2.3.19 Suppose that $A$ and $B$ are subgroups of $Z$, and let $x = y = 0$. Show that all the inequalities in (2.8) are in fact equalities.

2.3.20 Let $A, B, C$ be additive sets in an ambient group $Z$. Show that

$$\max(E(A,B), E(A,C)) \leq E(A, B \cup C)^{1/2} \leq E(A,B)^{1/2} + E(A,C)^{1/2}.$$

(Hint: use Lemma 2.9 and the triangle inequality for the $l^2$ norm.)

2.3.21 Let $A, B, C$ be additive sets in an ambient group $Z$ with $|A| = |B| = |C| = N$. Give examples of such sets where $E(A,B)$ and $E(A,C)$ are comparable to $N^2$ and $E(B,C)$ is comparable to $N^3$, or where $E(A,B)$ and $E(A,C)$ are comparable to $N^3$ and $E(B,C)$ are comparable to $N^2$. These examples show that there is no hope of any useful "triangle inequality" connecting $E(A,B)$, $E(B,C)$, and $E(A,C)$.

2.3.22 Suppose $A, B$ are additive sets in an ambient group $Z$. Show that $E(A,B) = |A|^2|B|$ holds if and only if $|A+B| = |B|$. One can thus use Proposition 2.2 to determine when the upper bound in (2.7) is obtained. Conclude in particular that $E(A,B) = |A|^{3/2}|B|^{3/2}$ if and only if $d(A,B) = 0$, which in turn occurs if and only if $A$ and $B$ are cosets of the same finite group $G$.

2.3.23 Give an example of an additive set $A \subset \mathbf{Z}$ of cardinality $|A| = N$ such that $E(A,A) \geq \frac{1}{100}N^3$ but $d(A,A) \geq \frac{1}{100}\log N$. Compare this with (2.8) (and with Corollary 2.31 below).

2.3.24 Let $A$ be an additive set. Show that there exists a subset $A'$ of $A$ of cardinality $|A'| \geq \frac{1}{2\sigma[A]}|A|$ and an element $a_0 \in A'$ such that $|(a+A) \cap (a_0 + A)| \geq \frac{1}{2\sigma[A]}|A|$ for all $a \in A'$. (Hint: first obtain a lower bound for $E(A,A)$.)

## 2.4 Covering lemmas

We now describe some covering lemmas, which roughly speaking have the following flavor: if $A$ and $B$ have similar additive structure (for instance, if their Ruzsa distance is small) then one can cover $A$ by a small number translates of $B$ (or some modification of $B$).

**Lemma 2.14 (Ruzsa's covering lemma)** *[300] For any additive sets $A, B$ with common ambient group $Z$, there exists an additive set $X_+ \subseteq B$ with*

$$B \subseteq A - A + X_+; \qquad |X_+| \leq \frac{|A+B|}{|A|}; \qquad |A + X_+| = |A||X_+|$$

*and similarly there exists an additive set $X_- \subseteq B$ with*

$$B \subseteq A - A + X_-; \qquad |X_-| \leq \frac{|A-B|}{|A|}; \qquad |A - X_-| = |A||X_-|.$$

*In particular, $B$ can be covered by* $\min(\frac{|A+B|}{|A|}, \frac{|A-B|}{|A|})$ *translates of $A - A$.*

**Remark 2.15** One useful side benefit of this covering lemma is that there exist at least $\frac{|B|}{|A-A|}$ disjoint translates $A + b$ of $A$ with $b \in B$, as can be seen by restricting $b$ to $X_+$.

*Proof* It suffices to prove the claim concerning $A + B$, since the claim concerning $A - B$ follows by replacing $B$ with $-B$ and $X_+$ with $-X_-$ (note that $A - A$ is symmetric around the origin). Consider the family $\{A + b : b \in B\}$ of translates of $A$ by elements of $B$. All of these translates have volume $|A|$ and are contained inside $A + B$. Thus if we take a maximal disjoint sub-family of these translates, i.e. $\{A + x : x \in X_+\}$ for some $X_+ \subseteq B$, then $X_+$ can have cardinality at most $\frac{|A+B|}{|A|}$. Also we have $|A + X_+| = |A||X_+|$ by construction. Now for any element $b \in B$, we see that $A + b$ cannot be disjoint from every member of $\{A + x : x \in X_+\}$ as this would contradict the maximality of $X_+$. Thus $A + b$ must intersect $A + X_+$, which implies that $b$ is in $A - A + X_+$. Since $b \in B$ was arbitrary, we thus have $B \subseteq A - A + X_+$ and the claim follows. □

