

Candidacy examination

Saúl Rodríguez

Research in metric geometry. GH distance

The *Hausdorff distance* between two subspaces A, B of a metric space (X, d_X) is

$$d_H^X(A, B) = \max \left(\sup_{a \in A} d_X(a, B), \sup_{b \in B} d_X(b, A) \right) \in [0, \infty].$$

The *Gromov-Hausdorff* (GH) distance between metric spaces (X, d_X) and (Y, d_Y) is

$$d_{\text{GH}}(X, Y) = \inf \left\{ d_H^Z(X', Y'); \begin{array}{l} (Z, d_Z) \text{ metric space,} \\ X', Y' \subseteq Z, \\ X' \xrightarrow{\text{isom}} X; Y' \xrightarrow{\text{isom}} Y \end{array} \right\}.$$

GH distance measures ‘how far two spaces are from being isometric’.

GH distances between spheres

Let \mathbb{S}^n be the unit n -sphere with the geodesic metric. What is the value of $d_{\text{GH}}(\mathbb{S}^n, \mathbb{S}^m)$, for each $n, m \in \mathbb{N}$?

It was already known (see [LMS,HJ]) that

$$d_{\text{GH}}(\mathbb{S}^1, \mathbb{S}^{2n}) = d_{\text{GH}}(\mathbb{S}^1, \mathbb{S}^{2n+1}) = \frac{(n-1)\pi}{2n} \text{ for all } n = 0, 1, 2, \dots$$

$$d_{\text{GH}}(\mathbb{S}^2, \mathbb{S}^3) = \frac{1}{2} \arccos\left(\frac{-1}{3}\right).$$

In [R1] we give new constructions which can be used to prove all the results above, and we use them to find the new value

$$d_{\text{GH}}(\mathbb{S}^3, \mathbb{S}^4) = \frac{1}{2} \arccos\left(\frac{-1}{4}\right).$$

This proves case $n = 3$ of the conjecture from [LMS] that

$d_{\text{GH}}(\mathbb{S}^n, \mathbb{S}^{n+1}) = \frac{1}{2} \arccos\left(\frac{-1}{n+1}\right)$ for all n (our method does not work for $n \geq 7$).

GH distances from \mathbb{S}^1 to simply connected spaces

A metric space (X, d_X) is called *geodesic* if between every two points $x, y \in X$ there is a path of length $d_X(x, y)$ (a geodesic).

Two examples of geodesic, simply connected spaces are intervals $I_x = [0, x]$ with their usual distance, and the spheres \mathbb{S}^n with their geodesic metric. It was proved in [LMS,Ka] that $d_{\text{GH}}(\mathbb{S}^1, \mathbb{S}^n) \geq \frac{\pi}{3}$ for all n and $d_{\text{GH}}(\mathbb{S}^1, I_x) \geq \frac{\pi}{3}$ for all $x \geq 0$.

In [LMO], Lim, Mémoli and Okutan proved that for any geodesic, simply connected space X we have $d_{\text{GH}}(\mathbb{S}^1, X) \geq \frac{\pi}{6}$, and they conjectured that in fact $d_{\text{GH}}(\mathbb{S}^1, X) \geq \frac{\pi}{3}$.

In [R3] we prove that we have $d_{\text{GH}}(\mathbb{S}^1, X) \geq \frac{\pi}{4}$ for all geodesic, simply connected spaces X , and that there is a metric tree E such that $d_{\text{GH}}(\mathbb{S}^1, E) = \frac{\pi}{4}$.

More generally, we prove the following:

Theorem

Let X, Y be geodesic spaces. Suppose there is a constant $D > 0$ such that $d_{\text{GH}}(X, Y) < D$ and all loops of diameter $< 4D$ are nullhomotopic in X and Y . Then $\pi_1(X)$ and $\pi_1(Y)$ are isomorphic.

