

From an entropic inequality for sums in abelian groups to the theorems of Ruzsa and Plünnecke

Chandra Nair¹, Aref Namayandeh², and Zhaobang Zhu³

^{1,2,3}Department of Information Engineering, CUHK, Hong Kong

October 8, 2026

Abstract

We give a direct information-theoretic proof of the Plünnecke–Ruzsa inequalities for finite subsets of abelian groups. The argument rests on an elementary coupling inequality proved by maximizing joint entropy, without tensor powers or asymptotic constructions. It also yields Ruzsa’s sumset triangle inequality and an extension to non-abelian groups.

1 Introduction

Inequalities for sumsets and inequalities for entropies measure the same thing — growth under addition — in two different languages. Ruzsa [1] proposed a “theory of translation” between them, and by now there is a substantial body of work developing this dictionary: the entropic Ruzsa calculus of Tao [2], the partition-determined inequalities of Madiman, Marcus and Tetali [3], the differential-entropy sumset inequalities of Kontoyiannis and Madiman [4], the recent refinements by Green, Manners and Tao [5], and the exact equivalence theorems of Ruzsa [1] and of Lau and Nair [6], the latter enlarging the translatable families via Sanov’s theorem and identifying maximal couplings of sums as the natural entropic counterpart of sumset cardinalities. This contrasts with many earlier approaches, in which sums of independent random variables served as analogues of sumset inequalities. One main motivation of the research is that inequalities for independent random variables often do not imply their additive-combinatorial counterparts.

We refer to the survey [7] for the state of this programme and for references to the large body of work that is not cited here.

Gaps remain in the connections between these fields. For example, cornerstone cardinality inequalities, including Ruzsa’s sumset triangle inequality

$$|A| |B + C| \leq |A + B| |A + C|,$$

Plünnecke’s inequality [8] and Ruzsa’s generalization [1] on magnification ratios, originally proved using graph-theoretic methods and later reproved by Petridis [9], were translatable into entropic formulation only through the equivalence theorems, whose typical-set arguments are asymptotic and require a torsion-free ambient group. In 2026, Lau, Nair, and Zhu [10] used ideas from convex optimization to give a direct information-theoretic proof of a maximal coupling form of Shearer’s lemma for sums of distributions, which implies a corresponding inequality in additive combinatorics. In the same paper, a maximal-coupling entropic analogue of the displayed inequality was explicitly conjectured for general abelian groups.

We prove the conjectured entropic analogue by establishing a stronger inequality. For any joint distribution $p_{X,Y,Z}$ with marginals p_X, p_Y, p_Z ,

$$H_p(X) + H_p(X + Y + Z) \leq \max_{q \in \Pi(p_X, p_Y)} H_q(X + Y) + \max_{r \in \Pi(p_X, p_Z)} H_r(X + Z). \quad (1)$$

Using this maximal-coupling inequality, we formulate and prove the entropic analogues of the Plünnecke–Ruzsa inequality for magnification ratios. Together with the entropic characterization of the magnification ratio in [6], these yield, in a few lines, Ruzsa’s sumset triangle inequality (Theorem 3.1), and the different-summand Plünnecke–Ruzsa inequality (Theorem 3.3), whose specialization is Plünnecke’s inequality (Theorem 3.2). These results make the connections between the entropic and additive-combinatorial statements explicit. We also establish a sumset analogue of the displayed maximal-coupling inequality (Proposition 3.5). Finally, carrying out the same argument with the ordering $U = Y \circ X \circ Z$ yields a new sumset inequality for arbitrary, possibly non-abelian groups (Corollary 4.2), recovering Ruzsa’s sumset triangle inequality in the abelian case.

Outline. Subsection 1.1 introduces the notation and elementary facts used throughout the paper. Section 2 states and proves the main coupling inequality and its entropic consequences. Section 3 transfers them to sumset inequalities. Section 4 gives the non-abelian extension.

1.1 Notation and elementary facts

Unless otherwise stated, G is an abelian group. We write $+$ for the operation in abelian groups and $\circ$ for the operation in general groups. The sets $A, B, C, D \subseteq G$ are finite and nonempty, and $A + B := \{a + b : a \in A, b \in B\}$ is the sumset of A and B . We write $\text{supp } p_X$ for the support of p_X . For distributions p_X and p_Y on finite alphabets, let $\Pi(p_X, p_Y)$ denote the convex and compact set of couplings, i.e., joint distributions of (X, Y) with $X \sim p_X$ and $Y \sim p_Y$. The magnification ratio of (A, D) is defined by $\mu(A, D) := \min_{\emptyset \neq S \subseteq A} |S + D|/|S|$. For given $\text{supp } p_X \subseteq A$, define $\Phi_D(p_X) := \max_{W_{Y|X}} [H(X + Y) - H(X)]$, where we consider $p_X, W_{Y|X}$ as an input distribution and a channel respectively, with the induced marginal $\text{supp } p_Y \subseteq D$.

