Received: 23 June 2023 | Revised: 20 June 2024 | Accepted: 20 July 2024

DOI: 10.1002/rsa.21252

RESEARCH ARTICLE

WILEY

Sumsets and entropy revisited

Ben Green[1] | **Freddie Manners**[2] | **Terence Tao**[3]

[1]Mathematical Institute, Oxford, UK
[2]Department of Mathematics, University of California, La Jolla, California, USA
[3]Department of Mathematics, UCLA, Los Angeles, California, USA

Correspondence
Ben Green, Mathematical Institute, Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Rd, Oxford OX2 6QW, UK.
Email: ben.green@maths.ox.ac.uk

Funding information
NSF, Grant/Award Number: DMS-1764034; Simons Investigator, Grant/Award Number: 376201, 256485.

Abstract

The entropic doubling $\sigma_{\mathrm{ent}}[X]$ of a random variable X taking values in an abelian group G is a variant of the notion of the doubling constant $\sigma[A]$ of a finite subset A of G, but it enjoys somewhat better properties; for instance, it contracts upon applying a homomorphism. In this paper we develop further the theory of entropic doubling and give various applications, including: (1) A new proof of a result of Pálvölgyi and Zhelezov on the "skew dimension" of subsets of $\mathbf{Z}^D$ with small doubling; (2) A new proof, and an improvement, of a result of the second author on the dimension of subsets of $\mathbf{Z}^D$ with small doubling; (3) A proof that the Polynomial Freiman–Ruzsa conjecture over $\mathbf{F}_2$ implies the (weak) Polynomial Freiman–Ruzsa conjecture over $\mathbf{Z}$.

KEYWORDS

entropy, Freiman–Ruzsa, Sumsets

1 | INTRODUCTION AND STATEMENT OF RESULTS

Notation. Throughout the paper we use standard asymptotic notation. The notations $X = O(Y)$, $X \ll Y$, or $Y \gg X$ all denote the bound $|X| \leq CY$ for an absolute constant C. Different instances of the notation may imply different constants C.

1.1 | Entropy doubling and Ruzsa distance

Let $G = (G, +)$ be an abelian group. In this paper, by a "G-valued random variable" we mean a random variable X taking values in a finite subset of G. Given such a variable, the *entropic doubling constant* (first introduced in [20]) $\sigma_{\mathrm{ent}}[X]$ is defined by the formula

$$\sigma_{\mathrm{ent}}[X] := \exp\left(\mathbf{H}(X_1 + X_2) - \mathbf{H}(X)\right),$$

where X_1, X_2 are independent copies of X. Here, $\mathbf{H}(X)$ denotes the Shannon entropy of X, the definition and basic properties of which we review in Appendix A.

If $A \subseteq G$ is a finite non-empty set, by abuse of notation we write $\sigma_{\text{ent}}[A] = \sigma_{\text{ent}}[U_A]$, where U_A is a uniform random variable drawn from A. For instance, if H is a finite subgroup of G, one can check that $\sigma_{\text{ent}}[H] = 1$.

The entropic doubling constant is related to other standard measures of additive structure via the inequalities

$$\frac{|A|^3}{\mathrm{E}[A]} \leq \sigma_{\text{ent}}[A] \leq \sigma[A]. \tag{1.1}$$

Here, $\sigma[A] := \frac{|A+A|}{|A|}$ is the doubling constant of A and

$$\mathrm{E}[A] := |\{(a_1, a_2, a_3, a_4) \in A^4 : a_1 + a_2 = a_3 + a_4\}|$$

is the additive energy of A.

The second inequality in (1.1) was noted in [20, eq. 10], and we recall the proof in Appendix B. The first inequality seems not to have appeared explicitly in the literature, but it follows easily either by a direct argument using the weighted AM–GM inequality, or by quoting the monotonicity of Rényi entropy. For completeness, we give this argument in Appendix B. Both inequalities can be far from tight: we give an example in Appendix B.

1.1.1 | Entropic Ruzsa distance

If X, Y are G-valued random variables (not necessarily independent, or even defined on the same sample space), then we define the *entropic Ruzsa distance* $d_{\text{ent}}(X, Y)$ between these variables by the formula

$$d_{\text{ent}}(X, Y) := \mathbf{H}(X' - Y') - \frac{1}{2}\mathbf{H}(X') - \frac{1}{2}\mathbf{H}(Y'), \tag{1.2}$$

where X', Y' are independent copies of X, Y respectively. This concept, introduced by Ruzsa [16] and studied in more detail by the third author [20], generalizes entropic doubling, since $\sigma_{\text{ent}}[X] = e^{d_{\text{ent}}(X,-X)}$.

It is easy to see that $d_{\text{ent}}(X, Y) = d_{\text{ent}}(Y, X) \geq 0$, and also that $d_{\text{ent}}(U_H, U_H) = 0$ for any finite subgroup H of G. Note that $d_{\text{ent}}(X, Y)$ depends only on the distributions

$$p_X(x) := \mathbf{P}(X = x); \quad p_Y(y) := \mathbf{P}(Y = y)$$

of X, Y. We have (see the final paragraph of [16], [20, theorem 1.10], or Lemma 1.1 below) the *entropic Ruzsa triangle inequality*

$$d_{\text{ent}}(X, Z) \leq d_{\text{ent}}(X, Y) + d_{\text{ent}}(Y, Z) \tag{1.3}$$

for any three G-valued random variables X, Y, Z.

> *Remark.* It is somewhat traditional to use the letter K for the combinatorial doubling constant $\sigma[A]$. We will generally use the letter k for distances $d_{\text{ent}}(X, Y)$. Where these arise from sets (for instance if $X = Y = U_A$) one should informally think of k being on the order of $\log K$. It should be carefully noted that k may take values in $[0, \infty)$ and is not constrained to be an integer.

It will be technically convenient to introduce a small modification of the entropic Ruzsa distance. Define the *maximal entropic Ruzsa distance* $d^*_{\mathrm{ent}}(X,Y)$ to be the quantity

$$d^*_{\mathrm{ent}}(X,Y) := \sup_{X',Y'} \Big(\mathbf{H}(X'-Y') - \frac{1}{2}\mathbf{H}(X') - \frac{1}{2}\mathbf{H}(Y') \Big) \tag{1.4}$$

where X', Y' range over all pairs of random variables with marginal distributions p_X, p_Y respectively (i.e., all couplings of X and Y). In particular, X', Y' are *not* required to be independent.

We have the following observations.

Lemma 1.1. *Let X, Y, Z be G-valued random variables. Then*:

(*i*) *We have $d^*_{\mathrm{ent}}(X,Z) \le d_{\mathrm{ent}}(X,Y) + d_{\mathrm{ent}}(Y,Z)$.*
(*ii*) *We have $d_{\mathrm{ent}}(X,Y) \le d^*_{\mathrm{ent}}(X,Y) \le 3d_{\mathrm{ent}}(X,Y)$.*

For the proof, see Section 2.

1.1.2 | Small Ruzsa distance

We turn now to our first main result, which gives a closer connection than (1.1) between small entropy doubling (or more generally small Ruzsa distance) and small doubling. Here, for a real parameter $p \in (0,1)$, we write $\mathrm{h}(p) := p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}$ for the entropy of the Bernouilli random variable with probability p.

Proposition 1.2. *Let $C \ge 4$ be a real parameter. For any G-valued random variables X, Y there is a non-empty finite subset S of G such that, if U_S is a uniform random variable on S, then*

$$d^*_{\mathrm{ent}}(U_S, Y) \le (C+2)d_{\mathrm{ent}}(X,Y) + \mathrm{h}\Big(1 - \frac{2}{C}\Big) \tag{1.5}$$

and

$$\log\frac{|S-S|}{|S|} \le (2C+4)d_{\mathrm{ent}}(X,Y) + 2\mathrm{h}\Big(1-\frac{2}{C}\Big). \tag{1.6}$$

We isolate two special cases of this proposition for future use:

(i) If we take $C = 4$ in the above proposition, then (using, in addition, Lemma 1.1 (ii)) we obtain the bounds $d_{\mathrm{ent}}(U_S,Y) \le 6d_{\mathrm{ent}}(X,Y) + \log 2$ and $|S-S| \le 4e^{12d_{\mathrm{ent}}(X,Y)}|S|$.
(ii) If $d_{\mathrm{ent}}(X,Y) = \varepsilon$ for some $0 < \varepsilon \le \frac{1}{16}$, then on taking $C := \varepsilon^{-1/2}$ we obtain the bounds $d_{\mathrm{ent}}(U_S,Y) \ll \varepsilon^{1/2}\log\frac{1}{\varepsilon}$ and $|S-S| \le \Big(1 + O(\varepsilon^{1/2}\log\frac{1}{\varepsilon})\Big)|S|$.

We also remark that a qualitative version of this proposition (with unspecified dependence on $d_{\mathrm{ent}}(X,Y)$ on the right-hand side) was previously established in [20, proposition 5.2].

In the regime where $d_{\mathrm{ent}}(X,Y)$ is small, we can in fact obtain the following more precise result.

Proposition 1.3. *There is absolute constant $\varepsilon_0 > 0$ such that the following is true. Let X, Y be G-valued random variables, and suppose that $d_{\mathrm{ent}}(X,Y) \le \varepsilon_0$. Then there is some finite subgroup H of G such that $d_{\mathrm{ent}}(X,U_H), d_{\mathrm{ent}}(Y,U_H) \le 12d_{\mathrm{ent}}(X,Y)$.*

Remark. The constant ε_0 could be specified explicitly if desired, but we have not carried out such a calculation. The constant 12 can be improved, but we will not attempt to optimise it here.

1.1.3 | Behaviour under homomorphisms

Given the close relation between notions of entropy doubling and Ruzsa distance and the usual combinatorial notions, one would be forgiven for wondering what the point of introducing the former is.

The answer is that the entropy notions are more flexible and behave better in various ways. Most obviously, they are defined for arbitrary random variables X, with no requirement that X be uniform on a set. Related to this is the fact that the entropy notions behave well under homomorphisms in a way that the combinatorial notions do not.

The following is our main result in this direction. Here (and below) we use $(X|E)$ to denote a random variable X conditioned to a positive probability event E. We adopt the convention that expressions such as $p_{Y_1}(y_1)p_{Y_2}(y_2)d_{\mathrm{ent}}((X_1|Y_1 = y_1), (X_2|Y_2 = y_2))$ vanish if one of the events $Y_1 = y_1$, $Y_2 = y_2$ occurs with zero probability.

Proposition 1.4. *Let $\pi : G \to H$ be a homomorphism, let X_1, X_2 be G-valued random variables, and set $Y_1 := \pi(X_1)$ and $Y_2 := \pi(X_2)$. Then we have*

$$d_{\mathrm{ent}}(X_1, X_2) \geq d_{\mathrm{ent}}(Y_1, Y_2) + \sum_{y_1, y_2 \in H} p_{Y_1}(y_1)p_{Y_2}(y_2)d_{\mathrm{ent}}((X_1|Y_1 = y_1), (X_2|Y_2 = y_2)).$$

In particular, we have

$$d_{\mathrm{ent}}(X_1, X_2) \geq d_{\mathrm{ent}}(Y_1, Y_2)$$

and thus

$$\sigma_{\mathrm{ent}}[\pi(X)] \leq \sigma_{\mathrm{ent}}[X] \tag{1.7}$$

for any G-valued random variable X.

Remark. The main inequality here is a precise version of the intuition that the doubling constant of a subset of G in the presence of a homomorphism $\pi : G \to H$ should somehow be at least the doubling constant of the 'base' times some combination of the doubling constants of the 'fibres'. To make sense of this rigorously we need to pass from sets to general random variables, and replace combinatorial doubling by entropy doubling.

An example of the failure of a similar result in the purely combinatorial setting (in fact of the analogue of (1.7)) is outlined in [22, exercise 2.2.10].

Remark. Many previous works have noted the advantageous properties of entropy in somewhat related settings. To give a few examples, in rough chronological order there is the work of Avez [1] and of Kaĭmanovich and Vershik [11] on random walks on discrete groups, the work of Hochman [10] on fractals, and the work of Breuillard–Varjú [3] on Bernouilli convolutions.

1.2 | Structure of sets with small doubling

We turn now to applications of the results of the previous subsection to inverse theorems for sets with small doubling.

1.2.1 | Skew dimension

The first application is a new proof of a result of Pálvölgyi and Zhelezov [15], which they used to give a new and much shorter proof of a celebrated result of Bourgain and Chang [2]. For the purposes of this result, an *affine coordinate space* is a subset of $\mathbf{Z}^D$ (for some D) obtained by fixing the values of some possibly empty set of coordinates. For instance, $\{(2,-1,x_3) : x_3 \in \mathbf{Z}\} \subseteq \mathbf{Z}^3$ is an affine coordinate space. If A is a finite subset of some affine coordinate space V, its[1] *skew-dimension* $\dim_*(A)$ is defined inductively, as follows:

1. $\dim_*(A) = 0$ if and only if A is a singleton (or empty).
2. If $r \geq 1$, then $\dim_*(A) \leq r$ if and only if there is a coordinate map $\pi : V \to \mathbf{Z}$ such that $\dim_*(\pi^{-1}(n) \cap A) \leq r-1$ for all $n \in \mathbf{Z}$.