Covering lemmas such as the one above are convenient for a number of reasons. Firstly, they allow for easy computation of iterated sum sets. For instance, if one knows that

$$A + B \subseteq A + X$$

then one can immediately deduce that

$$A + nB \subseteq A + nX \text{ for all } n \geq 0.$$

This is advantageous if $X$ is substantially smaller than $B$. Also, a covering property such as $A + B \subseteq A + X$ is preserved under Freiman homomorphisms, whereas bounds such as $|A + A| \leq K|A|$ are only preserved by Freiman isomorphisms (see Chapter 5, in particular Exercise 5.3.13).

**Remark 2.16** Observe that we are covering $B$ by $A - A$ rather than by $A$. This reflects the fact that $A - A$ is a "smoother" set than $A$, and tends to contain fewer "holes" that would render it unsuitable for covering other sets. Later on we shall see that higher-order sum-difference sets such as $2A - 2A$ are even smoother, in that they tend to contain very large arithmetic progressions; see Section 4.7 and Chapter 12 for further discussion.

One can modify Ruzsa's covering lemma in a number of ways. For instance, one can ensure the covering of $B$ by translates of $A - A$ has very high multiplicity (at the cost of increasing the number of covers by a factor of 2).

**Lemma 2.17 (Green–Ruzsa covering lemma)** *[154] Let $A$ and $B$ be additive sets with common ambient group. Then there exists an additive set $X \subseteq B$ with $|X| \leq 2\frac{|A+B|}{|A|} - 1$ such that for every $y \in B$ there are at least $|A|/2$ triplets $(x, a, a') \in X \times A \times A$ with $x + a - a' = y$. More informally, $A - A + X$ covers $B$ with multiplicity at least $|A|/2$. Furthermore, we have*

$$B - B \subseteq A - A + X - X.$$

*Similar claims hold if $\frac{|A+B|}{|A|}$ is replaced by $\frac{|A-B|}{|A|}$.*

*Proof* Again it suffices to prove the claim for $\frac{|A+B|}{|A|}$. We perform the following algorithm. Initialize $X$ to be the empty set, so that $X + A - A$ is also the empty set. We now run the following loop. If we cannot find any element $y$ in $B$ which is "sufficiently disjoint from $X + A - A$" in the sense that $|(y + A) \cap (X + A)| \leq |A|/2$, we terminate the algorithm. Otherwise, if there is such an element $y$, we add it to $X$, and then repeat the algorithm.

Every time we add an element to $X$, the size of $|X + A|$ increases by at least $|A|/2$, by construction, and at the first stage it increases by $|A|$. However, $X + A$ must always lie within the set $B + A$. Thus this algorithm terminates after at most $\frac{2|A+B|}{|A|} - 1$ steps.

Now let $y$ be any element of $B$. By construction, we have $|(y + A) \cap (X + A)| > |A|/2$, and hence $y$ has at least $|A|/2$ representations of the form $x + a - a'$ for some $(x, a, a') \in X \times A \times A'$, as desired.

Finally, if $y$ and $y'$ are two elements of $B$, then we have

$$|\{a \in A : y + a \in X + A\}| = |(y + A) \cap (X + A)| > |A|/2$$

and similarly we have $|\{a \in A : y' + a \in X + A\}| > |A|/2$. Thus by the pigeonhole principle there exists $a \in A$ such that $y + a \in X + A$ and $y' + a \in X + A$, thus $y - y' = (y + a) - (y' + a) \in X + A - (X + A) = A - A + X - X$. Since $y, y' \in B$ is arbitrary, we have $B - B \subseteq A - A + X - X$ as claimed. □

In Section 5.4 we develop yet another covering lemma (Lemma 5.31), in which the covering set $X$ is not arbitrary, but is in fact a cube.