Thesis project (ergodic Ramsey Theory)

Notions of density in \mathbb{N}

Densities are a way to measure the ‘size’ of a set of natural numbers. Given $A \subseteq \mathbb{N}$, we define:

$$\text{Upper density of } A: \overline{d}(A) = \limsup_{N \rightarrow \infty} \frac{|A \cap \{1, \dots, N\}|}{N}.$$

$$\text{Lower density of } A: \underline{d}(A) = \liminf_{N \rightarrow \infty} \frac{|A \cap \{1, \dots, N\}|}{N}.$$

If $\overline{d}(A) = \underline{d}(A)$, we denote them as $d(A)$, the *natural density* of A . For example, $d(\mathbb{N}) = 1$, $d(\{2n; n \in \mathbb{N}\}) = \frac{1}{2}$ and $d(\{\text{primes}\}) = 0$.

For all $A, B \subseteq \mathbb{N}$: $\overline{d}(A \cup B) \leq \overline{d}(A) + \overline{d}(B)$.

$$\overline{d}(A) = \overline{d}(A + 1).$$

Amenable groups

Let G be a countable group.

Left-Følner sequence in G : sequence of finite subsets $(F_N)_{N \in \mathbb{N}}$ of G (Følner sets), such that $\forall g \in G$

$$\lim_{N \rightarrow \infty} \frac{|gF_N \cap F_N|}{|F_N|} = 1.$$

We say G is *amenable* if it has a left-Følner sequence.

One can prove that all abelian groups (or more generally, all solvable groups) are amenable.

Some examples of Følner sequences:

- ▶ $F_N = \{1, \dots, N\}$ in \mathbb{Z} .
- ▶ $F_N = \{1, \dots, N\} \times \{1, \dots, 2^N\}$ in \mathbb{Z}^2 .
- ▶ $F_N = A_5$ in the alternating group A_5 .

An example of a countable, non-amenable group is the free group on two generators, F_2 .

Densities in amenable groups

From now, 'Fix $G, F = (F_N)_N$ ' means 'let G be a countable amenable group with a Følner sequence $F = (F_N)_N$ '.

Fix $G, (F_N)_N$. We define

Upper F -density of A : $\overline{d}_F(A) = \limsup_{N \rightarrow \infty} \frac{|A \cap F_N|}{|F_N|}$.

Lower F -density of A : $\underline{d}_F(A) = \liminf_{N \rightarrow \infty} \frac{|A \cap F_N|}{|F_N|}$.

If $\overline{d}_F(A) = \underline{d}_F(A)$, we denote them as $d_F(A)$, the *natural F-density* of A .

For all $A, B \subseteq G$: $\overline{d}_F(A \cup B) \leq \overline{d}_F(A) + \overline{d}_F(B)$.

$\overline{d}_F(A) = \overline{d}_F(gA)$ for all $g \in G$.

Measure preserving systems

A measure preserving system is an action of a (semi)-group on a measure space by measure-preserving transformations. More concretely:

By *m.p.s.* we will denote a quadruplet $(X, \mathcal{B}, \mu, (T_g)_{g \in G})$, where X is a set, G is a semigroup, $\mathcal{B} \subseteq \mathcal{P}(X)$ is a σ -algebra, $\mu : \mathcal{B} \rightarrow [0, 1]$ is a probability measure and $T_g : X \rightarrow X$ are measurable maps such that, for all $g, h \in G$:

- ▶ $T_g \circ T_h = T_{gh}$.
- ▶ T_g is measure-preserving: $\mu(T_g^{-1}(B)) = \mu(B) \quad \forall B \in \mathcal{B}$.

If $T : X \rightarrow X$ is a measure-preserving transformation, we call the m.p.s. (X, \mathcal{B}, μ, T) instead of $(X, \mathcal{B}, \mu, (T^n)_{n \in \mathbb{N}})$.

Translates in ergodic Ramsey theory

If $A \subseteq \mathbb{N}$, some statements about ‘patterns’ contained in A can be expressed using the translates of A .

Example 1. There are $a, b \in A$ such that $b - a$ is a nonzero perfect square iff $A \cap (A - n^2) \neq \emptyset$ for some $n \in \mathbb{N}$.

Example 2. A contains a nontrivial arithmetic progression of length k iff $(A - n) \cap \dots \cap (A - kn) \neq \emptyset$ for some $n \in \mathbb{N}$.

In particular, if $\overline{d}(A \cap (A - n^2)) > 0$ for some $n \in \mathbb{N}$, then A has square differences.