Throughout, we use the concavity of $H(X)$ in p_X , the bounds $0 \leq H(X) \leq \log |\text{supp } p_X|$, the chain rule, subadditivity $H(X_1 + X_2) \leq H(X_1, X_2) \leq H(X_1) + H(X_2)$, non-negativity of conditional mutual information, the fact that conditioning cannot increase entropy, and invariance of entropy under bijections of finite alphabets.

2 The main coupling inequality

In this section, we prove our main coupling inequality and use it to derive other non-trivial entropic inequalities. The next theorem strengthens (1) and directly yields our desired max-coupling sum inequality.

Theorem 2.1 (max-coupling entropy inequality). *Let $p_{X,Y,Z}$ be a distribution on $A \times B \times C$ and let $U = X + Y + Z$. Define*

$$\mathcal{M}(p_X, p_Y, p_Z, p_U) := \{q_{X,Y,Z} : q_X = p_X, q_Y = p_Y, q_Z = p_Z, q_U = p_U\},$$

the set of couplings with marginals p_X, p_Y, p_Z and sum distribution p_U . Then

$$H(X) + H_p(X + Y + Z) \leq \max_{q \in \mathcal{M}} (H(X + Y) + H(X + Z)) \quad (2a)$$

$$\leq \max_{\Pi(p_X, p_Y, p_Z)} (H(X + Y) + H(X + Z)) \quad (2b)$$

$$\leq \max_{\Pi(p_X, p_Y)} H(X + Y) + \max_{\Pi(p_X, p_Z)} H(X + Z). \quad (2c)$$

Proof. Fix the coupling $p_{X,Y,Z} \in \Pi(p_X, p_Y, p_Z)$ and set $U = X + Y + Z$, $R = X + Y$, $S = X + Z$; let p_U be the induced distribution of U . The set $\mathcal{M}$ is a nonempty, convex and compact subset of $\Pi(p_X, p_Y, p_Z)$. Since $H_q(X, Y, Z)$ is strictly concave in q , it has a unique maximizer $q^* \in \mathcal{M}$.

Construct a distribution on (X, R, U) by the Markov recombination $q_R^* q_{X|R}^* q_{U|R}^*$, and let $q_{X,Y,Z}^{(R)}$ be the joint distribution it induces via $Y = R - X$, $Z = U - R$. The pairwise marginals satisfy

$$q_{X,R}^* = q_{X,R}^{(R)}, \quad q_{R,U}^* = q_{R,U}^{(R)};$$

since $Y = R - X$ and $Z = U - R$ are functions of these pairs, all one-dimensional marginals of X, Y, Z, U match, so $q_{X,Y,Z}^{(R)} \in \mathcal{M}$. Moreover, (X, Y, Z) and (X, R, U) are in bijection, so

$$H_{q^{(R)}}(X, Y, Z) = H_{q^{(R)}}(X, R, U) = H_{q^{(R)}}(R) + H_{q^{(R)}}(X | R) + H_{q^{(R)}}(U | R).$$

As the pairwise marginals agree, this rewrites as

$$\begin{aligned} H_{q^{(R)}}(X, Y, Z) &= H_{q^*}(R) + H_{q^*}(X | R) + H_{q^*}(U | R) \\ &= H_{q^*}(X, Y, Z) + I_{q^*}(X; U | R). \end{aligned}$$

Maximality of $H_{q^*}(X, Y, Z)$ and non-negativity of $I(X; U | R)$ forces $I_{q^*}(X; U | R) = 0$.

By the symmetric Markov recombination on (X, S, U) , also $I_{q^*}(X; U | S) = 0$. In the abelian setting the tuples (X, Y, Z) , (X, R, U) , (X, S, U) , (R, X, S) , (R, U, S) are in bijection with one another and hence share the same joint entropy. Therefore, for any joint distribution $q_{X,Y,Z}$, chain rule yields

$$H_q(R) + H_q(S) - H_q(X) - H_q(U) = I_q(R; S | X) + I_q(R; S | U) - I_q(X; U | R) - I_q(X; U | S).$$

Evaluating the above equality at q^* , the last two terms vanish, so

$$H_{q^*}(R) + H_{q^*}(S) - H_{q^*}(X) - H_{q^*}(U) = I_{q^*}(R; S | X) + I_{q^*}(R; S | U) \geq 0.$$

Since $q_X^* = p_X$, $q_U^* = p_U$, and $q^* \in \mathcal{M}$, we conclude

$$H(X) + H(X + Y + Z) \leq \max_{q \in \mathcal{M}} (H(X + Y) + H(X + Z)),$$

which is (2a). Inequality (2b) follows from $\mathcal{M} \subseteq \Pi(p_X, p_Y, p_Z)$, and (2c) follows by bounding each term by its corresponding pairwise maximum. $\square$

Remark 2.2. The second recombination uses commutativity: it preserves the distributions of $(X, X + Z)$ and of $(X + Z, X + Y + Z)$, and in a non-abelian group this need not preserve the distribution of Y . The correct non-abelian ordering is given in Section 4.