We now give an application of the Green–Ruzsa covering lemma, namely a variant of (2.6) which controls quadruple sums rather than double sums.

**Proposition 2.18** *Let $A, B$ be additive sets in an ambient group $Z$. Then*

$$|2B - 2B| \leq 16\frac{|A+B|^4|A-A|}{|A|^4}.$$

*Proof* Applying the Green–Ruzsa covering lemma, we may find a set $X$ of cardinality $|X| \leq 2^{\frac{|A+B|}{|A|}}$ such that $A - A + X$ covers $B$ with multiplicity at least $|A|/2$.

Now let $z$ be any element of $B - B$. By definition, we have $z = b_1 - b_2$ for some $b_1, b_2 \in B$. By construction of $X$, we can find at least $|A|/2$ triplets $(x, a_1, a_2) \in X \times A \times A$ such that $b_2 = x + a_1 - a_2$, and thus

$$|\{(x, a_1, a_2) \in X \times A \times A : z = b_1 - a_1 + a_2 - x\}| \geq |A|/2.$$

Making the change of variables $c := b_1 + a_2 \in A + B$, we conclude that

$$|\{(x, c, a_1) \in X \times (A+B) \times A : z = c - a_1 - x\}| \geq |A|/2.$$

Similarly, if $z'$ is another element of $B - B$, we have

$$|\{(x', c', a_1') \in X \times (A+B) \times A : z' = c' - a_1' - x'\}| \geq |A|/2,$$

and hence

$$|\{(x, x', c, c', a_1, a_1') \in X \times X \times (A+B) \times (A+B) \times A \times A : z = c - a_1 - x, \quad z' = c' - a_1' - x'\}| \geq |A|^2/4.$$

Now write $d := a_1 - a_1' \in A - A$, and observe that if $z = c - a_1 - x$ and $z' = c' - a_1' - x'$ then

$$z - z' = c - c' - d - x + x'.$$

Also, if one fixes $z, z', c, c', d, x, x'$, then $a_1$ and $a_1'$ are determined by the equations $a_1 = c - x - z$, $a_1' = c' - x' - z'$. Thus we have

$$|\{(x, x', c, c', d) \in X \times X \times (A+B) \times (A+B) \times (A-A) : z - z' = c - c' - d - x + x'\}| \geq |A|^2/4.$$

Note that $z - z'$ is an arbitrary element of $(B - B) - (B - B) = 2B - 2B$. Thus we have shown that an arbitrary element of $2B - 2B$ has at least $|A|^2/4$ representations of the form $c - c' - d - x + x'$ where $(x, x', c, c', d) \in X \times X \times (A+B) \times (A+B) \times (A-A)$. The claim then follows since $|X| \leq 2^{\frac{|A+B|}{|A|}}$. □

We can eliminate the factor of 16 by the following elegant "tensor power trick" of Ruzsa [297]:

**Corollary 2.19** *Let $A, B$ be additive sets in an ambient group $Z$. Then*

$$|2B - 2B| \leq \frac{|A+B|^4|A-A|}{|A|^4}.$$

*Proof* Fix $A, B$, and let $M$ be a large integer parameter. We consider the $M$-fold Cartesian product $A^{\oplus M} := A \times \cdots \times A$, which is a subset of the additive group $Z^{\oplus M} := Z \oplus \cdots \oplus Z$; similarly consider $B^{\oplus M}$. Then one easily verifies

$$2B^{\oplus M} - 2B^{\oplus M} = (2B - 2B)^{\oplus M};$$
$$A^{\oplus M} + B^{\oplus M} = (A + B)^{\oplus M};$$
$$A^{\oplus M} - A^{\oplus M} = (A - A)^{\oplus M}.$$

Thus by applying Lemma 2.18 with $A, B$ replaced by $A^{\oplus M}, B^{\oplus M}$ we obtain

$$|2B - 2B|^M \leq 16 \frac{|A + B|^{4M} |A - A|^M}{|A|^{4M}}.$$

Taking $M$th roots of both sides and letting $M \to \infty$, we obtain the result. □

Specializing Corollary 2.19 to the case $B := -A$, we obtain

**Corollary 2.20** *Let $A$ be an additive set. Then*

$$|2A - 2A| \leq \frac{|A - A|^5}{|A|^4}$$

*or, in other words,*

$$d(A - A, A - A) \leq 4d(A, A).$$

**Remark 2.21** One can improve these estimates slightly by using the machinery of Plünnecke inequalities; see Corollary 6.28.

