y_1+x_2, x_4)	(x_4, x_0-x_2)	(x_2, x_4)	$x_0-y_1-x_2$
DFZ 7	$2.70 \cdot 10^{-4}$	$(y_1+x_2, y_0-y_1-x_4)$	$(x_0+y_0-x_4, x_0-x_2)$	(x_2, y_0-x_4)	$(y_0+x_2-x_4, x_0+y_0-y_1-x_4)$
DFZ 7	$1.95 \cdot 10^{-5}$	$(x_0-x_2, y_0-y_1-x_4)$	$(y_0+x_2, y_0-y_1-x_4)$	$(x_2, y_0-y_1-x_4)$	$x_0-y_0-x_2$
DFZ 8	$1.10 \cdot 10^{-3}$	$(x_0+y_0-x_4, x_0-x_2)$	$(x_0+y_1, y_0+x_2-x_4)$	$(x_0-x_4, x_0-y_0-x_2)$	$x_0+y_1-x_2$
DFZ 8	$4.73 \cdot 10^{-4}$	y_0-x_2	$(y_0+x_2, y_0-y_1-x_4)$	(y_0+x_2, y_1+x_2)	(y_0+x_2, y_0-x_4)
DFZ 8	$5.03 \cdot 10^{-5}$	$(x_0+y_1, x_0+y_0-x_4)$	$(y_0, x_0+y_0-x_4)$	$(x_0, x_0+y_0-x_4)$	$x_0+y_1-x_4$
DFZ 33	$1.65 \cdot 10^{-6}$	$(y_0+x_2, y_0-y_1-x_4)$	$(x_2, y_0-y_1-x_4)$	$(x_0-x_2, y_0-y_1-x_4)$	x_2+x_4
DFZ 35	$2.14 \cdot 10^{-5}$	$(x_0+y_0-x_4, y_1+x_2+x_4)$	$(x_0+y_1, x_0-x_2-x_4)$	$(x_0-x_4, x_0+y_1+x_2)$	$(y_1+x_2+x_4, x_0+y_0+y_1-x_4)$
DFZ 56	$1.71 \cdot 10^{-4}$	(y_0+x_2, x_0-x_4)	(x_0-x_2, x_0-x_4)	(x_2, x_0-x_4)	$x_0-y_0-x_2$
DFZ 60	$1.42 \cdot 10^{-3}$	$x_0+y_0-x_2$	$x_0+y_0+x_2$	$x_0-y_0-x_2$	$(y_1+x_4, x_0+y_0+y_1+x_2-x_4)$
DFZ 77	$3.74 \cdot 10^{-6}$	$(y_1, x_0-x_2-x_4)$	$(y_0-y_1, x_0-x_2-x_4)$	$(y_1+x_2, x_0+y_1-x_4)$	$x_0+y_0-y_1-x_4$
DFZ 107	$2.67 \cdot 10^{-7}$	$(y_1+x_4, x_0+y_1-x_2)$	$(x_0-x_2-x_4, y_0-y_1+x_2)$	$(y_1, x_0-x_2-x_4)$	$y_0-y_1+x_2-x_4$
DFZ 109	$1.25 \cdot 10^{-3}$	y_1-x_4	$(x_0+y_0-x_4, y_1+x_4)$	(x_0+y_1, y_1+x_4)	(y_1+x_4, y_0+y_1)
DFZ 109	$1.25 \cdot 10^{-3}$	(x_0+y_1, y_0+x_2)	(x_0+y_1, y_1+x_2)	(x_0+y_1, x_2)	$y_0+y_1+x_2$
DFZ 109	$1.22 \cdot 10^{-3}$	(x_0+y_0, y_1+x_2)	(x_0+y_0, y_0+x_2)	(x_0+y_0, x_2)	$y_0+y_1+x_2$
DFZ 109	$9.62 \cdot 10^{-4}$	(y_0, y_1+x_4)	$(y_0, x_0+y_0-x_4)$	(y_0, x_4)	$x_0+y_0-y_1-x_4$
DFZ 109	$1.80 \cdot 10^{-4}$	$(x_0+y_0-x_4, x_0-x_2)$	(y_0, x_0-x_2)	(x_0+y_0, y_0+x_2)	$y_0-y_1-x_2-x_4$
DFZ 109	$1.14 \cdot 10^{-4}$	$(x_0+y_1, x_0-y_0-x_2)$	$(x_0+y_1, x_0-x_2-x_4)$	(x_0+y_1, y_1+x_4)	y_0+x_2
DFZ 109	$8.16 \cdot 10^{-5}$	x_0-x_4	$x_0+y_0+y_1+x_2-x_4$	$x_0+y_0-x_4$	$x_0+y_1+x_2$
DFZ 109	$6.47 \cdot 10^{-5}$	$(x_0+y_1, x_0+y_0-x_4)$	(x_0+y_1, x_4)	(x_0+y_1, y_1+x_4)	(x_0+y_1, y_0-x_4)
DFZ 109	$3.87 \cdot 10^{-5}$	(x_0+y_0, y_1+x_2)	(x_0+y_1, y_1+x_2)	(x_0, y_1+x_2)	$x_0+y_0-x_2$
DFZ 109	$1.55 \cdot 10^{-5}$	x_0-x_4	$x_0-y_0-x_2$	x_0	$x_0-x_2-x_4$
DFZ 109	$1.39 \cdot 10^{-5}$	x_4	$x_0+y_0+y_1-x_4$	y_0-x_4	$x_0+y_1-x_4$
DFZ 109	$3.01 \cdot 10^{-6}$	x_0-y_0	$(x_0, y_0-y_1-x_4)$	$(x_0, x_0+y_0-x_4)$	y_0-y_1

DATA AVAILABILITY

The certificates, the checkers, the Lean proofs, the programs that found the certificates and the scripts behind Table 1 are archived at doi:10.5281/zenodo.23509966 and available at <https://github.com/tejasvi/sum-difference-exponents>.