Corollary 2.3 (general max-coupling entropy inequality). *Let $k \geq 1$ and let $(X, Y_1, \dots, Y_k) \sim p$ be a distribution on $A \times \prod_{i=1}^k B_i$, with marginals $p_X, p_{Y_1}, \dots, p_{Y_k}$. Then*

$$H_p(X + Y_1 + \dots + Y_k) - H(X) \leq \sum_{i=1}^k \left[\max_{\Pi(p_X, p_{Y_i})} H(X + Y_i) - H(X) \right].$$

Proof. Induct on k , the case $k = 1$ being immediate. For $k \geq 2$, put $T = Y_2 + \dots + Y_k$. By (2c),

$$H_p(X + Y_1 + T) - H(X) \leq \max_{\Pi(p_X, p_{Y_1})} H(X + Y_1) + \max_{\Pi(p_X, p_T)} H(X + T) - 2H(X).$$

Every coupling of p_X, p_T extends via $p_{Y_2, \dots, Y_k|T}$ to a coupling with the prescribed marginals and $T = Y_2 + \dots + Y_k$. Applying the induction hypothesis to each such extension bounds the second maximum by

$$H(X) + \sum_{i=2}^k \left[\max_{\Pi(p_X, p_{Y_i})} H(X + Y_i) - H(X) \right],$$

which gives the claim. $\square$

Corollary 2.4. *Let p_X, p_Y, p_Z be distributions on A, B, C , respectively, and let $(X, Y, Z) \sim p$ be any coupling with these marginals. Then*

$$H(X) + H_p(Y + Z) \leq \max_{\Pi(p_X, p_Y)} H(X + Y) + \max_{\Pi(p_X, p_Z)} H(X + Z). \quad (3)$$

Consequently,

$$H(X) + \max_{\Pi(p_Y, p_Z)} H(Y + Z) \leq \max_{\Pi(p_X, p_Y)} H(X + Y) + \max_{\Pi(p_X, p_Z)} H(X + Z). \quad (4)$$

Proof. Note that if W is independent of X , then

$$H(X + W) \geq H(X + W | X) = H(W | X) = H(W). \quad (5)$$

Take a coupling of p_Y, p_Z maximizing $H(Y + Z)$ and extend it by an independent $X \sim p_X$. Applying (5) with $W = Y + Z$ and then (2c) gives (4). Since $H_p(Y + Z)$ is bounded by the corresponding coupling maximum, (3) follows. $\square$

Remark 2.5. Inequality (4) was conjectured by Lau, Nair and Zhu [10] for distributions supported on finite subsets of abelian groups. We prove it here as a direct consequence of Theorem 2.1. For finitely generated torsion-free abelian groups, it was known via the equivalence theorem [6] (see Corollary 2 and Remark 4 therein), but no direct proof avoiding the equivalence theorem was previously known.

Corollary 2.6 (entropic Ruzsa distance triangle inequality). *Let p_X, p_Y, p_Z be supported on finite subsets of an abelian group G . Then $d(p_X, p_Z) \leq d(p_X, p_Y) + d(p_Y, p_Z)$, where*

$$d(p_X, p_Y) := \max_{\Pi(p_X, p_Y)} H(X + Y) - \frac{1}{2}H(X) - \frac{1}{2}H(Y).$$

Proof. Apply Corollary 2.4 with the three distributions cyclically permuted and rearrange. $\square$

For a distribution p_X such that $\text{supp}(p_X) \subseteq A$ and Y taking values in D , recall

$$\Phi_D(p_X) = \max_{W_{Y|X}} H(X + Y) - H(X).$$

Theorem 2.7 (entropic Plünnecke–Ruzsa inequality). *For every p_X on A and all finite nonempty $B, C \subseteq G$,*

$$\Phi_{B+C}(p_X) \leq \Phi_B(p_X) + \Phi_C(p_X). \quad (6)$$

Proof. Let $(X, W) \sim p_{X,W}$ be any coupling with $X \sim p_X$ and $\text{supp } p_W \subseteq B + C$. Choose a representation $W = Y + Z$, with $\text{supp } Y \subseteq B$ and $\text{supp } Z \subseteq C$, as a function of W , and denote the induced marginals by p_Y, p_Z . By (2c),

$$\begin{aligned} H(X) + H_p(X + W) &\leq \max_{\Pi(p_X, p_Y)} H_q(X + Y) + \max_{\Pi(p_X, p_Z)} H_q(X + Z) \\ &\leq 2H(X) + \Phi_B(p_X) + \Phi_C(p_X), \end{aligned}$$

since $\text{supp } p_Y \subseteq B$ and $\text{supp } p_Z \subseteq C$. Subtracting $2H(X)$ and maximizing over all such couplings of (X, W) , with a fixed p_X , gives (6). $\square$