Theorem 1.5 (Pálvölgyi–Zhelezov)**.** *Suppose A is a finite subset of some affine coordinate space with $\sigma[A] \leq K$ for some $K \geq 2$. Then there is $A' \subseteq A$ with $|A'| \geq K^{-O(1)}|A|$ and $\dim_* A' \ll \log K$.*

This result is essentially contained in a paper [15] of Pálvölgyi and Zhelezov: whilst it is not actually stated in that paper, it is mentioned in a talk by Zhelezov [23, min 27:30], and can be established using the methods of [15]. Lecture notes of the first author may be consulted for a detailed account with some simplifications [8], as well as details of the deduction of the result of Bourgain and Chang.

In fact we will establish the following slightly stronger result.

Theorem 1.6. *There is an absolute constant C with the following property. Suppose that $A, B \subseteq \mathbf{Z}^D$. Then there are $A' \subseteq A$ and $B' \subseteq B$ with $|A'||B'| \geq e^{-Cd_{\mathrm{ent}}(A,B)}|A||B|$, and such that $\dim_*(A'), \dim_*(B') \leq Cd_{\mathrm{ent}}(A,B)$.*

Setting $B = -A$ and using (1.1), we recover Theorem 1.5. The "bilinear" form of Theorem 1.6 will be convenient for induction purposes.

1.2.2 | Dimension and PFR over $\mathbf{Z}$

Whilst the notion of skew-dimension is useful in the context of the work of Bourgain and Chang, the actual (affine) dimension $\dim A$, defined as the dimension of the span of $A - A$ over the reals, is a more intrinsically natural quantity. Note that $\dim_* A \leq \dim A$ for any A. It is conjectured that Theorem 1.5 remains true with $\dim_* A'$ replaced by $\dim A'$ – this is sometimes (see, for instance, [4], [15, conjecture 1]) called the weak Polynomial Freiman–Ruzsa conjecture (PFR) over $\mathbf{Z}$. (The term 'weak' comes from the fact that only the dimension is controlled, and no attempt is made to put A economically inside a box or homomorphic image of the lattice points in a convex set. Such stronger statements are also speculated to be true, but care must be taken in their formulation, as discussed in [13].)

Conjecture 1.7 (Weak PFR over $\mathbf{Z}$)**.** *Suppose that $A \subseteq \mathbf{Z}^D$ is a set with $\sigma[A] \leq K$. Then there is a subset $A' \subseteq A$, $|A'| \geq K^{-O(1)}|A|$, with $\dim A' \ll \log K$.*

Prior to this paper, the best known bound in the direction of this conjecture was a result of the second author [14].

Theorem 1.8 ([14, theorem 1.5])**.** *Suppose that $A \subseteq \mathbf{Z}^D$ is a finite set with $\sigma[A] \leq K$. Then there is $A' \subseteq A$ with $\frac{|A'|}{|A|} \gg \exp(-C\log^2 K)$ and $\dim A' \ll \log K$.*

[1] Pálvölgyi and Zhelezov use the term *query complexity* instead of skew dimension.

The proof of this result in [14] was a little exotic, making use of projections modulo 2 and a kind of "U^3-energy". We provide a new, shorter, proof of this result, retaining the first feature but using entropic notions in place of the exotic energy.

We will eventually go further in this paper by using results on sets with additive structure in $\mathbf{F}_2^D$ to improve the bounds, but before doing that we make a detour into the world of structure theorems for sets of small doubling in $\mathbf{F}_2^D$.

1.2.3 | Small doubling in $\mathbf{F}_2^D$ and PFR over $\mathbf{F}_2$

In the following discussion, $\mathbf{F}_2^D$ denotes the vector space of dimension D over $\mathbf{F}_2$; the value of D is typically somewhat unimportant. Essentially everything we have to say would work equally well over other finite fields $\mathbf{F}$, but this introduces some further technicalities and implied constants would need to depend on $\mathbf{F}$, and we do not discuss this aspect here.

Denote by C_{PFR} any constant for which the following statement is true: if $A \subseteq \mathbf{F}_2^D$, and if the doubling constant $\sigma[A]$ is at most K, then A is covered by $\exp(O(\log^{C_{\mathrm{PFR}}}(2K)))$ cosets of some subspace $H \leq \mathbf{F}_2^D$ of size at most $|A|$. The implied constant in the $O()$ notation is allowed to depend on C_{PFR}.

A celebrated result of Sanders [18, corollary A.2] (together with standard covering lemmas) is that one may take $C_{\mathrm{PFR}} = 4$. By an improved version of the argument due to Konyagin (see [19, theorem 1.4]), one can in fact take any $C_{\mathrm{PFR}} > 3$. Strictly speaking, the statement in [19] applies to more general abelian groups than $\mathbf{F}_2^D$, but replaces the subspace H by a convex coset progression. However, an inspection of the arguments in the characteristic 2 case shows that the convex coset progression in this case can be taken to be a subspace (basically because the convex coset progressions are constructed via Bohr sets, which are automatically subspaces in the characteristic 2 setting). Alternatively, one can invoke the discrete John theorem (see [21, theorem 1.6]) to control the convex coset progression by a generalized arithmetic progression (up to acceptable losses, and increasing C_{PFR} by an epsilon), and then observe that in $\mathbf{F}_2^D$, all generalized arithmetic progressions are in fact subspaces. We leave the details of these arguments to the interested reader.

We have the following notorious conjecture, known as the Polynomial Freiman–Ruzsa conjecture over $\mathbf{F}_2$.

Conjecture 1.9. *We may take* $C_{\mathrm{PFR}} = 1$.

There are a large number of equivalent formulations of Conjecture 1.9; see [7,9,12,17]. We add a further equivalent form of Conjecture 1.9, formulated in terms of entropy. It says that, in the case $G = \mathbf{F}_2^D$, Proposition 1.3 is valid with no smallness restriction on the entropic distance $d_{\mathrm{ent}}(X, Y)$.

Proposition 1.10. *Conjecture 1.9 is equivalent to the claim that, for any* $\mathbf{F}_2^D$*-valued random variables* X, Y*, there is a finite subgroup* $H \leq \mathbf{F}_2^D$ *such that* $d_{\mathrm{ent}}(X, U_H) \ll d_{\mathrm{ent}}(X, Y)$.

1.2.4 | Small doubling and dimension, again

We now return to the main topic, and offer the following improvement of Theorem 1.8.

Theorem 1.11. *Suppose that* $A \subseteq \mathbf{Z}^D$ *is a finite set with* $\sigma[A] \leq K$*. Then there is* $A' \subseteq A$ *with* $\frac{|A'|}{|A|} \geq \exp(-C\log^{2-\frac{1}{C_{\mathrm{PFR}}}} K)$ *and* $\dim A' \ll \log K$.

We remark that the constant C is allowed to depend on C_{PFR} (and so by implication on the implied constant in the definition of C_{PFR}). As it turns out, the implied constant in the $\ll$ is independent of C_{PFR}, and in particular can be taken to be $40/\log 2$.

Thus, using the Konyagin/Sanders result we can obtain

$$\frac{|A'|}{|A|} \gg \exp(-C\log^{5/3+o(1)}K),$$

which is the strongest unconditional result currently known. Perhaps more interestingly, we obtain the following conditional implication between the two forms of the Polynomial Freiman–Ruzsa conjecture discussed above.

Corollary 1.12. *Conjecture* 1.9 *implies Conjecture* 1.7.

1.2.5 | Plan of the paper

We begin by developing the theory of entropy doubling and (entropy) Ruzsa distance, as discussed above. In Section 2 we establish Lemma 1.1. In Section 3, we look at the link between random variables and sets and establish Proposition 1.2. In Section 4 we look at homomorphisms and give the (short) proof of Proposition 1.4. Then, in Section 5, we combine these results to prove Proposition 1.3, which relates random variables with small entropy doubling to subgroups. This section is a little lengthy but, as we indicate at the appropriate points, not all of the analysis is needed in subsequent sections.

After this, we turn to the applications to small doubling in $\mathbf{Z}^D$. We begin, in Section 6, by proving Theorem 1.6 (and thus reproving Theorem 1.5). Then, we give a new proof of the result of the second author, Theorem 1.8.

Next, we take a brief detour into structural results over $\mathbf{F}_2$, establishing the equivalence of the Polynomial Freiman–Ruzsa conjecture in this setting with its entropic formulation (Proposition 1.10).

Finally, we return to small doubling in $\mathbf{Z}^D$, establishing Theorem 1.11 (and hence Corollary 1.12) in Section 9.

Finally, we remark that although we have written the paper in the context of an abelian group G, many of the arguments (e.g., the proof of Theorem 1.3) do not require this assumption.

2 | AN IMPROVED ENTROPIC RUZSA TRIANGLE INEQUALITY

In this section we prove Lemma 1.1.

Proof of Lemma 1.1. We begin with part (i). It suffices to show that

$$\mathbf{H}(X-Z) - \frac{1}{2}(\mathbf{H}(X)+\mathbf{H}(Z)) \leq d_{\mathrm{ent}}(X,Y) + d_{\mathrm{ent}}(Y,Z).$$

This is equivalent to establishing

$$\mathbf{H}(X-Z) \leq \mathbf{H}(X-Y) + \mathbf{H}(Y-Z) - \mathbf{H}(Y)$$

whenever Y is independent of (X,Z) (but X and Z are not required to be independent of each other).

We apply the submodularity inequality (A5) with $A = X-Y$, $B = Z$, $C = X-Z$. With these choices we have

$$\mathbf{H}(A,B,C) = \mathbf{H}(X,Y,Z) = \mathbf{H}(X,Z) + \mathbf{H}(Y),$$

$$\mathbf{H}(A,C) = \mathbf{H}(X-Y, X-Z) = \mathbf{H}(X-Y, Y-Z) \leq \mathbf{H}(X-Y) + \mathbf{H}(Y-Z)$$

and

$$\mathbf{H}(B,C) = \mathbf{H}(Z, X-Z) = \mathbf{H}(X,Z).$$

In the second display we used (A3). Applying (A5) gives part (i) of Lemma 1.1.

For part (ii), the first inequality $d_{\text{ent}}(X,Y) \leq d^*_{\text{ent}}(X,Y)$ is trivial. For the second inequality, we apply (i) and (1.3) to conclude that

$$\begin{aligned} d^*_{\text{ent}}(X,Y) &\leq d_{\text{ent}}(X,Y) + d_{\text{ent}}(Y,Y) \\ &\leq d_{\text{ent}}(X,Y) + d_{\text{ent}}(Y,X) + d_{\text{ent}}(X,Y), \end{aligned}$$

giving the claim. ∎

3 | FROM RANDOM VARIABLES TO SETS

The objective of this section is to prove Proposition 1.2. Let C, X, Y be as in that proposition. We may assume without loss of generality that X, Y are independent. For brevity we adopt the notation $k := d_{\text{ent}}(X,Y)$. We need to locate a set S satisfying (1.5) and (1.6). The key lemma is the following.

Lemma 3.1. *There exists a finite non-empty subset S of G such that*

$$\log|S| \geq \mathbf{H}(Y) - 2\text{h}\left(1 - \frac{2}{C}\right) - 4k \tag{3.1}$$

and such that

$$d^*_{\text{ent}}(Z,Y) \leq Ck + \frac{1}{2}\left(\mathbf{H}(Y) - \mathbf{H}(Z)\right) \tag{3.2}$$

whenever Z is an S-valued random variable.

Proof. As X, Y are independent and $k = d_{\text{ent}}(X,Y)$, we have

$$\mathbf{H}(X-Y) = \frac{1}{2}\mathbf{H}(X) + \frac{1}{2}\mathbf{H}(Y) + k, \tag{3.3}$$

and hence by (A14) it follows that

$$\mathbf{H}(X-Y) - \mathbf{H}(Y) \leq 2k.$$

Applying the equality case of (A18), we conclude that

$$\sum_x p_X(x) D_{KL}(x-Y \| X-Y) \leq 2k. \tag{3.4}$$

Inspired by this, we define S by the formula

$$S := \{x : p_X(x) > 0, D_{KL}(x-Y\|X-Y) \leq Ck\}. \tag{3.5}$$

Denote by A the random variable $A := 1_{X\in S}$, and write $p := \mathbf{P}(A = 1) = \mathbf{P}(X \in S)$. By Markov's inequality and (3.4), it follows that

$$p = \mathbf{P}(X \in S) \geq 1 - \frac{2}{C} \geq \frac{1}{2}. \tag{3.6}$$

Now we make some observations. First,

$$\begin{aligned} \mathbf{H}(X) &= \mathbf{H}(X, A) \\ &= \mathbf{H}(X|A) + \mathbf{H}(A) \\ &= p\mathbf{H}(X|A = 1) + (1 - p)\mathbf{H}(X|A = 0) + \mathrm{h}(p). \end{aligned} \tag{3.7}$$

Second, since Y is independent of X and A, it follows using (A13) that

$$\mathbf{H}(X - Y|A = i) \geq \mathbf{H}(Y), \mathbf{H}(X|A = i)$$

for $i = 0, 1$; therefore

$$\begin{aligned} \mathbf{H}(X - Y) &\geq \mathbf{H}(X - Y|A) \\ &= p\mathbf{H}(X - Y|A = 1) + (1 - p)\mathbf{H}(X - Y|A = 0) \\ &\geq p\mathbf{H}(Y) + \frac{1 - p}{2}\left(\mathbf{H}(Y) + \mathbf{H}(X|A = 0)\right). \end{aligned} \tag{3.8}$$

Combining (3.7), (3.8) with (3.3) we conclude after a short computation that

$$k \geq \frac{p}{2}\mathbf{H}(Y) - \frac{p}{2}\mathbf{H}(X|A = 1) - \frac{1}{2}\mathrm{h}(p). \tag{3.9}$$

By (A1), we have $\mathbf{H}(X|A = 1) \leq \log |S|$. Substituting into (3.9) and rearranging yields

$$\log |S| \geq \mathbf{H}(Y) - \frac{\mathrm{h}(p)}{p} - \frac{2k}{p}.$$

Using (3.6) (and the monotone decreasing nature of $\mathrm{h}(p)$ for $p \geq 1/2$), we obtain (3.1).