Combining Corollary 2.20 with the Ruzsa covering lemma (Lemma 2.14 with $B = 2A - A$) we obtain

**Corollary 2.22** *For any additive set $A$, $2A - A$ can be covered by $\delta[A]^5$ translates of $A - A$.*

This then shows that $3A - A$ is covered by $\delta[A]^5$ translates of $2A - A$, and hence by $\delta[A]^{10}$ translates of $A - A$. Continuing in this fashion, an easy induction then shows

$$mA - nA \text{ can be covered by } \delta[A]^{5(m+n-2)} \text{ translates of } A - A \tag{2.16}$$

for all $m, n \geq 1$. In particular we have

$$|mA - nA| \leq \delta[A]^{5(m+n-1)} |A| \text{ for all } m, n \geq 1. \tag{2.17}$$

From this (and the trivial estimates $|kA| \geq |A|$ for any $k \geq 1$) we obtain

**Corollary 2.23 (Symmetric sum set estimates, preliminary version)** *Let $A$ be an additive set. Then we have the estimates*

$$d(n_1 A - n_2 A, n_3 A - n_4 A) \leq 5(n_1 + n_2 + n_3 + n_4) d(A, A)$$

*for any non-negative integers $n_1, n_2, n_3, n_4$. (The constant 5 is not best possible; we will improve it later.)*

Thus if $A$ has small difference constant, then in fact all iterated sum sets of $A$ are close to each other in the Ruzsa metric. Another consequence of the corollary is that

$$\sigma[n_1 A - n_2 A] \leq \sigma[A]^{10(n_1+n_2)}$$

for all non-negative integers $n_1, n_2$. The factor of 10 is not best possible; we shall obtain improvements to this constant later when we develop the machinery of Plünnecke inequalities in Section 6.5. However, the linear growth in $n_1$ and $n_2$ is necessary; see Exercise 2.4.9.

By combining the above corollary with the Ruzsa triangle inequality one can obtain similar estimates for pairs of sets:

**Corollary 2.24 (Asymmetric sum set estimates, preliminary version)** *Let $A$, $B$ be additive sets with common ambient group $Z$. Then we have the estimates*

$$d(n_1 A - n_2 A + n_3 B - n_4 B, n_5 A - n_6 A + n_7 B - n_8 B) = O((n_1 + \cdots + n_8) d(A, B))$$

*for any $n_1, \ldots, n_8 \in \mathbf{N}$.*

The proof is left as an exercise.

We can use the above machinery to place additive sets with small difference or doubling constant inside a more structured set, namely an "approximate group".

**Definition 2.25 (Approximate groups)** Let $K \geq 1$. An additive set $H$ is said to be a *$K$-approximate group* if it is symmetric (so $H = -H$), contains the origin, and $H + H$ can be covered by at most $K$ translates of $H$.

Observe that a 1-approximate group is necessarily a finite group, and conversely every finite group is a 1-approximate group.

We can summarize many of the preceding results by giving the following partial generalization of Proposition 2.7.

**Proposition 2.26** *Let $A$ be an additive set and let $K \geq 1$. Then the following statements are equivalent up to constants, in the sense that if the $j$*th *property holds for some absolute constant $C_j$, then the $k$*th *property will also hold for some absolute constant $C_k$ depending on $C_j$:*

*(i)* $\sigma[A] \leq K^{C_1}$ *(i.e.* $|A + A| \leq K^{C_1}|A|$*);*
*(ii)* $\delta[A] \leq K^{C_2}$ *(equivalently,* $d(A, A) \leq C_2 \log K$ *or* $|A - A| \leq K^{C_2}|A|$*);*
*(iii)* $d(A, B) \leq C_3 \log K$ *for at least one additive set $B$;*
*(iv)* $|nA - mA| \leq K^{C_4(n+m)}|A|$ *for all non-negative integers $n, m$;*