Corollary 2.8 (entropic Plünnecke–Ruzsa inequality for k summands). *For every $k \geq 1$, finite nonempty $B_1, \dots, B_k \subseteq G$ and every $\text{supp } p_X \subseteq A$,*

$$\Phi_{B_1 + \dots + B_k}(p_X) \leq \sum_{i=1}^k \Phi_{B_i}(p_X).$$

Consequently,

$$\min_{\substack{p_X \\ \text{supp } p_X \subseteq A}} \Phi_{B_1 + \dots + B_k}(p_X) \leq \min_{\substack{p_X \\ \text{supp } p_X \subseteq A}} \sum_{i=1}^k \Phi_{B_i}(p_X).$$

Proof. The first claim follows by induction from Theorem 2.7, applied to $(B_1 + \dots + B_{k-1}, B_k)$. The second follows by minimizing over $\text{supp } p_X \subseteq A$. $\square$

These inequalities yield the combinatorial results in Section 3 through the following entropic characterization of the magnification ratio, due to Lau and Nair.

Theorem 2.9 (entropic characterization of magnification ratio [6]). *Let $A, D \subseteq G$ be finite nonempty sets. Then*

$$\min_{\substack{p_X \\ \text{supp } p_X \subseteq A}} \Phi_D(p_X) = \log \mu(A, D) = \log \min_{\emptyset \neq S \subseteq A} \frac{|S + D|}{|S|}. \quad (7)$$

The original proof of the lower bound in [6] (Theorem 7) analyzes an optimal channel $W_{Y|X}^*$ for each input distribution p_X using the KKT conditions, then reweights the input classes of an optimal p_X^* while preserving the optimality of $W_{Y|X}^*$. For completeness, we provide an alternative proof using the max-flow min-cut theorem in Appendix A.

3 Implications for additive combinatorics

We now use the entropic inequalities from the previous section to obtain standalone proofs of well-known inequalities in additive combinatorics, as well as inequalities that are new to us. The aim is to enrich the connection between inequalities in the two fields and contribute to the rich programme pioneered by Ruzsa [1] and Tao [2].

3.1 Ruzsa's triangle inequality for sumsets

Theorem 3.1 (Ruzsa's sumset triangle inequality). *For all finite nonempty $A, B, C \subseteq G$,*

$$|A||B + C| \leq |A + B||A + C|. \quad (8)$$

Proof. Choose a joint distribution $p_{Y,Z}$ on $B \times C$ such that $Y + Z$ is uniform on $B + C$, and let p_Y, p_Z be its marginals. Put $p_X = \text{unif}_A$. By (4),

$$H(X) + \max_{\Pi(p_Y, p_Z)} H(Y + Z) \leq \max_{\Pi(p_X, p_Y)} H(X + Y) + \max_{\Pi(p_X, p_Z)} H(X + Z).$$

Here $H(X) = \log |A|$ and $\max_{\Pi(p_Y, p_Z)} H(Y + Z) = \log |B + C|$, while the right-hand side is at most $\log |A + B| + \log |A + C|$. Exponentiating gives (8). $\square$

3.2 The Plünnecke–Ruzsa inequality and its strengthening

We first recall Plünnecke's inequality to explain the historical connections between the results below. Plünnecke's inequality is the special case of Ruzsa's lemma below (Theorem 3.3).

Theorem 3.2 (Plünnecke's inequality [8]). *For all finite nonempty $A, B \subseteq G$ and every $k \geq 1$,*

$$\mu(A, kB) = \min_{\emptyset \neq S \subseteq A} \frac{|S + kB|}{|S|} \leq \left(\frac{|A + B|}{|A|} \right)^k,$$

where $kB := B + \dots + B$ (k times).

Ruzsa's sumset triangle inequality (Theorem 3.1) was originally proved using different-summand Plünnecke–Ruzsa inequality (Theorem 3.3), which follows from Plünnecke's inequality (Theorem 3.2) and the tensor power trick. Later, Petridis [9] developed a lemma that directly implies both the sumset triangle inequality and Plünnecke's inequality. However, to our knowledge, no direct proof of Plünnecke–Ruzsa inequality using Petridis's machinery was previously known. This motivated us to seek an entropic counterpart of Plünnecke–Ruzsa inequality, leading to Corollary 2.8 and the strengthening in Theorem 3.4. Below, we give entropic proofs of both statements.