Now we prove (3.2). From (A18) (replacing X by $X - Y$ there) we have

$$\mathbf{H}(Z - Y) - \mathbf{H}(Y) \leq \sum_z p_Z(z) D_{KL}(z - Y \| X - Y).$$

Note here that the Kullback–Leibler divergence is well-defined and finite. Indeed, Z takes values $z \in S$, and hence by the definition of S we have $p_X(z) > 0$ for such z. Thus if $p_{z-Y}(t) > 0$ then $p_{X-Y}(t) = \sum_x p_X(x) p_{x-Y}(t) \geq p_X(z) p_{z-Y}(t) > 0$.

By definition of S, $D_{KL}(z - Y \| X - Y) \leq Ck$ for z in the range of Z, and the claim (3.2) follows. ∎

Now we are ready for the proof of Proposition 1.2 itself.

Proof of Proposition 1.2. We begin by establishing (1.5). Let S be as in Lemma 3.1. Taking $Z = U_S$ in (3.2), we have

$$d^*_{\mathrm{ent}}(U_S, Y) \leq Ck + \frac{1}{2}\left(\mathbf{H}(Y) - \log |S|\right).$$

The required bound (1.5) then follows from (3.1).

Now we prove (1.6). Let Z, Z' be any pair of S-valued random variables. From Lemma 1.1 (ii) and (3.2) we have

$$\begin{aligned} d^*_{\mathrm{ent}}(Z, Z') &\le d_{\mathrm{ent}}(Z, Y) + d_{\mathrm{ent}}(Z', Y) \\ &\le 2Ck + \mathbf{H}(Y) - \frac{1}{2}\mathbf{H}(Z) - \frac{1}{2}\mathbf{H}(Z') \end{aligned}$$

or equivalently

$$\mathbf{H}(Z - Z') \le 2Ck + \mathbf{H}(Y). \tag{3.10}$$

Now we observe that it is possible to choose Z, Z' supported on S so that $Z - Z'$ has the uniform distribution on $S - S$. To do this, simply take (Z, Z') to have distribution function

$$p_{(Z,Z')}(s_1, s_2) := \frac{1}{|S - S|\#\{(t_1, t_2) \in S : t_1 - t_2 = s_1 - s_2\}}$$

for $s_1, s_2 \in S$. In this case $\mathbf{H}(Z - Z') = \log |S - S|$. Using (3.10) and (3.1), (1.6) follows. ∎

Remark. The last part of this argument has considerable similarity with [16, sect. 5].

4 | ENTROPY DISTANCE UNDER HOMOMORPHISMS

In this section we establish Proposition 1.4. Let notation be as in the statement of that proposition.

Proof of Proposition 1.4. We have

$$\begin{aligned} &\mathbf{H}(X_1 - X_2 | Y_1, Y_2) \\ &\quad = \sum_{y_1, y_2 \in H} p_{Y_1}(y_1) p_{Y_2}(y_2) \mathbf{H}(X_1 - X_2 | Y_1 = y_1, Y_2 = y_2), \end{aligned} \tag{4.1}$$

$$\begin{aligned} \mathbf{H}(X_1 | Y_1) &= \sum_{y_1 \in H} p_{Y_1}(y_1) \mathbf{H}(X_1 | Y_1 = y_1) \\ &= \sum_{y_1, y_2 \in H} p_{Y_1}(y_1) p_{Y_2}(y_2) \mathbf{H}(X_1 | Y_1 = y_1), \end{aligned} \tag{4.2}$$

and similarly

$$\mathbf{H}(X_2 | Y_2) = \sum_{y_1, y_2 \in H} p_{Y_1}(y_1) p_{Y_2}(y_2) \mathbf{H}(X_2 | Y_2 = y_2). \tag{4.3}$$

Subtracting half of (4.2) and half of (4.3) from (4.1) gives

$$\begin{aligned} &\mathbf{H}(X_1 - X_2 | Y_1, Y_2) - \frac{1}{2}\mathbf{H}(X_1 | Y_1) - \frac{1}{2}\mathbf{H}(X_2 | Y_2) \\ &\quad = \sum_{y_1, y_2 \in H} p_{Y_1}(y_1) p_{Y_2}(y_2) d_{\mathrm{ent}}((X_1 | Y_1 = y_1), (X_2 | Y_2 = y_2)). \end{aligned} \tag{4.4}$$

Now X_i determines Y_i, and so

$$\mathbf{H}(X_1|Y_1) = \mathbf{H}(X_1) - \mathbf{H}(Y_1), \quad \mathbf{H}(X_2|Y_2) = \mathbf{H}(X_2) - \mathbf{H}(Y_2). \tag{4.5}$$

Moreover, by (A7),

$$\begin{aligned}\mathbf{H}(X_1 - X_2|Y_1, Y_2) &\le \mathbf{H}(X_1 - X_2|Y_1 - Y_2)\\ &= \mathbf{H}(X_1 - X_2) - \mathbf{H}(Y_1 - Y_2)\end{aligned} \tag{4.6}$$

(because $X_1 - X_2$ determines $Y_1 - Y_2$). Combining (4.4), (4.5), (4.6) gives the result. In fact one sees that the difference between the LHS and the RHS in the proposition is $\mathbf{H}(X_1 - X_2|Y_1 - Y_2) - \mathbf{H}(X_1 - X_2|Y_1, Y_2)$. ∎

5 | VERY SMALL ENTROPY DOUBLING

In this section we prove Proposition 1.3, which states that random variables X, Y for which $d_{\text{ent}}(X, Y)$ is small are close to uniform on a subgroup. We first handle the case $X = Y$ (in which case we will establish Proposition 1.3 with the improved constant of 6). Assume henceforth that X is a G-valued random variable with $d_{\text{ent}}(X, X) = \varepsilon \le \varepsilon_0$.

We first observe that a weak version of Proposition 1.3 (which in fact suffices for many applications) follows quickly from Proposition 1.2. As observed in item (ii) after Proposition 1.2, we see that there is S such that

$$d_{\text{ent}}(U_S, Y) \ll \varepsilon^{1/2} \log \frac{1}{\varepsilon} \tag{5.1}$$

and

$$|S - S| \le \left(1 + O\left(\varepsilon^{1/2} \log \frac{1}{\varepsilon}\right)\right)|S| < \frac{3}{2}|S|, \tag{5.2}$$

where the last inequality holds if ε_0 is small enough. A well-known classical observation of Freiman [5] now implies that $H := S - S$ is a group. We recall the short proof here.

For any $x, y \in S$, $x - S$ and $y - S$ both lie in $S - S$ and so $|(x - S) \cap (y - S)| > \frac{1}{2}|S|$. That is, there are $> \frac{1}{2}|S|$ pairs $(u, v) \in S \times S$ such that $x - u = y - v$. For each such pair, we have $x - y = u - v$. Now let $x', y' \in S$ be any other elements. Similarly, there are $> \frac{1}{2}|S|$ pairs $(u', v') \in S \times S$ such that $x' - y' = u' - v'$. There are $> \frac{1}{2}|S|$ values of v and $> \frac{1}{2}|S|$ values of u', and all these values lie in S; therefore we must have $v = u'$ for some pair of these elements. It then follows that $(x - y) + (x' - y') = (u - v) + (u' - v') = u - v' \in S - S$. Since x, y, x', y' were arbitrary, it follows that $S - S$ is closed under addition. Since it contains 0 and is closed under taking inverses, it must be a group.

From (A16) (noting that S is contained in a single coset of H) and (5.2) we have

$$d_{\text{ent}}(U_H, U_S) = \frac{1}{2} \log \frac{|H|}{|S|} \ll \varepsilon^{1/2} \log \frac{1}{\varepsilon}.$$

Therefore from (5.1) and (1.3) we have

$$d_{\text{ent}}(U_H, Y) \ll \varepsilon^{1/2} \log \frac{1}{\varepsilon}. \tag{5.3}$$

This is weaker than Proposition 1.3 only in the non-linear dependency on ϵ, which in many applications is not important.

We will deduce the stronger statement of Proposition 1.3 by bootstrapping this bound. To do this, we require two lemmas which are essentially special cases of Proposition 1.3 itself. First, we consider the case in which X is highly concentrated near one point.

Lemma 5.1. *There is $\delta_0 > 0$ such that the following is true. Suppose that X is a G-valued random variable and $x_0 \in G$ is a value such that $\mathbf{P}(X = x_0) \geq 1 - \delta_0$. Then $\mathbf{H}(X) \leq 2d_{\mathrm{ent}}(X, X)$.*

Proof. By replacing X by $X - x_0$ if necessary, we may assume without loss of generality that $x_0 = 0$. Let X_1, X_2 be independent copies of X. Then our task is equivalent to showing that

$$\mathbf{H}(X_1 - X_2) \geq \frac{3}{2}\mathbf{H}(X). \tag{5.4}$$

Write $p := \mathbf{P}(X \neq 0)$ (thus $p \leq \delta_0$), and let A denote the indicator function of the event that $X_1, X_2 \neq 0$; then $\mathbf{P}(A = 0) = 1 - p^2$ and $\mathbf{P}(A = 1) = p^2$. As a consequence, we have

$$\begin{aligned} \mathbf{H}(X_1 - X_2) &\geq \mathbf{H}(X_1 - X_2|A) \\ &= (1 - p^2)\mathbf{H}(X_1 - X_2|A = 0) + p^2\mathbf{H}(X_1 - X_2|X_1, X_2 \neq 0) \\ &\geq (1 - p^2)\mathbf{H}(X_1 - X_2|A = 0) + p^2\mathbf{H}(X|X \neq 0) \end{aligned} \tag{5.5}$$

where we used (A13) in the last line.

Now note that for any z, if $A = 0$ and $X_1 - X_2 = z$ then (X_1, X_2) can take only two values $(z, 0)$ and $(0, -z)$ if $z \neq 0$, and only one value $(0, 0)$ if $z = 0$. Hence

$$\begin{aligned} \mathbf{H}(X_1, X_2|A = 0) - \mathbf{H}(X_1 - X_2|A = 0) &= \mathbf{H}(X_1, X_2|X_1 - X_2, A = 0) \\ &\leq \mathbf{P}(X_1 - X_2 \neq 0|A = 0)\log 2 = \frac{2p(1-p)}{1-p^2}\log 2. \end{aligned}$$

Combining with (5.5), we obtain

$$\begin{aligned} \mathbf{H}(X_1 - X_2) \geq (1 - p^2)\mathbf{H}(X_1, X_2|A = 0) \\ + p^2\mathbf{H}(X|X \neq 0) - 2p(1 - p)\log 2. \end{aligned} \tag{5.6}$$

We also observe that

$$\begin{aligned} 2\mathbf{H}(X) = \mathbf{H}(X_1, X_2) = \mathbf{H}(X_1, X_2, A) &= \mathbf{H}(X_1, X_2|A) + \mathbf{H}(A) \\ &= (1 - p^2)\mathbf{H}(X_1, X_2|A = 0) + p^2\mathbf{H}(X_1, X_2|A = 1) + \mathrm{h}(p^2) \\ &= (1 - p^2)\mathbf{H}(X_1, X_2|A = 0) + 2p^2\mathbf{H}(X|X \neq 0) + \mathrm{h}(p^2). \end{aligned} \tag{5.7}$$

We further note that, writing I for the indicator of $X \neq 0$,

$$\mathbf{H}(X) = \mathbf{H}(X|I) + \mathbf{H}(I) = p\mathbf{H}(X|X \neq 0) + \mathrm{h}(p). \tag{5.8}$$

Taking (5.7) minus p times (5.8) gives

$$(2-p)\mathbf{H}(X) = (1-p^2)\mathbf{H}(X_1, X_2|A=0)+ \\ + p^2\mathbf{H}(X|X\neq 0) + \mathrm{h}(p^2) - p\mathrm{h}(p).$$

Combining this with (5.6), we obtain

$$\mathbf{H}(X_1 - X_2) \geq (2-p)\mathbf{H}(X) + p\mathrm{h}(p) - 2p(1-p)\log 2 - \mathrm{h}(p^2). \tag{5.9}$$

Recall that our aim is to demonstrate (5.4). To get this from (5.9), we first note that expansion to leading order gives

$$2p(1-p)\log 2 + \mathrm{h}(p^2) \leq \left(\frac{1}{2} - p\right)\mathrm{h}(p) \tag{5.10}$$

provided δ_0 is small enough: the LHS here is $\sim 2p\log 2$, whilst the right hand side is $\sim \frac{1}{2}p\log\frac{1}{p}$. (A more careful analysis shows that $\delta_0 = \frac{1}{20}$ is sufficient.) We also have

$$\mathrm{h}(p) = \mathbf{H}(I) \leq \mathbf{H}(X). \tag{5.11}$$

The desired bound (5.4) then follows immediately from (5.9), (5.10) and (5.11). ∎

Remark. The constant 2 in the statement of Lemma 5.1 can be replaced by anything larger than 1, at the expense of making δ_0 smaller. This may be shown with very minor modifications of the above argument.