Furstenberg used these ideas to prove the following:

Szemerédi Theorem

Let $A \subseteq \mathbb{N}$ satisfy $\overline{d}(A) > 0$. Then for all $k \in \mathbb{N}$, A contains an arithmetic progression of length k .

Furstenberg's proof of Szemerédi's theorem

But what Furstenberg actually proved is the following:

Density Szemerédi Theorem (DST)

Let $A \subseteq \mathbb{N}$ satisfy $\overline{d}(A) > 0$. Then $\forall k \in \mathbb{N} \ \exists n \in \mathbb{N}$ such that

$$\overline{d}((A - n) \cap (A - 2n) \cap \cdots \cap (A - kn)) > 0.$$

But what Furstenberg *actually* proved is the following:

Ergodic Szemerédi Theorem (EST)

Let (X, \mathcal{B}, μ, T) be a measure-preserving system and let $C \in \mathcal{B}$ satisfy $\mu(C) > 0$. Then $\forall k \in \mathbb{N} \ \exists n \in \mathbb{N}$ such that

$$\mu(T^{-n}C \cap T^{-2n}C \cap \cdots \cap T^{-kn}C) > 0.$$

The key step to prove that the DST implies the EST is now known as Furstenberg's correspondence principle:

Furstenberg's correspondence principle (FCP)

Let $A \subseteq \mathbb{N}$. There is a m.p.s. (X, \mathcal{B}, μ, T) and $C \in \mathcal{B}$ such that $\mu(C) = \overline{d}(A)$ and, for all $n_1, \dots, n_k \in \mathbb{N}$,

$$\overline{d}_F((A - n_1) \cap \cdots \cap (A - n_k)) \geq \mu(T^{-n_1} C \cap \cdots \cap T^{-n_k} C).$$

The same result holds for any amenable group:

FCP for amenable groups ([Be97])

Fix $G, (F_N)_N$ and $A \subseteq G$. There is a m.p.s. $(X, \mathcal{B}, \mu, (T_g)_{g \in G})$ and $C \in \mathcal{B}$ with $\mu(C) = \overline{d}_F(A)$ such that for all $k \in \mathbb{N}$ and $h_1, \dots, h_k \in G$ one has

$$\overline{d}_F(h_1 A \cap \cdots \cap h_k A) \geq \mu(T_{h_1}(C) \cap \cdots \cap T_{h_k}(C)).$$

Moreover, for all $h_1, \dots, h_k \in G$ such that $d_F(h_1 A \cap \cdots \cap h_k A)$ is defined, we have

$$d_F(h_1 A \cap \cdots \cap h_k A) = \mu(T_{h_1}(C) \cap \cdots \cap T_{h_k}(C)).$$

Inverse Furstenberg correspondence principle

Moreover, for all $h_1, \dots, h_k \in G$ such that $d_F(h_1A \cap \dots \cap h_kA)$ is defined, we have

$$d_F(h_1A \cap \dots \cap h_kA) = \mu(T_{h_1}(C) \cap \dots \cap T_{h_k}(C)). \quad (1)$$

A natural question is then, given a measurable set C , can we obtain A satisfying Equation 1 for all $h_1, \dots, h_k \in G$? Yes, we can. The following is one of the main results of [R2]:

Theorem (Inverse FCP, [R2, Theorem 1.16])

Fix infinite G , $F = (F_N)_N$. For every m.p.s. $(X, \mathcal{B}, \mu, (T_g)_{g \in G})$ and every $C \in \mathcal{B}$ there exists a subset $A \subseteq G$ such that, for all $k \in \mathbb{N}$ and $h_1, \dots, h_k \in G$, we have

$$d_F(h_1A \cap \dots \cap h_kA) = \mu(T_{h_1}C \cap \dots \cap T_{h_k}C).$$

In particular, $d_F(h_1A \cap \dots \cap h_kA)$ is defined.

A first application of the inverse FCP

In [BF] it is asked whether, for fixed $G, (F_N)_N$, there is always a set $E \subseteq G$ such that $\overline{d}(E) > 0$ but for all finite $G_0 \subseteq G$, we have $\overline{d}_F(\cup_{g \in G_0} gE) < \frac{3}{4}$.