Theorem 3.3 (Plünnecke–Ruzsa inequality [1]). *For every $k \geq 1$ and all finite nonempty $A, B_1, \dots, B_k \subseteq G$,*

$$\mu(A, B_1 + \dots + B_k) = \min_{\emptyset \neq S \subseteq A} \frac{|S + B_1 + \dots + B_k|}{|S|} \leq \prod_{i=1}^k \frac{|A + B_i|}{|A|}. \quad (9)$$

Proof. Write $D := B_1 + \dots + B_k$, so the left-hand side is $\mu(A, D)$. By Theorem 2.9 and Corollary 2.8,

$$\begin{aligned} \log \mu(A, D) &= \min_{\substack{p_X \\ \text{supp } p_X \subseteq A}} \Phi_D(p_X) \leq \min_{\substack{p_X \\ \text{supp } p_X \subseteq A}} \sum_{i=1}^k \Phi_{B_i}(p_X) \\ &\leq \sum_{i=1}^k \Phi_{B_i}(\text{unif}_A) \leq \sum_{i=1}^k \log \frac{|A + B_i|}{|A|}. \end{aligned}$$

Exponentiating gives (9). $\square$

Theorem 3.4 (strengthening of Plünnecke–Ruzsa inequality). *For every $k \geq 1$ and all finite nonempty $A, B_1, \dots, B_k \subseteq G$,*

$$\mu(A, B_1 + \dots + B_k) = \min_{\emptyset \neq S \subseteq A} \frac{|S + B_1 + \dots + B_k|}{|S|} \leq \min_{\emptyset \neq S \subseteq A} \prod_{i=1}^k \frac{|S + B_i|}{|S|}. \quad (10)$$

Proof. Write $D := B_1 + \dots + B_k$. For every nonempty $S \subseteq A$, evaluate the minimum in the proof of Theorem 3.3 at unif_S instead of unif_A . Then

$$\log \mu(A, D) \leq \sum_{i=1}^k \Phi_{B_i}(\text{unif}_S) \leq \sum_{i=1}^k \log \frac{|S + B_i|}{|S|}.$$

Exponentiating and minimizing over S gives (10). $\square$

3.3 A three-set sumset inequality

Proposition 3.5. *Let $A, B, C \subseteq G$ be finite and nonempty. Define*

$$\mathcal{G}(A, B + C) := \{p_{X,W} : p_X = \text{unif}_A, \text{supp } p_W \subseteq B + C, p_{X+W} = \text{unif}_{A+B+C}\}.$$

If $\mathcal{G}(A, B + C)$ is nonempty, then

$$|A||A + B + C| \leq |A + B||A + C|. \quad (11)$$

Proof. Choose $p_{X,W} \in \mathcal{G}(A, B + C)$ and let $(X, W) \sim p_{X,W}$. Choose a representation $W = Y + Z$, with $Y \in B$ and $Z \in C$, as a function of W , and denote the induced marginals by p_Y, p_Z . Then $X + Y + Z = X + W$ is uniform on $A + B + C$. By (2c),

$$\begin{aligned} \log |A| + \log |A + B + C| &\leq \max_{\Pi(p_X, p_Y)} H(X + Y) + \max_{\Pi(p_X, p_Z)} H(X + Z) \\ &\leq \log |A + B| + \log |A + C|. \end{aligned}$$

The last inequality follows because the sums are supported on $A + B$ and $A + C$, respectively, under every corresponding coupling. Exponentiating gives (11). $\square$

Remark 3.6 (the hypothesis cannot be dropped). Inequality (11) is false in general. In $G = \mathbb{Z}_{20}$ take

$$A = \{0, 2, 6, 7, 10, 14, 18\}, \quad B = \{11, 15\}, \quad C = \{0, 8\},$$

so that $|A| = 7$, $|A + B| = |A + C| = 9$ and $|A + B + C| = 13$. Then $|A||A + B + C| = 91 > 81 = |A + B||A + C|$. Consistently, $\mathcal{G}(A, B + C)$ is empty.

4 A non-abelian extension

The direct analogue of Theorem 2.1 is false in general non-abelian groups. The inequality

$$H(X) + H(X \circ Y \circ Z) \leq \max_{\Pi(p_X, p_Y)} H(X \circ Y) + \max_{\Pi(p_X, p_Z)} H(X \circ Z)$$

does not hold, and neither does $|A||B \circ C| \leq |A \circ B||A \circ C|$. The obstruction is the recombination step: preserving the distributions of $(X, X \circ Z)$ and $(X \circ Z, X \circ Y \circ Z)$ need not preserve the distribution of Y . With $U = Y \circ X \circ Z$, $R = Y \circ X$, and $S = X \circ Z$, however, both recombinations preserve the prescribed marginals, and the argument survives.