We next consider the case of a random variable supported on H.

Lemma 5.2. *Suppose that X is an H-valued random variable with $\mathbf{H}(X) \geq \log|H| - \frac{1}{8}$. Then*

$$\log|H| - \mathbf{H}(X) \leq 2d_{\mathrm{ent}}(X, X).$$

To prove this we will use the following lemma concerning couplings of almost uniform random variables, which is plausibly of independent interest. Here, for a probability distribution p on a group H, we write $\|p - u_H\|_1 := \sum_{x\in H}\left|p(x) - \frac{1}{|H|}\right|$ for the ℓ^1-distance of p from the uniform distribution (or, equivalently, twice the total variation distance of p from the uniform distribution).

Lemma 5.3. *Suppose $p_1, p_2, p_3 : H \to \mathbf{R}_{\geq 0}$ are three probability distributions on H such that*

$$\|p_1 - u_H\|_1 + \|p_2 - u_H\|_1 + \|p_3 - u_H\|_1 \leq 1. \tag{5.12}$$

Then there exists a pair of random variables (X, Y) on H (not necessarily independent) having the marginal distributions $p_X = p_1$, $p_Y = p_2$ and $p_{X-Y} = p_3$.

Proof. We wish to show that the triple of distributions $(p_1, p_2, p_3) \in \mathbf{R}^H \times \mathbf{R}^H \times \mathbf{R}^H$ lies in the convex hull of the set $\Sigma := \{(\delta_x, \delta_y, \delta_{x-y}) : x, y \in H\} \subseteq \mathbf{R}^H \times \mathbf{R}^H \times \mathbf{R}^H$. Here (as usual) $\delta_t(u) = 1$ if $u = t$, and $\delta_t(u) = 0$ otherwise. By the (finite-dimensional) Hahn–Banach theorem, this is equivalent to showing that there is no hyperplane separating (p_1, p_2, p_3) from Σ, or in other words whenever $f_1, f_2, f_3 : H \to \mathbf{R}$ are functions such that

$$f_1(x)+f_2(y)+f_3(x-y)\geq 0 \tag{5.13}$$

for all $x,y\in H$, one also has

$$\sum_{x\in H} f_1(x)p_1(x)+\sum_{y\in H} f_2(y)p_2(y)+\sum_{z\in H} f_3(z)p_3(z)\geq 0. \tag{5.14}$$

Henceforth, assume (5.13). Note that (5.13) and (5.14) are both unaffected if we shift f_1,f_2,f_3 by constants c_1,c_2,c_3 summing to zero. Thus we may normalize so that

$$\min f_1=\min f_2=\min f_3.$$

If this quantity is non-negative then (5.14) is immediate, so we may assume that it is negative. By rescaling we may thus normalize so that

$$\min f_1=\min f_2=\min f_3=-1. \tag{5.15}$$

In particular, there exists $x_0\in H$ such that $f_1(x_0)=-1$. From (5.13) and (5.15), we conclude that for every $y\in H$ one has

$$f_2(y)+f_3(x_0-y)\geq 1 \quad \text{and} \quad \min(f_2(y),f_3(x_0-y))\geq -1.$$

This implies that

$$\begin{aligned}
&f_2(y)p_2(y)+f_3(x_0-y)p_3(x_0-y)\\
&\quad\geq (f_2(y)+f_3(x_0-y))\min(p_2(y),p_3(x_0-y))\\
&\qquad+\min(f_2(y),f_3(x_0-y))|p_2(y)-p_3(x_0-y)|\\
&\quad\geq \min(p_2(y),p_3(x_0-y))-|p_2(y)-p_3(x_0-y)|\\
&\quad=\frac{p_2(y)+p_3(x_0-y)}{2}-\frac{3}{2}\left|p_2(y)-p_3(x_0-y)\right|\\
&\quad\geq \frac{p_2(y)+p_3(x_0-y)}{2}-\frac{3}{2}\left|p_2(y)-\frac{1}{|H|}\right|-\frac{3}{2}\left|p_3(x_0-y)-\frac{1}{|H|}\right|.
\end{aligned}$$

Summing over y, we conclude that

$$\sum_{y\in H} f_2(y)p_2(y)+\sum_{z\in H} f_3(z)p_3(z)\geq 1-\frac{3}{2}\|p_2-u_H\|_1-\frac{3}{2}\|p_3-u_H\|_1.$$

Cyclically permuting the roles of f_1,f_2,f_3 and p_1,p_2,p_3 and averaging, the desired bound (5.14) then follows from (5.12). ∎

Proof of Lemma 5.2. By (A10) and Pinsker's inequality (A12) it follows that

$$\|p_X-u_H\|_1\leq\sqrt{2(\log|H|-\mathbf{H}(X))}\leq\frac{1}{2}. \tag{5.16}$$

Applying Lemma 5.3 (with $p_1=p_2=p_X$ and $p_3=\frac{1}{|H|}$), it follows that there exists a pair of random variables (X_1,X_2) such that X_1,X_2 each have the same marginal distribution as X, and X_1-X_2 is uniform on H.

Finally, Lemma 1.1 gives

$$\begin{aligned}\log|H| = \mathbf{H}(X_1 - X_2) &\leq \mathbf{H}(X) + d^*_{\mathrm{ent}}(X, X)\\ &\leq \mathbf{H}(X) + d_{\mathrm{ent}}(X, X) + d_{\mathrm{ent}}(X, X),\end{aligned}$$

which immediately implies the result. ∎

Proof of Proposition 1.3. We first establish the case $X = Y$ (with the constant 12 replaced by 6). Suppose, as we have throughout the section, that $d_{\mathrm{ent}}(X, X) = \varepsilon \leq \varepsilon_0$. Let $\pi : G \to G/H$ be the quotient projection. Recall from (A16) that

$$d_{\mathrm{ent}}(X, U_H) = \mathbf{H}(\pi(X)) + \frac{1}{2}\left(\log|H| - \mathbf{H}(X)\right). \tag{5.17}$$

From (5.3) we have the weak bound $d_{\mathrm{ent}}(X, U_H) \ll \varepsilon^{1/2}\log\frac{1}{\varepsilon}$. Thus

$$\mathbf{H}(\pi(X)) \ll \varepsilon^{1/2}\log\frac{1}{\varepsilon} \tag{5.18}$$

and

$$\mathbf{H}(X) \geq \log|H| - O\left(\varepsilon^{1/2}\log\frac{1}{\varepsilon}\right). \tag{5.19}$$

Now by Proposition 1.4 (replacing H there by G/H, and recalling that $d_{\mathrm{ent}}(X, X) = \varepsilon$) we obtain

$$d_{\mathrm{ent}}\left(\pi(X), \pi(X)\right) \leq \varepsilon \tag{5.20}$$

and

$$\sum_{y_1, y_2 \in G/H} p_{\pi(X)}(y_1)p_{\pi(X)}(y_2)d_{\mathrm{ent}}(X_{y_1}, X_{y_2}) \leq \varepsilon, \tag{5.21}$$

where X_y denotes X conditioned to the event $\pi(X) = y$.

By (5.18) and (A2), we see that there is some $y_0 \in G/H$ such that $\mathbf{P}(\pi(X) = y_0) \geq 1 - O\left(\varepsilon^{1/2}\log\frac{1}{\varepsilon}\right)$. By translating X if necessary, we may assume without loss of generality that $y_0 = 0$, that is to say

$$p_{\pi(X)}(0) = \mathbf{P}(X \in H) \geq 1 - O\Big(\varepsilon^{1/2}\log\frac{1}{\varepsilon}\Big) \geq \max\Big(\frac{10}{11}, 1 - \delta_0\Big) \tag{5.22}$$

where δ_0 is the constant from Lemma 5.1, and we assume that ε_0 from the statement of Proposition 1.3 is sufficiently small.

Applying Lemma 5.1 to $\pi(X)$ using (5.20), (5.22), we conclude that

$$\mathbf{H}(\pi(X)) \leq 2\varepsilon. \tag{5.23}$$

Meanwhile, discarding all terms in the sum over y_1 in (5.21) except the term $y_1 = 0$, and using (5.22), it follows that

$$\sum_{y \in G/H} p_{\pi(X)}(y)d_{\mathrm{ent}}(X_0, X_y) \leq 1.1\varepsilon.$$

By (A14), this implies that

$$\sum_{y\in G/H} p_{\pi(X)}(y)\big|\mathbf{H}(X_y)-\mathbf{H}(X_0)\big| \le 2.2\varepsilon,$$

and hence by the triangle inequality

$$\Big|\mathbf{H}(X|\pi(X))-\mathbf{H}(X_0)\Big| \le 2.2\varepsilon.$$

Using $\mathbf{H}(X)=\mathbf{H}(X|\pi(X))+\mathbf{H}(\pi(X))$ and (5.23), we conclude that

$$|\mathbf{H}(X)-\mathbf{H}(X_0)| \le 4.2\varepsilon. \tag{5.24}$$

In particular, from (5.19) we deduce

$$\mathbf{H}(X_0) \ge \log|H| - O\Big(\varepsilon^{1/2}\log\frac{1}{\varepsilon}\Big). \tag{5.25}$$

Now by discarding all terms in (5.21) except the one with $y_1 = y_2 = 0$, and using (5.22), we have

$$d_{\mathrm{ent}}(X_0,X_0) \le 1.21\varepsilon.$$

It follows from Lemma 5.2 that $\mathbf{H}(X_0)\ge \log|H|-2.42\varepsilon$, and hence by (5.24) we obtain

$$\mathbf{H}(X) \ge \log|H| - 6.62\varepsilon.$$

Combining this with (5.17) and (5.23) gives $d_{\mathrm{ent}}(X,U_H) \le 5.31\varepsilon \le 6\varepsilon$, which is the statement of Proposition 1.3 (with a better constant) in the symmetric case $X=Y$.

Finally, we deduce the general case in which X and Y may be different. Suppose now that $d_{\mathrm{ent}}(X,Y)=\varepsilon\le\varepsilon_0'$, where $\varepsilon_0' := \varepsilon_0/2$ with ε_0 the constant above. By the triangle inequality, $d_{\mathrm{ent}}(X,X)\le 2\varepsilon\le\varepsilon_0$, and so by the symmetric case of Proposition 1.3 established above we have $d_{\mathrm{ent}}(X,U_H)\le 12\varepsilon$ for some subgroup $H\le G$. Similarly, we have $d_{\mathrm{ent}}(Y,U_{H'})\le 12\varepsilon$ for some subgroup $H'\le G$.

It remains to argue that $H=H'$. For this, we observe that by the triangle inequality we have

$$d(U_H,U_{H'}) \le 25\varepsilon. \tag{5.26}$$

If $H\ne H'$, then $H+H'$ is a subgroup of G properly containing H,H' and therefore of size at least $2\max(|H|,|H'|)$. Since $U_H-U_{H'}$ is uniform on $H+H'$, we have $d(U_H,U_{H'})\ge\log 2$, which contradicts (5.26) if ε_0 is small enough. Therefore we do indeed have $H=H'$, and this concludes the proof. ∎

6 | SKEW DIMENSION AND A RESULT OF PÁLVÖLGYI AND ZHELEZOV

In this section we give the proof of Theorem 1.6 (and thus Theorem 1.5).

Proof of Theorem 1.6. Let $\varepsilon>0$ be a small constant to be specified later, and set $C := 2/\varepsilon$. We will prove Theorem 1.6 with this particular value of C.

We proceed by induction on $|A||B|$ and on D. Denote by $\pi : \mathbf{Z}^D \to \mathbf{Z}$ projection onto the first coordinate. We may assume that at least one of the sets $\pi(A), \pi(B)$ is not a singleton (otherwise D may be reduced to $D-1$).