The answer is positive: consider some m.p.s. $(X, \mathcal{B}, \mu, (T_g)_{g \in G})$ and $C \in \mathcal{B}$, where

- ▶ $\mu(C) = \frac{1}{2}$.
- ▶ $T_g = \text{Id}_X$ for all $g \in G$.

Then by the inverse FCT, there is some subset A of G such that $d_F(A) = \mu(C) = \frac{1}{2}$ and for all $G_0 \subseteq G$ finite and nonempty,

$$\overline{d}_F(\cup_{g \in G_0} gE) = \mu(\cup_{g \in G_0} T_g C) = \mu(C) = \frac{1}{2}.$$

Cesaro averages of functions vs sequences.

Note that:

- ▶ Subsets C of X correspond to functions $\chi_C = f : X \rightarrow \{0, 1\}$, with $\mu(C \cap T_h^{-1}C) = \int_X f(x)f(T_hx)dx$.
- ▶ Subsets A of G correspond to sequences $(z_g)_{g \in G}$, where $z_g \in \{0, 1\} \forall g$, with $d(A \cap h^{-1}A) = \lim_N \frac{1}{|F_N|} \sum_{g \in F_N} z_g z_{hg}$.

We can change $\{0, 1\}$ by any compact subset of \mathbb{C} in the previous theorem and the inverse FCP will still hold true:

Theorem ([R2, Theorem 1.14] or [FT, Theorem 3.3])

Fix infinite G , $F = (F_N)_N$ and let $D \subseteq \mathbb{C}$ be compact. Then for any m.p.s. $(X, \mathcal{B}, \mu, (T_g)_{g \in G})$ and any measurable function $f : X \rightarrow D$ there is a sequence $(z_g)_{g \in G}$ of complex numbers in D such that, for all $j \in \mathbb{N}$ and $h_1, \dots, h_j \in G$,

$$\lim_N \frac{1}{|F_N|} \sum_{g \in F_N} z_{h_1g} \cdots z_{h_jg} = \int_X f(T_{h_1}x) \cdots f(T_{h_j}x) d\mu.$$

Some applications of the inverse FCP

Turning $[0, 1]$ -valued functions into sets

Let G be a countably infinite amenable group. For every m.p.s. $(X, \mathcal{B}, \mu, (T_g)_{g \in G})$ and every measurable $f : X \rightarrow [0, 1]$ there exists a m.p.s. $(Y, \mathcal{C}, \nu, (S_g)_{g \in G})$ and $A \in \mathcal{C}$ such that for all $k \in \mathbb{N}$ and all distinct $h_1, \dots, h_k \in G$ we have

$$\nu(S_{h_1}^{-1}A \cap \dots \cap S_{h_k}^{-1}A) = \int_X f(T_{h_1}(x)) \cdots f(T_{h_k}(x)) d\mu.$$

Question: Is the same true for non-amenable groups?

Some applications of the inverse FCP: vdC sets

Fix $G, (F_N)_N$. We say that a sequence $(x_g)_{g \in G}$ in \mathbb{R} is F -u.d. mod 1 if for every interval $(a, b) \subseteq (0, 1)$ we have

$$d_F(\{g \in G; x_g \in (a, b) \text{ mod } 1\}) = b - a.$$

Van der Corput sets

Fix $G, (F_N)_N$. We say a subset H of G is F -vdC if any sequence $(x_g)_{g \in G}$ in \mathbb{T} such that $(x_{hg} - x_g)_{g \in G}$ is F -u.d. mod 1 for all $h \in H$, is itself F -u.d. mod 1.

In [BL] it is asked whether, given two Følner sequences F_1 and F_2 in G , a subset H of G is F_1 -vdC iff it is F_2 -vdC. The answer is yes:

Theorem ([R2, Theorem 1.5])

Fix $G, (F_N)_N$. A set $H \subseteq G$ is F -vdC in G if and only if for any m.p.s. $(X, \mathcal{B}, \mu, (T_g)_{g \in G})$ and for any function $f \in L^\infty(\mu)$,

$$\int_X f(T_h(x)) \cdot \overline{f(x)} d\mu(x) = 0 \text{ for all } h \in H \text{ implies } \int_X f d\mu = 0.$$

Uniform density

Let G be countable, amenable. We say that $A \subseteq G$ has *uniform density* λ , $d_u(A) = \lambda$, if $d_F(A) = \lambda$ for all Følner sequences F in G .