Theorem 4.1 (non-abelian max-coupling entropy inequality). *Let $(G, \circ)$ be a group, let $A, B, C \subseteq G$ be finite and nonempty, and let $(X, Y, Z) \sim p_{X,Y,Z}$ be any coupling of marginals p_X, p_Y, p_Z on A, B, C , respectively. Then*

$$H(X) + H_p(Y \circ X \circ Z) \leq \max_{\Pi(p_X, p_Y)} H(Y \circ X) + \max_{\Pi(p_X, p_Z)} H(X \circ Z). \quad (12)$$

Proof. Set $U = Y \circ X \circ Z$, $R = Y \circ X$, and $S = X \circ Z$, and let p_U be the induced distribution of U . Define

$$\mathcal{M}(p_X, p_Y, p_Z, p_U) := \{q_{X,Y,Z} : q_X = p_X, q_Y = p_Y, q_Z = p_Z, q_U = p_U\}.$$

As in the proof of Theorem 2.1, let q^* be the unique maximizer of $H_q(X, Y, Z)$ over $\mathcal{M}$. The identities

$$Y = R \circ X^{-1}, \quad Z = R^{-1} \circ U, \quad Z = X^{-1} \circ S, \quad Y = U \circ S^{-1}$$

show that recombination on (X, R, U) and on (X, S, U) preserves all prescribed marginals. The same maximality argument therefore gives

$$I_{q^*}(X; U \mid R) = I_{q^*}(X; U \mid S) = 0.$$

Since $U = R \circ X^{-1} \circ S$, any three of X, R, S, U determine the fourth. The corresponding triples are also in bijection with (X, Y, Z) , so the entropy identity in the proof of Theorem 2.1 applies:

$$H_{q^*}(R) + H_{q^*}(S) - H_{q^*}(X) - H_{q^*}(U) = I_{q^*}(R; S \mid X) + I_{q^*}(R; S \mid U) \geq 0.$$

Using the prescribed marginals and bounding the two sum entropies by their corresponding pairwise coupling maxima gives (12). $\square$

Corollary 4.2 (a non-abelian sumset inequality). *For all finite nonempty subsets A, B, C of a group $(G, \circ)$, we have*

$$\sum_{x \in A} |B \circ x \circ C| \leq |B \circ A| |A \circ C|. \quad (13)$$

Consequently,

$$|A| \min_{x \in A} |B \circ x \circ C| \leq |B \circ A| |A \circ C|. \quad (14)$$

Proof. For $x \in A$, put $n_x := |B \circ x \circ C|$ and $N := \sum_{x \in A} n_x$. Consider the distribution $p_X(x) = \frac{n_x}{N}$ defined over A . For every $x \in A$ and every $u \in B \circ x \circ C$, fix a representation

$$u = b_x(u) \circ x \circ c_x(u), \quad b_x(u) \in B, \quad c_x(u) \in C.$$

Conditionally on $X = x$, let U be uniform on $B \circ x \circ C$, and set $Y = b_x(U)$ and $Z = c_x(U)$. Then $U = Y \circ X \circ Z$ almost surely. The construction gives a compatible coupling for Theorem 4.1, with

$$H(U \mid X = x) = \log n_x$$

for every $x \in A$. Consequently,

$$\begin{aligned} \log N &= \sum_{x \in A} \frac{n_x}{N} \left(\log n_x - \log \frac{n_x}{N} \right) \\ &= H(U \mid X) + H(X) \\ &\leq H(U) + H(X) \\ &\leq \max_{\Pi(p_X, p_Y)} H(Y \circ X) + \max_{\Pi(p_X, p_Z)} H(X \circ Z) \\ &\leq \log |B \circ A| + \log |A \circ C|. \end{aligned}$$

The penultimate inequality follows from Theorem 4.1, and the last follows because the products are supported on $B \circ A$ and $A \circ C$, respectively. Exponentiating gives (13). The minimum bound (14) follows by bounding each summand below by the minimum. $\square$

Remark 4.3. This generalizes Ruzsa's sumset triangle inequality (Theorem 3.1): in an abelian group, $|B + x + C| = |B + C|$ for every $x \in A$, so (13) reduces to $|A||B + C| \leq |A + B||A + C|$.

Conclusion

In this work, we derive and extend some known inequalities in additive combinatorics using information-theoretic arguments. This adds to a growing body of work linking the two fields.