Let X_1, X_2 be uniform random variables on A, B respectively, and let $Y_i = \pi(X_i)$. Applying Proposition 1.4 and rearranging, we obtain

$$\sum_{i,j} p_{Y_1}(i)p_{Y_2}(j) \log \frac{K}{K_{i,j}} \geq d_{\mathrm{ent}}(Y_1, Y_2) \tag{6.1}$$

where

$$K := \exp\left(d_{\mathrm{ent}}(X_1, X_2)\right)$$

and

$$K_{i,j} := \exp\left(d_{\mathrm{ent}}((X_1|Y_1 = i), (X_2|Y_2 = j))\right).$$

We now divide into two cases, according to whether $d_{\mathrm{ent}}(Y_1, Y_2) \leq \varepsilon$ or not.

Case 1: $d_{\mathrm{ent}}(Y_1, Y_2) \leq \varepsilon$. Let ε_0 be the constant from Proposition 1.3, and assume that $\varepsilon \leq \min\left(\varepsilon_0, \frac{1}{24}\right)$. By Proposition 1.3 and the fact that $H = \{0\}$ is the only finite subgroup of $\mathbf{Z}$, we have

$$d_{\mathrm{ent}}(Y_1, 0), d_{\mathrm{ent}}(Y_2, 0) \leq 12 d_{\mathrm{ent}}(Y_1, Y_2).$$

Since $d_{\mathrm{ent}}(Y_i, 0) = \frac{1}{2}\mathbf{H}(Y_i)$, it follows that

$$\mathbf{H}(Y_1) + \mathbf{H}(Y_2) \leq 48 d_{\mathrm{ent}}(Y_1, Y_2) \leq C d_{\mathrm{ent}}(Y_1, Y_2) \tag{6.2}$$

by the choice of C, ε. Inserting this into (6.1) and rearranging, we obtain

$$\sum_{i,j} p_{Y_1}(i)p_{Y_2}(j) \log\left(\frac{K_{i,j}}{K(p_{Y_1}(i)p_{Y_2}(j))^{1/C}}\right) \leq 0.$$

In particular, there exist i, j such that

$$K_{i,j} \leq K(p_{Y_1}(i)p_{Y_2}(j))^{1/C} \leq K.$$

Invoking the induction hypothesis (with A, B replaced by $A \cap \pi^{-1}(\{i\})$ and $B \cap \pi^{-1}(\{j\})$ respectively), we see that there are sets $A' \subseteq A, B' \subseteq B$ with

$$\dim_* A', \dim_* B' \leq C \log K_{i,j} \leq C \log K$$

and

$$\begin{aligned} |A'||B'| &\geq K_{i,j}^{-C} |A \cap \pi^{-1}(\{i\})||B \cap \pi^{-1}(\{j\})| = K_{i,j}^{-C} p_{Y_1}(i)p_{Y_2}(j)|A||B| \\ &\geq K_{i,j}^{-C} \left(\frac{K_{i,j}}{K}\right)^C |A||B| = K^{-C}|A||B|. \end{aligned}$$

This closes the induction in Case 1.

Case 2: $d_{\text{ent}}(Y_1, Y_2) \geq \varepsilon$.

In this case we see from (6.1) that

$$\sum_{i,j} p_{Y_1}(i) p_{Y_2}(j) \log \frac{K}{K_{i,j}} \geq \varepsilon.$$

The contribution from those (i,j) with $\log \frac{K}{K_{i,j}} \leq \frac{\varepsilon}{2}$ is at most $\frac{\varepsilon}{2}$. Thus if we set

$$S := \left\{ (i,j) : \log \frac{K}{K_{i,j}} > \frac{\varepsilon}{2} \right\}$$

then

$$\sum_{(i,j)\in S} p_{Y_1}(i) p_{Y_2}(j) \log \frac{K}{K_{i,j}} \geq \frac{\varepsilon}{2}. \tag{6.3}$$

Note in particular that, if $(i,j) \in S$,

$$K_{i,j} < K. \tag{6.4}$$

By the induction hypothesis, for each pair $(i,j) \in S$ there are sets $A'_{i,j} \subseteq A$, $B'_{i,j} \subseteq B$ with

$$|A'_{i,j}||B'_{i,j}| \geq K_{i,j}^{-C} p_{Y_1}(i) p_{Y_2}(j) |A||B|, \tag{6.5}$$

and all with skew-dimension at most

$$C \log K_{i,j} \leq C\left(\log K - \frac{\varepsilon}{2}\right) = C \log K - 1. \tag{6.6}$$

(Here we used the fact that $C = 2/\varepsilon$.)

For each $i \in \mathbf{Z}$, set A'_i to be the largest of the sets $A'_{i,j}$, $(i,j) \in S$ (or $A'_i = \emptyset$ if $(i,j) \notin S$ for every j), and similarly for each $j \in \mathbf{Z}$ set B'_j to be the largest of the sets $B'_{i,j}$, $(i,j) \in S$, breaking ties arbitrarily. Finally, set $A' := \bigcup_{i\in\mathbf{Z}} A'_i$ and $B' := \bigcup_{j\in\mathbf{Z}} B'_j$. By the definition of skew-dimension and the bound (6.6), we have $\dim_* A', \dim_* B' \leq C \log K$.

From the elementary inequality $t \geq \log t$ for $t \geq 1$ applied to $t = (K/K_{i,j})^C$ (noting by (6.4) that we do indeed have $t \geq 1$), we have

$$K_{i,j}^{-C} \geq CK^{-C} \log \frac{K}{K_{i,j}}$$

for any $(i,j) \in S$. From this and (6.5), (6.3) we have

$$\begin{aligned}
|A'||B'| &= \sum_{(i,j)\in\mathbf{Z}^2} |A'_i||B'_j| \\
&\geq \sum_{(i,j)\in S} |A'_{i,j}||B'_{i,j}| \\
&\geq |A||B| \sum_{(i,j)\in S} K_{i,j}^{-C} p_{Y_1}(i) p_{Y_2}(j) \\
&\geq |A||B| \sum_{(i,j)\in S} \left(CK^{-C} \log \frac{K}{K_{i,j}} \right) p_{Y_1}(i) p_{Y_2}(j) \\
&\geq \frac{C\varepsilon}{2} K^{-C} |A||B| = K^{-C} |A||B|.
\end{aligned}$$

This completes the induction, and the theorem is proved. ∎

7 | DIMENSION AND A RESULT OF THE SECOND AUTHOR

We turn now to the question of the dimension (as opposed to the weaker skew-dimension) of subsets of $\mathbf{Z}^D$ with small doubling. Our aim in this section is to give an entropic proof of Theorem 1.8. In so doing, we will also lay the groundwork for the proof of Theorem 1.11, our improvement upon this result.

As in [14, slogan 2.5], a key idea is that a set $A \subseteq \mathbf{Z}^D$ with small doubling must look rather singular under the projection map $\phi : \mathbf{Z}^D \to \mathbf{F}_2^D$. In Lemma 7.2 below, we give an entropic formulation of this principle. We isolate the following lemma from the proof.

Lemma 7.1. *Let G be torsion-free, and let X, Y be G-valued random variables. Then $d_{\mathrm{ent}}(X, 2Y) \leq 5d_{\mathrm{ent}}(X, Y)$.*

Proof. We assume X, Y are independent. Then[2]

$$\begin{aligned} \mathbf{H}(X - 2Y) &= \mathbf{H}((X - Y) - Y) \\ &\leq d^*_{\mathrm{ent}}(X - Y, Y) + \frac{1}{2}\mathbf{H}(X - Y) + \frac{1}{2}\mathbf{H}(Y) \end{aligned} \tag{7.1}$$

by definition of d^*_{ent}. By Lemma 1.1,

$$\begin{aligned} d^*_{\mathrm{ent}}(X - Y, Y) &\leq d_{\mathrm{ent}}(Y, Y) + d_{\mathrm{ent}}(X - Y, Y) \\ &\leq 2d_{\mathrm{ent}}(X, Y) + d_{\mathrm{ent}}(X - Y, Y). \end{aligned} \tag{7.2}$$

Letting Y_1, Y_2 be independent copies of Y (which are also independent of X) we have

$$d_{\mathrm{ent}}(X - Y, Y) = \mathbf{H}(X - Y_1 - Y_2) - \frac{1}{2}\mathbf{H}(X - Y) - \frac{1}{2}\mathbf{H}(Y). \tag{7.3}$$

Writing $A := Y_1$, $B := Y_2$ and $C := X - Y_1 - Y_2$, we have

$$\mathbf{H}(A, B, C) = \mathbf{H}(X, Y_1, Y_2) = \mathbf{H}(X) + 2\mathbf{H}(Y),$$

and

$$\mathbf{H}(A, C) = \mathbf{H}(A, C + A) = \mathbf{H}(Y_1, X - Y_2) = \mathbf{H}(Y) + \mathbf{H}(X - Y_2),$$

$$\mathbf{H}(B, C) = \mathbf{H}(B, C + B) = \mathbf{H}(Y_2, X - Y_1) = \mathbf{H}(Y) + \mathbf{H}(X - Y_1)$$

so applying the submodularity inequality (A5) gives

$$\mathbf{H}(X - Y_1 - Y_2) \leq \mathbf{H}(X - Y_1) + \mathbf{H}(X - Y_2) - \mathbf{H}(X).$$

Combining this with (7.3) gives

$$d_{\mathrm{ent}}(X - Y, Y) \leq \frac{3}{2}\mathbf{H}(X - Y) - \mathbf{H}(X) - \frac{1}{2}\mathbf{H}(Y)$$

[2]The use of d^*_{ent} here simplifies an earlier version of the argument, and was suggested to the authors by Noah Kravitz.

which, together with (7.1) and (7.2), yields

$$\mathbf{H}(X-2Y) \leq 2d_{\mathrm{ent}}(X,Y) + 2\mathbf{H}(X-Y) - \mathbf{H}(X) = 4d_{\mathrm{ent}}(X,Y) + \mathbf{H}(Y)$$

and so

$$d_{\mathrm{ent}}(X,2Y) \leq 4d_{\mathrm{ent}}(X,Y) + \frac{1}{2}(\mathbf{H}(Y) - \mathbf{H}(X)) \leq 5d_{\mathrm{ent}}(X,Y)$$

where we used (A14) in the last step. ∎

Lemma 7.2. *Let X, Y be $\mathbf{Z}^D$-valued random variables for some $D \geq 0$. Denote by $\phi : \mathbf{Z}^D \to \mathbf{F}_2^D$ the natural homomorphism. Then*

$$\mathbf{H}(\phi(X)), \mathbf{H}(\phi(Y)) \leq 10d_{\mathrm{ent}}(X,Y).$$

Proof. By Proposition 1.4 and Lemma 7.1,

$$d_{\mathrm{ent}}(\phi(X), \phi(2Y)) \leq d_{\mathrm{ent}}(X,2Y) \leq 5d_{\mathrm{ent}}(X,Y). \tag{7.4}$$

However, $\phi(2Y)$ is identically zero and so

$$d_{\mathrm{ent}}(\phi(X), \phi(2Y)) = d_{\mathrm{ent}}(\phi(X), 0) = \frac{1}{2}\mathbf{H}(\phi(X)).$$

Combining this with (7.4) gives the stated bound for $\mathbf{H}(\phi(X))$. The bound for $\mathbf{H}(\phi(Y))$ follows in the same way. ∎

Remark. It is perhaps worth remarking on the meaning and proof of this statement. Supposing that $A \subset \mathbf{Z}^D$ is a set with small (combinatorial) doubling K, it follows that the dilate $2 \cdot A$, which is contained in $A + A$, is commensurate (up to polynomial factors in K) with A. Projecting mod 2, one therefore expects the projection $\pi(A)$ to be commensurate with the projection $\pi(2 \cdot A) = \{0\}$. A version of this argument appears in [14, appendix B]. In the entropy setting, Lemma 7.1 acts as a replacement for the trivial observation that $2 \cdot A$ is contained in $A + A$.

Now we are ready for the proof of Theorem 1.8 itself. To make the argument work, we will in fact need to establish the following bipartite variant of the result.

Theorem 7.3. *There is an absolute constant C_1 such that, setting $f(t) := C_1 t(1+t)$, the following is true. Let $D \in \mathbf{N}$, and suppose that $A, B \subseteq \mathbf{Z}^D$ are finite non-empty sets. Then there exist nonempty $A' \subseteq A$, $B' \subseteq B$ with*

$$\log \frac{|A|}{|A'|} + \log \frac{|B|}{|B'|} \leq f\left(d_{\mathrm{ent}}(U_A, U_B)\right) \tag{7.5}$$

and such that $\dim A', \dim B' \leq C_1 d_{\mathrm{ent}}(U_A, U_B)$.

It is clear from (1.1) that this indeed implies Theorem 1.8.

We first prove a simple lemma which will be used several times in what follows.