Do we have an inverse FCP for uniform density? That is, given a m.p.s. $(X, \mathcal{B}, \mu, (T_g)_{g \in G})$, is there $A \subseteq G$ such that

$$d_u(h_1 A \cap \cdots \cap h_k A) = \mu(T_{h_1} C \cap \cdots \cap T_{h_k} C) \quad \forall h_1, \dots, h_k \in G?$$

Not in general: There are m.p.s.s (X, \mathcal{B}, μ, T) and $C \in \mathcal{B}$ such that $\mu(C) = \mu(C \cap T^{-1}(C)) = \frac{1}{2}$, but there is no $E \subseteq \mathbb{N}$ such that $d_u(E) = d_u(E \cap (E - 1)) = \frac{1}{2}$.

Question: Is the answer to the question above always positive if T is ergodic?

Partial result: if the m.p.s. is uniquely ergodic and $\mu(\partial C) = 0$, the answer is positive: one can take $A = \{g \in G; T^g x \in C\}$ for any $x \in X$ (see [BM22]).

Sumsets and difference sets

Let $A \subseteq \mathbb{Z}$. We define $A - A = \{a - b; a, b \in A\}$ and $A + A = \{a + b; a, b \in A\}$.

The following was proved by Bergelson in [Be84]:

Theorem

If $A \subseteq \mathbb{N}$ and $\overline{d}(A) = a > 0$, then there exists $B \subseteq \mathbb{N}$ such that $\overline{d}(B) > 0$ and $B + B \subseteq A - A$.

This leads to several questions. Firstly, can we achieve $d(B) > 0$ instead of $\overline{d}(B) > 0$? The answer is yes, as proved in [BR].

Secondly, how big can $\overline{d}(B)$ be? The proof from [Be84] gives us $\overline{d}(B) \geq \frac{a^4}{4}$.

Sumsets and difference sets

But a modification of the proof in [Be84] implies that

Theorem

If $A \subseteq \mathbb{N}$ and $\overline{d}(A) = a > 0$, then there exists $B \subseteq \mathbb{N}$ such that $\overline{d}(B) \geq a^2$ and $B + B \subseteq A - A$.

Is the constant a^2 optimal?

Question: Given $a > 0$, what is the biggest constant $\lambda(a)$ such that for all $A \subseteq \mathbb{N}$ with $\overline{d}(A) \geq a$ there is $B \subseteq \mathbb{N}$ such that $\overline{d}(B) \geq \lambda(a)$ and $B + B \subseteq A - A$?

Let us prove that $\lambda(a) \geq a^2$.

Some necessary lemmas

The following results are well known and we take them for granted:

Lemma (Corollary of ergodic theorems)

Let (X, \mathcal{B}, μ, T) be a m.p.s. and let $B \in \mathcal{B}$. Then

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \mu(B \cap T^{-n}B) \text{ exists and is at least } \mu(B)^2.$$

Intersectivity Lemma

Let (X, \mathcal{B}, μ) be a measure space and let $(A_n)_n$ be a sequence of measurable subsets of X and let $\lambda := \limsup_N \frac{1}{N} \sum_{n=1}^N \mu(A_n)$.

Then there is a set $E \subseteq \mathbb{N}$ with $\overline{d}(E) \geq \lambda$ such that any finite intersection of the sets A_e , $e \in E$, has positive measure.

Theorem

If $A \subseteq \mathbb{N}$ and $\overline{d}(A) = a > 0$, then there exists $B \subseteq \mathbb{N}$ such that $\overline{d}(B) \geq a^2$ and $B + B \subseteq A - A$.

Sketch of proof.

By the FCP, choose a m.p.s. (X, \mathcal{B}, μ, T) and $C \in \mathcal{B}$ such that $\mu(C) = \overline{d}(A) = a$ and $\mu(C \cap T^{-n}C) \leq \overline{d}(A \cap (A - n))$ for all $n \in \mathbb{N}$. We can assume that T is invertible.

Now, as $\mu(C) \geq a$ we have

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \mu(T^{-n}C \cap T^nC) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \mu(C \cap (T^2)^{-n}C) \geq a^2.$$

So letting $D_n = T^{-n}C \cap T^nC$, by the intersectivity lemma there is a set $B \subseteq \mathbb{N}$ such that $\overline{d}(B) \geq a^2$ and for all $b, c \in B$, $\mu(D_b \cap D_c) > 0$.