(v) *there exists a $K^{C_5}$-approximate group $H$ such that $A \subseteq x + H$ for all $x \in A$, and furthermore $|A| \geq K^{-C_5}|H|$.*

*Proof* The equivalence of the first three properties follows from the Ruzsa triangle inequality and (2.11). The equivalence of the fourth property with (say) the second follows from Corollary 2.24. To see that the fifth property implies (say) the first, observe that if the former holds, then

$$|A + A| \leq |H + H| \leq K^{C_5}|H| \leq K^{2C_5}|A|.$$

To deduce the fifth from the fourth, take $H = A - A$ and apply the Ruzsa covering lemma. □

Thus, in a qualitative sense, we have reduced the study of additive sets with small difference or doubling constant to the study of approximate groups, or precisely to the study of dense subsets of translates of approximate groups. This is a fairly satisfactory state of affairs, except for the fact that we do not have a good characterization of which sets are approximate groups. The well known structure theorem for finite groups (see Corollary 3.8 below) asserts that every finite group is the product of finite cyclic groups; we shall eventually be able to obtain a somewhat similar characterization of approximate groups, showing that they are efficiently contained in a generalized arithmetic progression. For some other properties of approximate groups, see the exercises below.

There is an asymmetric counterpart to Proposition 2.26, whose proof we leave as an exercise.

**Proposition 2.27** *Let $A, B$ be additive sets in an ambient group $Z$, and let $K \geq 1$. Then the following statements are equivalent up to constants, in the sense that if the $j$*th *property holds for some absolute constant $C_j$, then the $k$*th *property will also hold for some absolute constant $C_k$ depending on $C_j$:*

(i) $d(A, B) \leq C_1 \log K$;
(ii) $d(A, -B) \leq C_2 \log K$;
(iii) $|A + B| \leq K^{C_3} \min(|A|, |B|)$;
(iv) $|A - B| \leq K^{C_4} \min(|A|, |B|)$;
(v) $|n_1 A - n_2 A + n_3 B - n_4 B| \leq K^{C_5(n_1+n_2+n_3+n_4)}|A|$ *for all non-negative integers $n_1, n_2, n_3, n_4$;*
(vi) $\sigma[A], \sigma[B] \leq K^{C_6}$, *and there exists $x \in Z$ such that* $|A \cap (B + x)| \geq K^{-C_6}|A|^{1/2}|B|^{1/2}$;
(vii) $\sigma[A], \sigma[B] \leq K^{C_7}$, *and* $E(A, B) \geq K^{-C_7}|A|^{3/2}|B|^{3/2}$;
(viii) *there exists a $K^{C_8}$-approximate group $H$ such that $A \subseteq H + a$ and $B \subseteq H + b$ for all $a \in A$, $b \in B$, and furthermore $|A|, |B| \geq K^{-C_8}|H|$.*

Observe that Exercise 2.3.7 is essentially the $K = 1$ case of this Proposition.

Proposition 2.27 gives a satisfactory characterization of pairs of sets with small Ruzsa distance, in terms of approximate groups, provided that one is ready to lose some absolute constants in the exponents. Note however that it is restricted to treating those sets $A$, $B$ which are comparable in magnitude up to powers of $K$ (cf. Exercise 2.3.6). A partial analogue of this proposition exists in the case when $A$ and $B$ are very different in magnitude, but the theory here is not as satisfactory; see Section 2.6.

## Exercises

2.4.1 Let $Z$ be a finite additive group, and let $A$ be a random subset of $Z$ such that the events $a \in A$ are independent with probability $3/4$ for all $a \in Z$. Show that with probability $1 - o_{|Z|\to\infty}(1)$, $|A| > |Z|/2$ (so in particular $A + A = A - A = Z$, by Exercise 2.1.6), but that it is not possible to cover $Z$ using fewer than $\frac{1}{10}\log|Z|$ translates of $A$. (Hint: if $X$ is an additive set with $|X| \leq \frac{1}{10}\log|Z|$, use Lemma 2.14 to find an additive set $Y$ with $|Y| = \Theta(|Z|/\log^2|Z|)$ such that the translates $y - X$ are disjoint for all $y \in Y$. Compute the probability that $A$ is disjoint from at least one of the sets $y - X$, and conclude an upper bound for the probability that $A + X = Z$. Now take the union bound over all choices of $X$.) This shows that we cannot replace $A - A$ by $A$ in Lemma 2.14 without admitting some sort of logarithmic loss.