Lemma 7.4. *Let $\phi : G \to H$ be a homomorphism, and $A, B \subseteq G$ finite subsets. For $x, y \in H$ write $A_x = A \cap \phi^{-1}(x)$ and $B_y = B \cap \phi^{-1}(y)$ for the fibres of A and B, and write $\alpha_x := \frac{|A_x|}{|A|}$ and $\beta_y := \frac{|B_y|}{|B|}$. Write $k = d_{\mathrm{ent}}(U_A, U_B)$, $\overline{k} = d_{\mathrm{ent}}(\phi(U_A), \phi(U_B))$ and $M = \mathbf{H}(\phi(U_A)) + \mathbf{H}(\phi(U_B))$. Then there exist $x, y \in H$ such that A_x, B_y are non-empty and with*

$$\bar{k} \log \frac{1}{\alpha_x \beta_y} \leq M \left(k - d_{\text{ent}}(U_{A_x}, U_{B_y}) \right). \tag{7.6}$$

Proof. First observe that the random variables $(U_A|\phi(U_A) = x)$ and $(U_B|\phi(U_B) = y)$ are equal in distribution to U_{A_x}, U_{B_y} respectively, that is to say the uniform distributions on the fibres. It follows from Proposition 1.4 that

$$\sum_{x,y \in H} \alpha_x \beta_y d_{\text{ent}}(U_{A_x}, U_{B_y}) \leq k - \bar{k}. \tag{7.7}$$

By definition, $M = \sum_{x,y} \alpha_x \beta_y \log \frac{1}{\alpha_x \beta_y}$ and hence

$$\sum_{x,y \in H} \alpha_x \beta_y \left(M d_{\text{ent}}(U_{A_x}, U_{B_y}) + \bar{k} \log \frac{1}{\alpha_x \beta_y} \right) \leq Mk.$$

It follows by the pigeonhole principle that there is at least one choice of x, y such that $\alpha_x, \beta_y > 0$ and

$$M d_{\text{ent}}(U_{A_x}, U_{B_y}) + \bar{k} \log \frac{1}{\alpha_x \beta_y} \leq Mk.$$

Rearranging gives (7.6). ∎

We now turn to the proof of Theorem 7.3.

Proof of Theorem 7.3. Let us begin by noting the simple inequality

$$\begin{aligned} f(b) &= C_1 b(1+b) \\ &\leq C_1 b(1+a) = f(a) - C_1(a-b)(1+a) \end{aligned} \tag{7.8}$$

for all $a, b \in \mathbf{R}$ with $0 \leq b \leq a$.

Let us turn now to the main proof. We will proceed by induction on $|A| + |B|$. We may also assume that A, B do not sit inside cosets of a proper subgroup of $\mathbf{Z}^D$, else we may replace $\mathbf{Z}^D$ by that subgroup. We also suppose $D \geq 1$, as the result is trivial otherwise.

Let $\phi : \mathbf{Z}^D \to \mathbf{F}_2^D$ be the natural homomorphism. Then, by the preceding remark and the fact that $\ker \phi$ is a proper subgroup of $\mathbf{Z}^D$, we may assume that at least one of $\phi(A), \phi(B)$ is not a singleton. For $x, y \in \mathbf{F}_2^D$, denote by $A_x := A \cap \phi^{-1}(x)$ and $B_y := B \cap \phi^{-1}(y)$ the fibres of A, B. Note that

$$|A_x| + |B_y| < |A| + |B| \tag{7.9}$$

for all x, y.

Write $k := d_{\text{ent}}(U_A, U_B)$ and $\varepsilon := d_{\text{ent}}(\phi(U_A), \phi(U_B))$. Let $\delta > 0$ be a small positive constant to be determined later, and set $C_1 := \max(20/\delta, 100)$. We will divide into two cases, according to whether or not $\varepsilon \leq \delta$.

Case 1: $\varepsilon > \delta$. By Lemma 7.2 with $X = U_A$, $Y = U_B$, we have

$$\mathbf{H}(\phi(U_A)) + \mathbf{H}(\phi(U_B)) \leq 20k. \tag{7.10}$$

By Lemma 7.4 applied to $G = \mathbf{Z}^D$ and $H = \mathbf{F}_2^D$, we may find $x, y \in \mathbf{F}_2^D$ such that (7.6) holds. Fix such x, y, and for brevity set $k' := d_{\mathrm{ent}}(U_{A_x}, U_{B_y})$. Then (7.6) implies that $k' \le k$ and

$$\log \frac{|A|}{|A_x|} + \log \frac{|B|}{|B_y|} \le \frac{20k}{\varepsilon}(k - k'). \tag{7.11}$$

Noting (7.9), we may apply the induction hypothesis to conclude that there are $A' \subseteq A_x$, $B' \subseteq B_y$ with

$$\log \frac{|A_x|}{|A'|} + \log \frac{|B_x|}{|B'|} \le f(k')$$

such that $\dim A', \dim B' \le C_1 k' \le C_1 k$. This and (7.11) immediately imply

$$\log \frac{|A|}{|A'|} + \log \frac{|B|}{|B'|} \le f(k') + \frac{20k}{\varepsilon}(k - k').$$

By (7.8), this is at most $f(k)$, since $C_1 \ge 20/\delta \ge 20/\varepsilon$. This closes the induction in Case 1.

Case 2: $\varepsilon \le \delta$. Recall here that $\varepsilon = d_{\mathrm{ent}}(\phi(U_A), \phi(U_B))$, and note that $\varepsilon \le k$ by Proposition 1.4. Let ε_0 be the constant from Proposition 1.3 and suppose $\delta \le \varepsilon_0$. By Proposition 1.3 there is some $H \le \mathbf{F}_2^D$ such that

$$d_{\mathrm{ent}}(\phi(U_A), U_H), d_{\mathrm{ent}}(\phi(U_B), U_H) \le 12\varepsilon.$$

It is possible that $H = \mathbf{F}_2^D$. In this case, we have by (A14) and Lemma 7.2 that

$$\log(2^D) = \mathbf{H}(U_H) \le \mathbf{H}(\phi(U_A)) + 2d_{\mathrm{ent}}(\phi(U_A), U_H) \le 10k + 24\varepsilon \le 34k,$$

and so $D \le 100k$. This gives Theorem 7.3 simply by taking $A = A'$, $B = B'$, since $C_1 \ge 100$.

Alternatively, suppose that H is a proper subgroup of $\mathbf{F}_2^D$. Denote by $\tilde{\phi}$ the composition of ϕ with projection to $\mathbf{F}_2^D/H$. By (A17) we have

$$\mathbf{H}(\tilde{\phi}(U_A)) \le 2d_{\mathrm{ent}}(\phi(U_A), U_H) \le 32\varepsilon.$$

By (A2) there is some x_0 such that $\mathbf{P}(\tilde{\phi}(U_A) = x_0) \ge e^{-32\varepsilon} \ge e^{-32\delta}$. Choosing δ sufficiently small, this is $\ge 1 - \delta_0$ where δ_0 is the constant in Lemma 5.1, and so by Lemma 5.1

$$\mathbf{H}(\tilde{\phi}(U_A)) \le 2d_{\mathrm{ent}}\left(\tilde{\phi}(U_A), \tilde{\phi}(U_A)\right) \le 4d_{\mathrm{ent}}(\tilde{\phi}(U_A), \tilde{\phi}(U_B))$$

where the second inequality is by (1.3). The same bound holds for $\mathbf{H}(\tilde{\phi}(U_B))$.

Hence by Lemma 7.4 applied to $\tilde{\phi}$, A and B (noting that we cannot have $\mathbf{H}(\tilde{\phi}(U_A)) = \mathbf{H}(\tilde{\phi}(U_B)) = 0$, as then A, B would be contained in cosets of a proper subgroup) we deduce that there exist $x \in \mathbf{F}_2^D/H$, $y \in \mathbf{F}_2^D/H$ such that

$$\log \frac{|A|}{|A_x|} + \log \frac{|B|}{|B_y|} \le 8\left(k - d_{\mathrm{ent}}(U_{A_x}, U_{B_y})\right), \tag{7.12}$$

where $A_x = A \cap \tilde{\phi}^{-1}(x)$, $B_y = B \cap \tilde{\phi}^{-1}(y)$.

We now finish the proof as before. Set $k' = d_{\mathrm{ent}}(U_{A_x}, U_{A_y})$, which is $\leq k$ by (7.12). Since A, B are not contained in cosets of a proper subgroup of $\mathbf{Z}^D$, we have

$$|A_x| + |B_y| < |A| + |B|$$

and so by induction we may find $A' \subseteq A_x$, $B' \subseteq B_y$ with

$$\log \frac{|A_x|}{|A'|} + \log \frac{|B_y|}{|B'|} \leq f(k')$$

and $\dim A', \dim B' \leq C_1 k' \leq C_1 k$. Combining with (7.12) gives

$$\log \frac{|A|}{|A'|} + \log \frac{|B|}{|B'|} \leq f(k') + 8(k - k').$$

By (7.8) (and since $C_1 \geq 8$) this is at most $f(k)$. This closes the induction in Case 2 and the proof of Theorem 7.3 is complete. ∎

Remark. For this argument, the full strength of Proposition 1.3 was not needed, and the weaker bound (5.3) would have sufficed.

8 | ENTROPY FORMULATION OF PFR OVER $\mathbf{F}_2$

In this section we establish Proposition 1.10. Recall that the content of this proposition is that the following two statements are equivalent:

Statement 1. If $A \subseteq \mathbf{F}_2^D$ and if $\sigma[A] \leq K$ then A is covered by $O(K^{O(1)})$ cosets of some subspace $H \leq \mathbf{F}_2^D$ of size at most $|A|$.

Statement 2. If X, Y are two $\mathbf{F}_2^D$-valued random variables, there is some subgroup $H \leq \mathbf{F}_2^D$ such that $d_{\mathrm{ent}}(X, U_H), d_{\mathrm{ent}}(Y, U_H) \ll d_{\mathrm{ent}}(X, Y)$.

Proof of Proposition 1.10. We first derive the entropic statement, that is to say Statement 2 above, from the combinatorial one (Statement 1). Write $k := d_{\mathrm{ent}}(X, Y)$ and set $K := e^k$. We may assume that $k \geq \varepsilon_0$, where ε_0 is the constant in Proposition 1.3, since the claim follows immediately from that proposition otherwise. Applying Proposition 1.2 with $C = 4$, we obtain a set $S \subseteq \mathbf{F}_2^D$ with

$$d_{\mathrm{ent}}(X, U_S) \ll k \tag{8.1}$$

and (recalling that $\frac{|S+S|}{|S|} \leq \left(\frac{|S-S|}{|S|}\right)^3$; see for example, [22, corollary 2.12])

$$|S + S| \ll K^{O(1)}|S|. \tag{8.2}$$

By Statement 1 there is a subgroup $H \leq \mathbf{F}_2^D$, $|H| \leq |S|$, such that S is covered by $O(K^{O(1)})$ cosets of H. Note, in particular, that $S + H$ is contained in the union of the aforementioned cosets, and so $|S + H| \ll K^{O(1)} \min(|S|, |H|)$. Now for any sets A, B we have

$$\begin{aligned} d_{\mathrm{ent}}(U_A, U_B) &= \mathbf{H}(U_A - U_B) - \frac{1}{2}(\mathbf{H}(U_A) + \mathbf{H}(U_B)) \\ &\leq \log|A - B| - \frac{1}{2}(\log|A| + \log|B|) \\ &= \log\left(\frac{|A - B|}{|A|^{1/2}|B|^{1/2}}\right). \end{aligned}$$

(This is the bipartite version of (1.1).) Applying this with $A = S$ and $B = H$ (and noting $H = -H$) gives $d_{\mathrm{ent}}(U_S, U_H) \ll k$, and so by the triangle inequality and (8.1) we have $d_{\mathrm{ent}}(X, U_H) \ll k$, which is the conclusion in Statement 2.

We turn now to the reverse implication, deriving the combinatorial Statement 1 from the entropic Statement 2. Suppose that $A \subseteq \mathbf{F}_2^D$ is a set and write $K := \sigma[A]$ and $k := \log K$. Then, by (1.1), we have $d_{\mathrm{ent}}(A, -A) = \log \sigma_{\mathrm{ent}}[A] \leq k$. Assuming Statement 2, there is some finite subgroup $H \leq \mathbf{F}_2^D$ with $d_{\mathrm{ent}}(U_A, U_H) \ll k$. By (A14) and the fact that $\mathbf{H}(U_A) = \log|A|$, $\mathbf{H}(U_H) = \log|H|$, we have

$$K^{-O(1)}|A| \ll |H| \ll K^{O(1)}|A|. \tag{8.3}$$

Writing $p(x)$ for the density function of $U_A - U_H$, thus $p(x) = \frac{|A \cap (H+x)|}{|A||H|}$, it follows from (A2) that there is some x_0 such that

$$p(x_0) \geq e^{-\mathbf{H}(U_A - U_H)} = e^{-d_{\mathrm{ent}}(U_A, U_H)}|A|^{-1/2}|H|^{-1/2} \gg K^{-O(1)}|A|^{-1},$$

or in other words $|A \cap (H + x_0)| \gg K^{-O(1)}|H|$.

Recall the Ruzsa covering lemma (see e.g., [22, lemma 2.14]), which states that if $|U + V| \leq K|U|$ then V is covered by K translates of $U - U$. Applying this with $U = A \cap (H + x_0)$ and $V = A$, and using the fact that $U + V \subseteq A + A$ and $U - U \subseteq H$, it follows that A is covered by $O(K^{O(1)})$ translates of H.