But $D_b \cap D_c \subseteq T^{-b}C \cap T^cC$, thus for all $b, c \in B$,

$$\overline{d}(A \cap (A - (b+c))) = \overline{d}((A-b) \cap (A+c)) \geq \mu(T^{-b}C \cap T^cC) > 0.$$

So $b+c \in A - A$, as we wanted. □

Using the same reasoning, one can obtain several modifications of the original theorem. In the last lines of [Be84] the following plausible statement is made (no proof was given):

Statement

Given $A \subseteq \mathbb{N}$ with $\overline{d}(A) = a > 0$, there is $B \subseteq \mathbb{N}$ with $\overline{d}(B) \geq \frac{a^4}{4}$ such that $b_1^2 + b_2^2 \in A - A$ for all $b_1, b_2 \in B$.

This would be true by the same proof if the following was true:

Statement

Given a m.p.s. (X, \mathcal{B}, μ, T) and $B \in \mathcal{B}$, we have

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \mu(B \cap T^{-n^2}B) \geq \frac{\mu(B)^4}{4}.$$

For $a > 0$, let $\delta_{n^2}(a)$ be the least possible value of

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \mu(B \cap T^{-n^2} B)$$

among all m.p.s. (X, \mathcal{B}, μ, T) and $B \in \mathcal{B}$ with $\mu(B) \geq a$.

Question: What is the growth of $\delta_{n^2}(a)$ in terms of a ? Is it polynomial? For small $a > 0$, the best bounds we have are

$$e(-a^{0.001}) \leq \delta_{n^2}(a) \leq a^{2.87555}.$$

Where 0.001 means $\varepsilon > 0$ and $2.87555 < \frac{\ln(12/205^2)}{\ln(12/205)}$.

Sumsets in difference sets: abelian groups

We can formulate a $B + B \subseteq A - A$ result for abelian groups:

Proposition

Fix (G, \cdot) , $(F_N)_N$ and let $A \subseteq G$ satisfy $\overline{d}_F(A) = a > 0$. Then there is some $B \subseteq G$ with $\overline{d}_F(B) \geq a^2$ and $BB \subseteq A^{-1}A$.

The proof is the same as for \mathbb{N} . However, that proof does not work for amenable groups.

Question: Is the proposition above true for any countable amenable group?

Countable fields. Double Følner sequences

Let $(Q, +, \cdot)$ be a countable field.

Definition

A *double Følner sequence* in Q is a sequence $F = (F_N)_N$ of finite subsets of a field such that

- ▶ F is a $(Q, +)$ -Følner sequence.
- ▶ $(F_N \setminus \{0\})_N$ is a (Q, \times) -Følner sequence.

Thus, if F is a double Følner sequence and $\overline{d}_F(A) > 0$, then A is 'large both additively and multiplicatively'.

Bergelson and Moreira proved that every countable field has a double Følner sequence.

$$B + B \subseteq A - A \text{ and } BB \subseteq A^{-1}A$$

By the results we have seen about sumsets in difference sets, we know that if F is a double Følner sequence in a countable field Q and $\overline{d}_F(A) > 0$, then there are sets B_+, B_\times such that

- ▶ $\overline{d}_F(B_+) > 0$ and $B_+ + B_+ \subseteq A - A$.
- ▶ $\overline{d}_F(B_\times) > 0$ and $B_\times B_\times \subseteq A^{-1}A$.

Question: Is there a set B such that $\overline{d}_F(B) > 0$ and we have both $B + B \subseteq A - A$ and $BB \subseteq A^{-1}A$?

A last open question about sumsets in difference sets is the following:

Question: Let $A \subseteq \mathbb{N}$ satisfy $\overline{d}(A) > 0$. Is there a set $B \subseteq \mathbb{N}$ with $\overline{d}(B) > 0$ and $B + B + B \subseteq A - A$?

Bergelson and Ruzsa proved in [BR] that for some sets A of positive density, there is no B such that $\overline{d}(B) > 0$ and $B + B - 2B \subseteq A - A$.