2.4.2 Let $A$ be an additive set in a group $Z$, and let $\phi : Z \to Z'$ be a group homomorphism. Establish the inequalities

$$|A| \leq |\phi(A)| \sup_{x\in Z'} |A \cap \phi^{-1}(x)| \leq |2A|.$$

(Hint: use the Ruzsa covering lemma to cover $A$ by translates of a subset of $\phi^{-1}(0)$.) In particular equality is attained in both inequalities when $A$ is the coset of a group.

2.4.3 Prove Corollary 2.24. What value of the implicit constant in the $O()$ notation do you get?

2.4.4 Let $A$ be an additive set such that $|2A - 2A| < 2|A|$. Conclude that $A - A$ is a group. (Hint: use Lemma 2.14.) From this and Corollary 2.19 we see that if $|A - A| < 2^{1/5}|A|$, then $A - A$ is a group. The constant $2^{1/5}$ can be improved to $\frac{3}{2}$; see Exercise 2.6.5 below.

2.4.5 Let $G$ be a $K$-approximate group for some integer $K \geq 1$. Show that $|nG| \leq \binom{K+n-1}{n}|G|$ for all integers $n \geq 1$. Conclude in particular the bounds

$$|nG| \leq \min(K^n, n^{K-1})|G| \text{ for all } n \geq 1;$$

thus the numbers $|nG|$ grow exponentially in $n$ for $n \leq K$ but settle down to become polynomial growth for $n > K$. In fact for any additive set, $|nA|$ *is* a polynomial in $n$ for sufficiently large $n$; see [261] for a proof of this fact and some further discussion.

2.4.6 Let $A$ be an additive set with doubling constant $\sigma[A] = K$ for some $K \geq 1$. Show that

$$|nA| \leq \min(K^{Cn}, n^{K^C - 1})|A|$$

for all $n \geq 1$ and some absolute constant $C > 0$. (Note that if $K$ is very close to 1, then one can use Exercise 2.4.4 to obtain a much stronger bound.)

2.4.7 Let $G$ be a $K$-approximate group in an ambient group $Z$, and let $H$ be a $K'$-approximate group in $Z$. Show that $G + H$ is a $KK'$-approximate group. Show that $2G \cap 2H$ is a $(KK')^3$-approximate group. (Hint: first show that $(2G \cap 2H) - (2G \cap 2H) \subset (G + X) \cap (H + Y)$ for some $X, Y$ of cardinality at most $K^3$ and $(K')^3$ respectively, and then show that each set of the form $(G + x) \cap (H + y)$ is contained in a translate of $2G \cap 2H$.) Modify Exercise 2.2.9 to show that this type of statement fails quite badly if the set $2G \cap 2H$ is replaced by $G \cap H$. Also, establish the cardinality bounds

$$\frac{|G||H|}{|G + H|} \leq |2G \cap 2H| \leq \frac{1}{(KK')^3} \frac{|G||H|}{|G + H|}.$$

(Hint: use (2.8) for the lower bound, and the Ruzsa triangle inequality for the upper bound.) Conclude the estimates

$$d(G, H) \leq d(G, G + H) + d(G + H, H) \leq d(G, H) + \log KK'$$

and

$$d(G, H) \leq d(G, 2G \cap 2H) + d(2G \cap 2H, H) \leq d(G, H) + 3 \log KK',$$

and compare this with Exercise 2.3.11.

2.4.8 For each $j = 1, 2, 3$, let $G_j$ be a $K_j$-approximate group in an ambient group $Z$. Using the Ruzsa triangle inequality, show that

$$|G_1 + G_2 + G_3| \leq K_2 \frac{|G_1 + G_2||G_2 + G_3|}{|G_2|}.$$

Conclude that

$$d(G_1 + G_2, G_1 + G_2 + G_3) \leq d(G_2, G_2 + G_3) + \log K_1 K_2.$$