USE OF AI TOOLS

Generative AI tools were used to find and prove the results, to write the programs and the Lean formalization, and to draft the text. The author reviewed the arguments, the programs and the formal proofs, and takes responsibility for the content.

REFERENCES

- [1] T. F. Bloom, *Erdős problem #1097*, <https://www.erdosproblems.com/1097>, accessed October 20, 2026; the problem was posed at the 1989 Great Western Number Theory problem session.
- [2] J. Bourgain, *On the dimension of Kakeya sets and related maximal inequalities*, Geom. Funct. Anal. **9** (1999), 256–282.
- [3] M. Carneiro, *Lean4Lean: Verifying a typechecker for Lean*, in *Lean*, arXiv:2403.14064, 2024.
- [4] E. P. Csirmaz and L. Csirmaz, *Information inequalities for five random variables*, Computation **14** (2026), no. 2, article 42; arXiv:2512.23316.
- [5] R. Dougherty, C. Freiling and K. Zeger, *Non-Shannon information inequalities in four random variables*, arXiv:1104.3602, 2011.
- [6] A. Farnamfar, *Sharp optimality of 11/6 for literal ladder constructions*, Zenodo, doi:10.5281/zenodo.23337952, 2026.
- [7] A. Farnamfar, *Sharp colour bounds and structural obstructions for three-direction sums-differences constructions*, Zenodo, doi:10.5281/zenodo.23385419, 2026.
- [8] G. A. Freiman and V. P. Pigarev, *The relation between the invariants R and T* (Russian), Kalinin. Gos. Univ., Moscow, 1973, 172–174.
- [9] B. Georgiev, J. Gómez-Serrano, T. Tao and A. Z. Wagner, *Mathematical exploration and discovery at scale*, arXiv:2511.02864, 2025.
- [10] B. Green and I. Z. Ruzsa, *On the arithmetic Kakeya conjecture of Katz and Tao*, Period. Math. Hungar. **78** (2019), 135–151.
- [11] K. Gyarmati, F. Hennecart and I. Z. Ruzsa, *Sums and differences of finite sets*, Funct. Approx. Comment. Math. **37** (2007), 175–186.
- [12] F. Hennecart, G. Robert and A. Yudin, *On the number of sums and differences*, Astérisque **258** (1999), 173–178.
- [13] Q. Huangfu and J. A. J. Hall, *Parallelizing the dual revised simplex method*, Math. Program. Comput. **10** (2018), 119–142.
- [14] N. H. Katz and T. Tao, *Bounds on arithmetic projections, and applications to the Kakeya conjecture*, Math. Res. Lett. **6** (1999), 625–630.
- [15] N. H. Katz and T. Tao, *New bounds for Kakeya problems*, J. Anal. Math. **87** (2002), 231–263.
- [16] L. J. Kleinwaks, *Improved sum-difference inequalities in abelian groups*, proof paper, version 1.1 (October 6, 2026), and Lean formalization, <https://github.com/kleinwaks/sum-difference>, archived as doi:10.5281/zenodo.23200803.
- [17] M. Lemm, *New counterexamples for sums-differences*, Proc. Amer. Math. Soc. **143** (2015), 3863–3868.
- [18] M. Madiman, *On the entropy of sums*, in: Proc. IEEE Information Theory Workshop, Porto, 2008, 303–307.
- [19] The mathlib Community, *The Lean mathematical library*, in: Proc. 9th ACM SIGPLAN Int. Conf. Certified Programs and Proofs (CPP 2020), 2020, 367–381.
- [20] F. Matúš, *Infinitely many information inequalities*, in: Proc. IEEE Int. Symp. Information Theory, Nice, 2007, 41–44.
- [21] Mosaic Intelligence, *A mechanized certificate ladder and a certified Shannon wall for the Katz–Tao sum-difference problem*, Zenodo, doi:10.5281/zenodo.20646386, 2026.
- [22] Mosaic Intelligence, *Certified sum-difference lower-bound certificates for C_{3a} , C_{3b} , and C_{3c}* , certificate archive, doi:10.5281/zenodo.20794135, 2026.
- [23] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction – CADE 28, Lecture Notes in Comput. Sci. **12699**, Springer, 2021, 625–635.
- [24] *nanoda_lib*, a type checker for Lean 4, https://github.com/ammkrn/nanoda_lib.

- [25] G. Petridis, *New proofs of Plünnecke-type estimates for product sets in groups*, *Combinatorica* **32** (2012), 721–733.
- [26] I. Z. Ruzsa, *An analog of Freiman’s theorem in groups*, *Astérisque* **258** (1999), 323–326.
- [27] I. Z. Ruzsa, *Sumsets and entropy*, *Random Structures Algorithms* **34** (2009), 1–10.
- [28] T. Tao, *Sumset and inverse sumset theory for Shannon entropy*, *Combin. Probab. Comput.* **19** (2010), 603–639.
- [29] T. Tao, *Sum-difference exponents for boundedly many slopes, and rational complexity*, arXiv:2511.15135, 2025.
- [30] T. Tao et al., *Optimization constants in mathematics*, <https://teorth.github.io/optimizationproblems/>, pages 3a and 3b, accessed October 19, 2026.
- [31] Z. Zhang and R. W. Yeung, *On characterization of entropy function via information inequalities*, *IEEE Trans. Inform. Theory* **44** (1998), 1440–1452.

ORCID: <https://orcid.org/0000-0003-4668-3639>