References

- [1] I. Z. Ruzsa, “Sumsets and entropy,” *Random Structures & Algorithms*, vol. 34, no. 1, pp. 1–10, 2009.
- [2] T. Tao, “Sumset and inverse sumset theory for Shannon entropy,” *Combinatorics, Probability and Computing*, vol. 19, no. 4, pp. 603–639, 2010.
- [3] M. Madiman, A. W. Marcus, and P. Tetali, “Entropy and set cardinality inequalities for partition-determined functions,” *Random Structures & Algorithms*, vol. 40, no. 4, pp. 399–424, 2012.
- [4] I. Kontoyiannis and M. Madiman, “Sumset and inverse sumset inequalities for differential entropy and mutual information,” *IEEE Transactions on Information Theory*, vol. 60, no. 8, p. 4503–4514, Aug. 2014.
- [5] B. Green, F. Manners, and T. Tao, “Sumsets and entropy revisited,” *Random Structures & Algorithms*, vol. 66, no. 1, 2024.
- [6] C. W. Lau and C. Nair, “Information inequalities via ideas from additive combinatorics,” *IEEE Transactions on Information Theory*, vol. 71, no. 6, pp. 4055–4068, 2025, conference version: ISIT 2023; preprint: arXiv:2312.11017.
- [7] C. Nair, “Inequalities in additive combinatorics and information theory: a short survey of the translation programme,” *IEEE BITS the Information Theory Magazine*, 2026, to appear.
- [8] H. Plünnecke, “Eine zahlentheoretische Anwendung der Graphentheorie,” *Journal für die reine und angewandte Mathematik*, vol. 243, pp. 171–183, 1970.
- [9] G. Petridis, “New proofs of Plünnecke-type estimates for product sets in groups,” *Combinatorica*, vol. 32, no. 6, pp. 721–733, 2012.
- [10] C. W. Lau, C. Nair, and Z. Zhu, “A maximal-coupling information inequality for sums on finite subsets of Abelian groups,” in *2026 IEEE International Symposium on Information Theory (ISIT)*, Guangzhou, 2026.
- [11] L. R. Ford, Jr. and D. R. Fulkerson, “Maximal flow through a network,” *Canadian Journal of Mathematics*, vol. 8, pp. 399–404, 1956.

A Alternative proof of Theorem 2.9

We give an alternative proof of Theorem 2.9 based on max-flow min-cut theorem from network flow theory.

Definition A.1 (Flow network). A flow network is a finite directed graph $G = (V, E)$, together with distinct vertices $s, t \in V$, called the source and sink, and a capacity function $c : E \rightarrow \mathbb{R}_{\geq 0} \cup \{\infty\}$. For $A \subseteq V$, write

$$\begin{aligned}\delta^+(A) &= \{(u, v) \in E : u \in A, v \notin A\}, \\ \delta^-(A) &= \{(u, v) \in E : u \notin A, v \in A\}.\end{aligned}$$

These are the edges leaving and entering A , respectively. For a single vertex v , abbreviate $\delta^\pm(\{v\})$ by $\delta^\pm(v)$.

Definition A.2 (Flow and its value). A feasible s - t flow is a function $f : E \rightarrow \mathbb{R}_{\geq 0}$ satisfying the capacity constraints

$$0 \leq f(e) \leq c(e) \quad \text{for every } e \in E,$$

and flow conservation at every vertex other than the source and sink:

$$\sum_{e \in \delta^+(v)} f(e) = \sum_{e \in \delta^-(v)} f(e) \quad \text{for every } v \in V \setminus \{s, t\}.$$

The value of f is its outflow from the source:

$$|f| = \sum_{e \in \delta^+(s)} f(e) = \sum_{e \in \delta^-(t)} f(e).$$

The second equality follows from flow conservation.

Definition A.3 (Cut and its capacity). An s - t cut is a partition (S, T) of V with $s \in S$ and $t \in T$. Its capacity $c(S, T)$ is

$$c(S, T) = \sum_{e \in \delta^+(S)} c(e).$$

For every feasible flow f and every such cut (S, T) , conservation gives

$$|f| = \sum_{e \in \delta^+(S)} f(e) - \sum_{e \in \delta^-(S)} f(e) \leq c(S, T).$$

Theorem A.1 (max-flow min-cut theorem [11]). In every flow network (G, s, t, c) as defined above, the maximum value of a feasible s - t flow equals the minimum capacity of an s - t cut, if the latter is finite:

$$\max_{f \in \mathcal{F}} |f| = \min_{\substack{S \subseteq V \\ s \in S, t \notin S}} c(S, V \setminus S),$$

where $\mathcal{F}$ is the set of feasible s - t flows. Both the maximum and the minimum are attained.

We use the following lemma.

Lemma A.2. Let $G = (A, B, E)$ be a nonempty bipartite graph without any isolated point in A , and magnification ratio

$$\mu = \mu_{A \rightarrow B}(G) := \min_{\emptyset \neq S \subseteq A} \frac{|N(S)|}{|S|},$$

where $N(S) \subseteq B$ is the neighborhood of S . Let $\mathcal{W}(G)$ be the set of channels from A to B whose transition probabilities vanish outside E . Then there exists a universal channel $W_{Y|X} \in \mathcal{W}(G)$ such that, for every input distribution p_X on A ,

$$H(Y) - H(X) \geq \log \mu,$$

where $p_Y = W_{Y|X} \circ p_X$ is the induced output distribution.