If $|H| \leq |A|$, we are done. If $|H| > |A|$, pass to a subgroup $H' \leq H$ of size in the range $(\frac{1}{2}|A|, |A|]$; then A is covered by $O(K^{O(1)})$ translates of H', and the proof is complete in this case also. ∎

A minor modification of the first part of the above proof, using the quantity C_{PFR} from the introduction in place of Statement 1, gives the following statement.

Proposition 8.1. *Let X, Y be $\mathbf{F}_2^D$-valued random variables, and suppose that $d_{\mathrm{ent}}(X, Y) = k$. Then there is some subgroup $H \leq \mathbf{F}_2^D$ such that $d_{\mathrm{ent}}(X, U_H) \leq Ck(1 + k^{C_{\mathrm{PFR}}-1})$, for some absolute constant C (which may depend on C_{PFR}).*

9 | DIMENSION AND THE WEAK PFR CONJECTURE

We now prove Theorem 1.11 (and hence Corollary 1.12). The proof is along somewhat similar lines to the proof of Theorem 1.8 given in Section 7, but more involved. An important ingredient will be the following lemma.

Throughout this section, C will be the constant in Proposition 8.1 (but the precise nature of this constant is not important).

Lemma 9.1. *Suppose that X and Y are $\mathbf{F}_2^D$-valued random variables. Then there is a subgroup $H \leq \mathbf{F}_2^D$ such that, denoting by $\psi : \mathbf{F}_2^D \to \mathbf{F}_2^D/H$ the natural projection, and setting $k := d_{\mathrm{ent}}(\psi(X), \psi(Y))$, we have*

$$\log |H| \leq 2(\mathbf{H}(X) + \mathbf{H}(Y)) \tag{9.1}$$

and

$$\mathbf{H}(\psi(X)) + \mathbf{H}(\psi(Y)) \leq 8Ck\left(1 + k^{C_{\mathrm{PFR}}-1}\right). \tag{9.2}$$

We isolate the following (sub-) lemma from the proof.

Lemma 9.2. *Let $n \in \mathbf{N}$. Let X, Y be $\mathbf{F}_2^n$-valued random variables. Set $k := d_{\mathrm{ent}}(X, Y)$, and suppose that*

$$\mathbf{H}(X) + \mathbf{H}(Y) > 8Ck\left(1 + k^{C_{\mathrm{PFR}}-1}\right). \tag{9.3}$$

Then there is a nontrivial subgroup $H \leq \mathbf{F}_2^n$ such that

$$\log |H| \leq \mathbf{H}(X) + \mathbf{H}(Y) \tag{9.4}$$

and (writing $\psi : \mathbf{F}_2^n \to \mathbf{F}_2^n/H$ as above)

$$\mathbf{H}(\psi(X)) + \mathbf{H}(\psi(Y)) \leq \frac{1}{2}\left(\mathbf{H}(X) + \mathbf{H}(Y)\right). \tag{9.5}$$

Proof. Set $k := d_{\mathrm{ent}}(X, Y)$. Applying Proposition 8.1, we obtain a subgroup H such that $d_{\mathrm{ent}}(X, U_H), d_{\mathrm{ent}}(Y, U_H) \leq Ck(1 + k^{C_{\mathrm{PFR}}-1})$. By (A17) and (9.3), it follows that

$$\mathbf{H}(\psi(X)) + \mathbf{H}(\psi(Y)) \leq 4Ck\left(1 + k^{C_{\mathrm{PFR}}-1}\right) < \frac{1}{2}(\mathbf{H}(X) + \mathbf{H}(Y)),$$

which is (9.5). To prove (9.4), an application of (A14) yields

$$\log |H| - \mathbf{H}(X) \leq 2d_{\mathrm{ent}}(X, U_H) \leq 2Ck\left(1 + k^{C_{\mathrm{PFR}}-1}\right),$$

and similarly for Y. Therefore using (9.3) we have

$$\log |H| \leq \frac{1}{2}(\mathbf{H}(X) + \mathbf{H}(Y)) + 2Ck\left(1 + k^{C_{\mathrm{PFR}}-1}\right) < \mathbf{H}(X) + \mathbf{H}(Y),$$

which gives the required bound (9.4).

If H were trivial we would have $\psi(X) = X, \psi(Y) = Y$ and so (9.5) would imply $\mathbf{H}(X) + \mathbf{H}(Y) = 0$, which then contradicts (9.3). ∎

Proof of Lemma 9.1. We iteratively define a sequence $\{0\} = H_0 < H_1 < \cdots$ of subgroups of $\mathbf{F}_2^D$. Denote by $\psi_i : \mathbf{F}_2^D \to \mathbf{F}_2^D/H_i$ the ith associated projection operator, and set $k_i := d_{\mathrm{ent}}(\psi_i(X), \psi_i(Y))$. We stop the iteration at the ith stage if we have

$$\mathbf{H}(\psi_i(X)) + \mathbf{H}(\psi_i(Y)) \leq 8Ck_i\left(1 + k_i^{C_{\mathrm{PFR}}-1}\right). \tag{9.6}$$

Otherwise, we apply Lemma 9.2 to $\psi_i(X), \psi_i(Y)$, obtaining a nontrivial subgroup $H_{i+1}/H_i \leq \mathbf{F}_2^D/H_i$ such that

$$\log \frac{|H_{i+1}|}{|H_i|} \leq \mathbf{H}(\psi_i(X)) + \mathbf{H}(\psi_i(Y)) \tag{9.7}$$

and

$$\mathbf{H}(\psi_{i+1}(X)) + \mathbf{H}(\psi_{i+1}(Y)) \leq \frac{1}{2}\left(\mathbf{H}(\psi_i(X)) + \mathbf{H}(\psi_i(Y))\right). \tag{9.8}$$

Clearly from iterated application of (9.8) we obtain

$$\mathbf{H}(\psi_i(X)) + \mathbf{H}(\psi_i(Y)) \leq 2^{-i}(\mathbf{H}(X) + \mathbf{H}(Y)).$$

Then, from a telescoping application of (9.7) we get

$$\log |H_i| \leq 2(\mathbf{H}(X) + \mathbf{H}(Y)). \tag{9.9}$$

Since the groups H_i form a strictly increasing sequence, the iteration does terminate at some time i. At this time we have both (9.6) and (9.9) and so, setting $\psi = \psi_i$, the proof of Lemma 9.1 is concluded. ∎

Now we turn our attention to Theorem 1.11. It is a consequence of the following bipartite statement, which should be compared to Theorem 7.3.

Theorem 9.3. *There are absolute constants C_1, C_2 such that, setting $f(t) := C_1 t(1 + t^{1-1/C_{\mathrm{PFR}}})$, the following is true. Let $D \in \mathbf{N}$, and suppose $A, B \subseteq \mathbf{Z}^D$ are finite non-empty sets, and set $k := d_{\mathrm{ent}}(U_A, U_B)$. Then there exist nonempty $A' \subseteq A$, $B' \subseteq B$ with*

$$\log \frac{|A|}{|A'|} + \log \frac{|B|}{|B'|} \leq f(k)$$

and such that $\dim A', \dim B' \leq C_2 k$.

Proof. We will proceed by induction on $|A| + |B|$. We may also assume that A, B do not sit inside cosets of a proper subgroup of $\mathbf{Z}^D$, else we may replace $\mathbf{Z}^D$ by that subgroup.

Let $\phi : \mathbf{Z}^D \to \mathbf{F}_2^D$ be the natural homomorphism. By Lemma 7.2 we have

$$\mathbf{H}(\phi(U_A)), \mathbf{H}(\phi(U_B)) \leq 10k. \tag{9.10}$$

Applying Lemma 9.1 to $\phi(U_A), \phi(U_B)$, we find a subgroup $H \leq \mathbf{F}_2^D$ and associated projection $\psi : \mathbf{F}_2^D \to \mathbf{F}_2^D/H$ such that, denoting by $\tilde{\phi} = \psi \circ \phi : \mathbf{Z}^D \to \mathbf{F}_2^D/H$ the natural (composite) projection, we have

$$\log |H| \leq 2(\mathbf{H}(\phi(U_A)) + \mathbf{H}(\phi(U_B))) \leq 40k \tag{9.11}$$

and

$$\mathbf{H}(\tilde{\phi}(U_A)) + \mathbf{H}(\tilde{\phi}(U_B)) \leq 8Cd\left(1 + d^{C_{\mathrm{PFR}}-1}\right) \tag{9.12}$$

where

$$d := d_{\text{ent}}\left(\tilde{\phi}(U_A), \tilde{\phi}(U_B)\right). \tag{9.13}$$

Now by (9.10), (A4) we also have

$$\mathbf{H}(\tilde{\phi}(U_A)) + \mathbf{H}(\tilde{\phi}(U_B)) \leq 20k. \tag{9.14}$$

In the following, set $\gamma := 1/C_{\text{PFR}}$ for convenience. If $d \geq 1$ then taking (9.12) to the power γ times (9.14) to the power $1-\gamma$ gives

$$\mathbf{H}(\tilde{\phi}(U_A)) + \mathbf{H}(\tilde{\phi}(U_B)) \leq 20Ck^{1-\gamma}d.$$

If $d \leq 1$ then the right-hand side of (9.12) is $\leq 16Cd$. Thus in all cases we have

$$\mathbf{H}(\tilde{\phi}(U_A)) + \mathbf{H}(\tilde{\phi}(U_B)) \leq 20C(1+k^{1-\gamma})d. \tag{9.15}$$

Now if H is all of $\mathbf{F}_2^D$ then it follows from (9.11) (taking $C_2 = 40/\log 2$) that $D \leq C_2 k$, and so Theorem 9.3 is true simply by taking $A' = A$, $B' = B$.

Suppose, then, that H is not all of $\mathbf{F}_2^D$. For $x, y \in \mathbf{F}_2^D/H$, denote by $A_x := A \cap \tilde{\phi}^{-1}(x)$ and $B_y := B \cap \tilde{\phi}^{-1}(y)$ the fibres of A, B above x, y respectively. Since we are assuming that A, B do not sit inside cosets of a proper subgroup of $\mathbf{Z}^D$, we may assume that at least one of $\tilde{\phi}(A), \tilde{\phi}(B)$ is not a singleton, and so

$$|A_x| + |B_y| < |A| + |B|$$

and $\mathbf{H}(\tilde{\phi}(U_A)) + \mathbf{H}(\tilde{\phi}(U_B)) > 0$, whereby $d > 0$ by (9.12). Applying Lemma 7.4 once again, and noting (9.13) and (9.15), we find $x, y \in \mathbf{F}_2^D/H$ such that

$$\log \frac{|A|}{|A_x|} + \frac{|B|}{|B_y|} \leq 20C(1+k^{1-\gamma})\left(k - d_{\text{ent}}(U_{A_x}, U_{B_y})\right) \tag{9.16}$$

Set $k' = d_{\text{ent}}(U_{A_x}, U_{B_y})$. By induction on A_x, B_y we may find $A' \subseteq A_x$ and $B' \subseteq B_y$ such that $\dim A', \dim B' \leq C_2 k' \leq C_2 k$ and

$$\log \frac{|A_x|}{|A'|} + \log \frac{|B_y|}{|B'|} \leq f(k').$$

Adding this to (9.16) yields

$$\log \frac{|A|}{|A'|} + \log \frac{|B|}{|B'|} \leq f(k') + 20C(1+k^{1-\gamma})(k-k'). \tag{9.17}$$

However,

$$\begin{aligned} f(k') &= C_1 k'(1+(k')^{1-\gamma}) \\ &\leq C_1 k'(1+k^{1-\gamma}) \\ &= f(k) - C_1(k-k')(1+k^{1-\gamma}). \end{aligned}$$

This, provided $C_1 \geq 20C$, the right-hand side of (9.17) is at most $f(k)$, and this closes the induction. The proof is complete. ∎

ACKNOWLEDGMENTS

We thank Zachary Hunter and Noah Kravitz for some corrections to the first version of the paper. BG and TT are supported by Simons Investigator Award 376201 and 256485. FM is supported by a Sloan Fellowship. During part of the preparation of this work, he was also supported by a von Neumann Fellowship from the Institute for Advanced Study. TT is supported by NSF grant DMS-1764034 and by a Simons Investigator Award.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Ben Green https://orcid.org/0000-0002-2224-1193