Proof. Introduce an auxiliary source s and sink t , and construct the flow network $s \rightarrow A \rightarrow B \rightarrow t$ with capacities

$$c(s, x) = 1, \quad c(x, y) = +\infty \quad ((x, y) \in E), \quad c(y, t) = \frac{1}{\mu}.$$

For any finite s - t cut, let $A' \subseteq A$ be the vertices of A on the source side. To avoid an infinite-capacity edge crossing the cut, every neighbor of A' must also lie on the source side. Hence, the cut capacity is at least

$$|A \setminus A'| + \frac{|N(A')|}{\mu} \geq |A \setminus A'| + |A'| = |A|,$$

using $|N(A')| \geq \mu|A'|$. The cut $\{s\}$ has capacity $|A|$, so the min-cut is $|A|$. By Theorem A.1, there is a flow f of value $|A|$, where all edges (s, x) are saturated. For $(x, y) \in A \times B$, define

$$W_{Y|X}(y|x) := f(x, y).$$

Then $W_{Y|X}(y|x) = 0$ for $(x, y) \notin E$, $\sum_y W_{Y|X}(y|x) = 1$, and

$$\sum_x W_{Y|X}(y|x) \leq \frac{1}{\mu}.$$

Fix any p_X on A . Let u_A, u_B denote the uniform distributions on A, B , respectively, and put $q_Y = W_{Y|X} \circ p_X$ and $r_Y = W_{Y|X} \circ u_A$. By the data-processing inequality for relative entropy,

$$D(q_Y \| r_Y) \leq D(p_X \| u_A).$$

Since $\sum_x W(y|x) \leq 1/\mu$,

$$r_Y(y) \leq \frac{1}{|A|\mu},$$

so

$$\frac{r_Y(y)}{u_B(y)} \leq \frac{|B|}{|A|\mu}.$$

Therefore

$$\begin{aligned} D(q_Y \| u_B) &= D(q_Y \| r_Y) + \sum_y q_Y(y) \log \frac{r_Y(y)}{u_B(y)} \\ &\leq D(p_X \| u_A) + \log \frac{|B|}{|A|\mu}. \end{aligned}$$

Using

$$D(p_X \| u_A) = \log |A| - H(X), \quad D(q_Y \| u_B) = \log |B| - H(Y),$$

we obtain

$$\log |B| - H(Y) \leq \log |A| - H(X) + \log \frac{|B|}{|A|\mu}.$$

Canceling terms gives

$$H(Y) - H(X) \geq \log \mu.$$

Thus the same channel $W_{Y|X}$ works for every p_X . □

Proof of Theorem 2.9. In a slight abuse of notation, to account for the additive nature of the settings considered earlier, we assume that the channel output is $X + Y$ and the input is X . Here X takes values in A and Y takes values in D . Choose $S^* \in \arg \min_{\emptyset \neq S \subseteq A} |S + D|/|S|$ and put $p_X = \text{unif}_{S^*}$. Then, for every channel $W_{Y|X}$ with output alphabet D , $H(X + Y) \leq \log |S^* + D|$, and

$$\min_{p_X} \max_{W_{Y|X}} [H(X + Y) - H(X)] \leq \log \frac{|S^* + D|}{|S^*|} = \log \mu(A, D).$$

For the reverse direction, setting $B = A + D$, and define the graph G by adding edges between pairs $(a, a + d)$ for $a \in A$ and $d \in D$, Lemma A.2 asserts that for every p_X supported on A ,

$$\max_{W_{Y|X}} [H(X + Y) - H(X)] \geq \log \mu(A, D).$$

Taking the minimum over p_X completes the proof. $\square$

Remark A.3. While Prof. Venkat Anantharam was recently visiting CUHK, we discussed our research directions as well as the characterization of the magnification ratio using an entropic functional with him. He conveyed to us that Gemini gave him an alternate proof of the result using the max-flow min-cut theorem. While no further details were exchanged, we would still like to acknowledge this discussion.

Bibliographic remarks and the use of AI

These investigations originated as a research programme between Chandra Nair and Ken Lau (who has since graduated), and has now evolved into a joint research programme pursued by Chandra Nair, Aref Namayandeh, and Zhaobang Zhu. The original motivation was to employ the ideas from additive combinatorics to aid in establishing the Gaussian optimality for certain information functionals arising in the scalar Gaussian Z-interference channel. The core mathematical objectives, connections to Plünnecke–Ruzsa theory, and the overarching strategy for translating information inequalities into additive-combinatorial statements were entirely human-conceived.

Nair provided foundational prior work—including papers by Lau–Nair and Lau–Nair–Zhu—as context for an extended dialogue with an AI assistant (accessed via Perplexity). This assistant aided in exploring candidate proof strategies, deriving optimality conditions, implementing numerical experiments, and drafting working notes and manuscript revisions. As part of this iterative process, numerous proposed arguments failed, and several mathematical claims and numerical outputs required correction or rejection. In parallel, Namayandeh and Zhu conducted extensive independent numerical investigations into feasible couplings, generating evidence that propelled the search for a direct proof.

A separate AI system, suggested the Markov recombination construction, for a related version, used in the final proof. We explicitly acknowledge this substantive and elegant observation. Consequently, the final argument leverages recombination and maximality directly, bypassing the exploratory KKT calculations. The authors have written the entire article, with minimal stylistic help for polishing and notation from AI.