REFERENCES

1. A. Avez, *Entropie des groupes de type fini*, C. R. Acad. Sci. Paris Sér. A-B **275** (1972), A1363–A1366.
2. J. Bourgain and M.-C. Chang, *On the size of k-fold sum and product sets of integers*, J. Am. Math. Soc. **17** (2004), no. 2, 473–497.
3. E. Breuillard and P. Varjú, *Entropy of Bernoulli convolutions and uniform exponential growth for linear groups*, J. Anal. Math. **140** (2020), no. 2, 443–481.
4. M.-C. Chang, *Some consequences of the polynomial Freiman-Ruzsa conjecture*, C. R. Math. Acad. Sci. Paris **347** (2009), no. 11–12, 583–588.
5. G. A. Freiman, "*Number-theoretic studies in the Markov spectrum and in the structural theory of set addition*," In groups and the inverse problems of additive number theory (in Russian), Kalinin. Gos. Univ, Moscow, 1973.
6. R. Gray, Entropy and information theory, Springer-Verlag, New York, 1990.
7. B. J. Green, *Finite field models in additive combinatorics, in surveys in combinatorics*, London Math. Soc. Lecture Notes **327** (2005), 1–27.
8. B. J. Green, Course notes for C3.10, Oxford, 2022 Available on request.
9. B. J. Green and T. C. Tao, *An equivalence between inverse sumset theorems and inverse conjectures for the U^3-norm*, Math. Proc. Camb. Philo. Soc. **149** (2010), no. 1, 1–19.
10. M. Hochman, *On self-similar sets with overlaps and inverse theorems for entropy*, Ann. Math. **180** (2014), no. 2, 773–822.
11. V. A. Kaĭmanovich and A. M. Vershik, *Random walks on discrete groups: Boundary and entropy*, Ann. Probab. **11** (1983), 457–490.
12. S. Lovett, *Equivalence of polynomial conjectures in additive combinatorics*, Combinatorica **32** (2012), no. 5, 607–618.
13. S. Lovett and O. Regev, *A counterexample to a strong variant of the polynomial Freiman–Ruzsa conjecture*, Discrete Anal **8** (2017), 6.
14. F. R. W. M. Manners, *Finding a low-dimensional piece of a set of integers*, Int. Math. Res. Not. **15** (2017), 4673–4703.
15. D. Pálvölgyi and D. Zhelezov, *Query complexity and the polynomial Freiman–Ruzsa conjecture*, Adv. Math. **392** (2021), 108043.
16. I. Z. Ruzsa, *Sumsets and entropy*, Random Struct. Alg. **34** (2009), 1–10.
17. A. Samorodnitsky. Low-degree tests at large distances, In Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing, 506–515. 2007.
18. T. Sanders, *On the Bogolyubov–Ruzsa lemma*, Anal. PDE **5** (2012), no. 3, 627–655.
19. T. Sanders, *The structure theory of set addition revisited*, Bull. Amer. Math. Soc. **50** (2013), 93–127.
20. T. C. Tao, *Sumset and inverse sumset theory for Shannon entropy*, Comb. Probab. Comput. **19** (2010), no. 4, 603–639.

21. T. C. Tao and V. H. Vu, *John-type theorems for generalized arithmetic progressions and iterated sumsets*, Adv. Math. **219** (2008), no. 2, 428–449.
22. T. C. Tao and V. H. Vu, "*Additive combinatorics*," Cambridge studies in advanced mathematics, Vol **105**, Cambridge University Press, Cambridge, 2010.
23. D. Zhelezov, available at https://www.youtube.com/watch?v=37JXZiMtVvA.

How to cite this article: B. Green, F. Manners, and T. Tao, *Sumsets and entropy revisited*, Random Struct. Alg. (2024), 1–33. https://doi.org/10.1002/rsa.21252

APPENDIX A: BASIC FACTS ABOUT ENTROPY

In this section we gather together basic facts about entropy, referring the reader to other sources (e.g., [20, appendix A] or [6]) for the (standard, and mostly easy) proofs.

We begin with the most basic results.

A.1 | BASIC ENTROPY RESULTS

If X is an S-valued random variable for some finite S, the Shannon entropy is defined as

$$\mathbf{H}(X) := \sum_x p_X(x) \log \frac{1}{p_X(x)},$$

where x is understood to range over S and[3] we adopt the convention that any term involving a factor of $p_X(x)$ vanishes when $p_X(x) = 0$. From Jensen's inequality we have

$$\mathbf{H}(X) \leq \log |S|. \tag{A1}$$

Also,

$$\mathbf{H}(X) = \sum_x p_X(x) \log \frac{1}{p_X(x)} \geq \min_{x: p_X(x)>0} \log \frac{1}{p_X(x)},$$

and therefore

$$\max_x p_X(x) \geq e^{-\mathbf{H}(X)}. \tag{A2}$$

If X, Y are random variables then

$$\mathbf{H}(X, Y) \leq \mathbf{H}(X) + \mathbf{H}(Y), \tag{A3}$$

and equality occurs if X, Y are independent. At the other end of the spectrum, if X determines Y then $\mathbf{H}(X, Y) = \mathbf{H}(X)$. See for instance [6, lemma 2.3.2].

[3]We use the natural logarithm in this paper, but one could easily work with other bases of the logarithm if desired.

A.2 | CONDITIONAL ENTROPY

We define

$$\mathbf{H}(X|Y) = \sum_y p_Y(y)\mathbf{H}(X|Y = y).$$

Then we have the *chain rule*

$$\mathbf{H}(X, Y) = \mathbf{H}(X|Y) + \mathbf{H}(Y).$$

If $Y = f(X)$ for some function f then, since $\mathbf{H}(X, Y) = \mathbf{H}(X)$, it follows that

$$\mathbf{H}(f(X)) \leq \mathbf{H}(X). \tag{A4}$$

A.3 | SUBMODULARITY

For any three random variables A, B, C we have the submodularity inequality

$$\mathbf{H}(A, B, C) + \mathbf{H}(C) \leq \mathbf{H}(A, C) + \mathbf{H}(B, C) \tag{A5}$$

(which is equivalent to the non-negativity of the conditional mutual information $\mathbf{I}(A : B|C)$); see for instance [6, lemma 2.5.5].

An equivalent and useful way to write the submodularity inequality is

$$\mathbf{H}(A|B, C) \leq \mathbf{H}(A|C). \tag{A6}$$

Note also that, if B determines C, then $\mathbf{H}(A, B, C) = \mathbf{H}(A, B)$ and $\mathbf{H}(B, C) = \mathbf{H}(B)$, and submodularity implies that

$$\mathbf{H}(A|B) \leq \mathbf{H}(A|C). \tag{A7}$$

A.4 | KULLBACK–LEIBLER DIVERGENCE

Suppose that X, Y are random variables with distribution functions μ_X, μ_Y respectively. Then we define

$$D_{KL}(X\|Y) := \sum_t \mu_X(t) \log\left(\frac{\mu_X(t)}{\mu_Y(t)}\right).$$

It is conventional to define the summand here to be 0 if $\mu_X(t) = 0$ and ∞ if $\mu_Y(t) = 0$ but $\mu_X(t) \neq 0$; in practice, we will avoid the latter situation.

It is convenient to relate this to the *cross-entropy*

$$\mathbf{H}(X : Y) := \sum_t \mu_X(t) \log \frac{1}{\mu_Y(t)} \tag{A8}$$

(where the same conventions are in force). Thus

$$D_{KL}(X\|Y) = \mathbf{H}(X : Y) - \mathbf{H}(X). \tag{A9}$$

In particular, if X takes values in a finite set S, then $\mathbf{H}(X : U_S) = \log |S|$ and thus

$$D_{KL}(X\|U_S) = \log |S| - \mathbf{H}(X). \tag{A10}$$

Note that $\mathbf{H}(X : Y)$ is *not* at all the same thing as $\mathbf{H}(X, Y)$ (or $\mathbf{H}(X|Y)$). Indeed, the former depends only on the distribution functions of X, Y and not in any way on their dependence, and it is also asymmetric in that in general $\mathbf{H}(X : Y) \neq \mathbf{H}(Y : X)$. From a standard application of Jensen's inequality we obtain *Gibbs' inequality*

$$D_{KL}(X\|Y) \geq 0 \tag{A11}$$

(see e.g., [6, theorem 2.3.1]); we also have the well known *Pinsker's inequality*

$$\sum_t |p_X(t) - p_Y(t)| \leq \sqrt{2D_{KL}(X\|Y)}, \tag{A12}$$

see for example, [6, lemma 5.2.8].

Now we turn to some simple results about G-valued random variables, where G is abelian, and we assume all random variables to have finite support. The reader may wish to recall the definitions of d_{ent} and d^*_{ent}, given at (1.2) and (1.4) respectively.

First, if X, Y are independent such variables then

$$\mathbf{H}(X - Y) \geq \mathbf{H}(X - Y|Y) = \mathbf{H}(X). \tag{A13}$$

From this we see that

$$d_{\text{ent}}(X, Y) = d_{\text{ent}}(Y, X) \geq \frac{|\mathbf{H}(X) - \mathbf{H}(Y)|}{2} \geq 0. \tag{A14}$$

Let X be a G-valued random variable, and let H be a finite subgroup of G. Denote by $\pi : G \to G/H$ the quotient map. Let U_H be a uniform random variable on H, independent of X. Then we have

$$\mathbf{H}(X + U_H) = \mathbf{H}(\pi(X)) + \mathbf{H}(U_H) = \mathbf{H}(\pi(X)) + \log |H|. \tag{A15}$$

It follows that

$$d_{\text{ent}}(X, U_H) = \mathbf{H}(\pi(X)) + \frac{1}{2}(\log |H| - \mathbf{H}(X)). \tag{A16}$$

From this and (A14) we have

$$\mathbf{H}(\pi(X)) \leq 2d_{\text{ent}}(X, U_H). \tag{A17}$$

Also, from Lemma 1.1 and $d_{\text{ent}}(U_H, U_H) = 0$ we observe that

$$d^*_{\text{ent}}(X, U_H) = d_{\text{ent}}(X, U_H).$$

Finally, if X, Y, Z are G-valued random variables (not necessarily independent), we observe from the Gibbs inequality (A11) the useful bound

$$\begin{aligned}\mathbf{H}(Z-Y)-\mathbf{H}(Y) &\leq \mathbf{H}(Z-Y:X)-\mathbf{H}(Y)\\ &= \sum_z p_Z(z)\left(\mathbf{H}(z-Y:X)-\mathbf{H}(z-Y)\right)\\ &= \sum_z p_Z(z) D_{KL}(z-Y\|X)\end{aligned} \tag{A18}$$

where we have used the permutation-invariance of Shannon entropy to observe that $\mathbf{H}(z-Y)=\mathbf{H}(Y)$, as well as the fact that $p_{Z-Y}(t)=\sum_z p_Z(z)p_{z-Y}(t)$. Note that we in fact have equality when $X=Z-Y$.

APPENDIX B: ENERGY, ENTROPY AND DOUBLING

In this section we prove the inequalities (1.1). Recall the statement, which is that

$$\frac{|A|^3}{\mathrm{E}[A]} \leq \sigma_{\mathrm{ent}}[A] \leq \sigma[A]. \tag{B1}$$

Proof. Denote $X := U_A + U_A'$ to be the sum of two independent uniform random variables on A. The right-hand inequality is immediate from the inequality $\mathbf{H}(X) \leq \log|A+A|$, which is a special case of Jensen's inequality. As for the left-hand inequality, observe that

$$p_X(x) := \frac{|A\cap(x-A)|}{|A|^2}.$$

and then by the weighted AM–GM inequality,

$$e^{-\mathbf{H}(X)} = \prod_x p_X(x)^{p_X(x)} \leq \sum_x p_X(x)^2 = \frac{\mathrm{E}[A]}{|A|^4}.$$

The result follows immediately. ∎

The above argument can be reformulated in terms of the *Rényi entropies* $\mathbf{H}_\alpha(X)$, defined for $\alpha \neq 1$ by

$$\mathbf{H}_\alpha(X) := \frac{1}{1-\alpha}\log\left(\sum_x p_X(x)^\alpha\right)$$

and extended by continuity to $\alpha = 1$ by setting $\mathbf{H}_1(X) := \mathbf{H}(X)$. A brief calculation reveals the identities

$$\begin{aligned}\exp(\mathbf{H}_0(X)) &= |A+A|\\ \exp(\mathbf{H}_1(X)) &= \sigma_{\mathrm{ent}}[A]|A|\\ \exp(\mathbf{H}_2(X)) &= \frac{|A|^4}{\mathrm{E}[A]},\end{aligned}$$

and the claim now follows from the well-known fact that the Rényi entropy $\mathbf{H}_\alpha(X)$ is non-increasing in α.

We conclude with a simple example showing that both inequalities in (B1) can be far from tight. Suppose that $n = 2m$ is even and $A = H \cup \{x_1, \dots, x_m\}$, with H a subgroup of size m and $x_1, \dots, x_m$ highly dissociated with respect to H, for instance with $x_i + x_j - x_k - x_l \in H$ only if $\{i,j\} = \{k,l\}$. Then we have $|A|^3/\mathrm{E}[A] = \frac{1}{16} + o(1)$ as $n \to \infty$. Turning to $\sigma_{\mathrm{ent}}[A]$, we of course have $\mathbf{H}(U_A) = \log n$. The variable $U_A + U'_A$ may be conditioned to subvariables which are, respectively, uniformly distributed on H, on the set $\bigcup_{i=1}^m (x_i + H)$, and on the multiset $\bigcup_{i,j=1}^m \{x_i + x_j\}$, with the conditioning probabilities being $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$. One therefore computes that $\mathbf{H}(U_A + U'_A) = (\frac{7}{4} + o(1)) \log n$ and so $\sigma_{\mathrm{ent}}[A] = n^{3/4+o(1)}$. Finally, $\sigma[A] = (\frac{3}{4} + o(1))n$.