Lean Bourgain Extractor

Daniel Weber

May 12, 2024

Chapter 1

Additive Combinatorics

Lemma 1.1. *For any two sets A, B, we have* $|A - B| \leq \frac{|A+B|^3}{|A||B|}$

Proof. By the triangle inequality we have $|A - B| \leq \frac{|A+B||B+B|}{|B|}$, and from the Plünnecke-Ruzsa inequality we have $|B + B| \leq (\frac{|A+B|}{|A|})^2|A|$. □

Lemma 1.2. *For any set A and a non-zero value x, we have* $|xA| = |A|$

Proof. This is obvious from the bijection of multiplication by x. □

Lemma 1.3. *we have* $-(A \cap B) = -A \cap -B$

Proof. Trivial from the definitions. □

Lemma 1.4. *For any set A and two values a, b, we have* $(a + b)A \subseteq aA + bA$.

Proof. For any value $(a + b)v$ with $v \in A$ we have $av \in aA$, $bv \in bA$, and $av + bv = (a + b)v$ □

Lemma 1.5. *For any set A and two values a, b, we have* $(a - b)A \subseteq aA - bA$.

Proof. Exactly the same as the previous lemma. □

Lemma 1.6. *If $A \cap C \neq \emptyset$, we have* $|B + C| \leq \frac{|B+A||C+C|}{|A \cap C|}$.

Proof. By the triangle inequality, we have $|B + C| \leq \frac{|B+(A\cap C)||(A\cap C)+C|}{|A\cap C|}$, and this is less than $\frac{|B+A||C+C|}{|A\cap C|}$ because $B + (A \cap C) \subseteq B + A$ and $(A \cap C) + C \subseteq C + C$. □

Lemma 1.7. *For any three sets A, B, C, we have* $|A + B + C| \leq \frac{|C+A||A+B|^8}{|A|^6|B|^2}$

Proof. If either A or B are empty this is trivial. Otherwise we have an element $v \in B$. We obviously have $(A + B) \cap (A + \{v\}) = A + \{v\}$, and it is nonempty. So by 1.6 we have

$$|A+B+C| = |C+(A+B)| \leq \frac{|C + A + \{v\}||(A + B) + (A + B)|}{|A + \{v\}|} = \frac{|C + A||(A + B) + (A + B)|}{|A|}$$

By Ruzsa's covering lemma we have a set u of size $\leq \frac{|A+B|}{|B|}$ such that $A \subseteq u + B - B$. This gives $\frac{|C+A||(A+B)+(A+B)|}{|A|} \leq \frac{|C+A||(u+B-B+B)+(u+B-B+B)|}{|A|} = \frac{|C+A||2\cdot u+4\cdot B-2\cdot B|}{|A|} \leq \frac{|C+A||u|^2|4\cdot B-2\cdot B|}{|A|}$. By the Plünnecke-Ruzsa inequality we now have $|4 \cdot B - 2 \cdot B| \leq (\frac{|A+B|}{|A|})^6|A|$, and the result follows from this and the bound on $|u|$. □

Lemma 1.8. *We have that $Q(A, xA)$ for $x \neq 0$ is the number of quadruples $(a, b, c, d) \in A^4$ such that $a + xb = c + xd$.*

Proof. By a direct bijection from quadruples $(a, b, c, d) \in A \times (xA) \times A \times (xA)$ such that $a + b = c + d$. □

Chapter 2

Growth

Theorem 2.1. *For any set A over a finite field of size q there is a value $a \neq 0$ such that $|A + aA| \geq \frac{\min(|A|^2,q)}{2}$.*

Proof. First, we show it's sufficient for a to have $Q(A, aA) \leq |A|^2 + \frac{|A|^2(|A|^2-1)}{q-1}$. We have $|A + aA| \geq \frac{|A|^2|aA|^2}{Q(A,aQ)} \geq \frac{|A|^4}{|A|^2+\frac{|A|^2(|A|^2-1)}{q-1}}$. We need to show $\frac{x^2}{x+\frac{x(x-1)}{q-1}} \geq \frac{\min(x,q)}{2}$. If $x < q$ then

$$\frac{x^2}{x + \frac{x(x-1)}{q-1}} \geq \frac{x^2}{x + \frac{x^2}{x}} = \frac{x}{2}.$$

Otherwise, if $q \leq x$, we need to show

$$\frac{x^2}{x + \frac{x(x-1)}{q-1}} - \frac{q}{2} \geq 0.$$

By directly expanding, we have

$$\frac{x^2}{x + \frac{x(x-1)}{q-1}} - \frac{q}{2} = \frac{(q-2)(x-q)}{2(q+x-2)}$$

We have $2 \leq q$, so this value is nonnegative. Now to show that for some a, $Q(A, aA) \leq |A|^2 + \frac{|A|^2(|A|^2-1)}{q-1}$. Now we show it suffices to show that $\sum_{a\neq 0} Q(A, aA) \leq |A|^2(q-1) + |A|^2(|A|^2-1)$. This is because if all values were larger than $|A|^2 + \frac{|A|^2(|A|^2-1)}{q-1}$, the sum couldn't've been so small.

To show $\sum_{a\neq 0} Q(A, aA) \leq |A|^2(q-1) + |A|^2(|A|^2-1)$, we can use 1.8. The quadruples with $a = c, b = d$ contribute at most $|A|^2(q-1)$, and the other quadruples contribute at most $|A|^2(|A|^2-1)$, because they determine a unique a. □

Theorem 2.2. *For any set A in $\mathbb{F}_p$ (for p prime), we have $|3A^2 - 3A^2| \geq \frac{\min(|A|^2,p)}{2}$.*

Proof. If $|A| \leq 1$ then $|3A^2 - 3A^2| = |A|$, and this is greater than $|A|^2/2$. Otherwise, we split into cases by whether $\frac{A-A}{A-A}$ is the entire universe. If it is, then by 2.1 we have some value $v = (a-b)/(c-d)$ such that $|A+vA| \geq \frac{\min(|A|^2,p)}{2}$. By 1.2, we have $|A+vA| = |(c-d)A+(a-b)A|$.

Now $(c-d)A+(a-b)A$, by 1.5, this is a subset of $cA+aA-dA-bA$, which is a subset of $2A^2-2A^2$, and then $|3A^2-3A^2| = |A^2-A^2+2A^2-2A^2| \geq |2A^2-2A^2| \geq \frac{\min(|A|^2,p)}{2}$.

Otherwise, there must be some value such that $v=(a-b)/(c-d)$ such that $(a-b+c-d)/(c-d) = (a-b)/(c-d)+1 \notin \frac{A-A}{A-A}$. Because of that $|A+(a-b+c-d)/(c-d)A| = |A|^2$, so $|(c-d)A+(a-b+c-d)A| = |A|^2$. Using 1.5 and 1.4 we have $(c-d)A+(a-b+c-d)A \subseteq 3A^2-3A^2$, so $|3A^2-3A^2| \geq |A|^2 \geq \frac{|A|^2}{2}$. $\square$

Chapter 3

Stabilizer

Definition 3.1. $\mathrm{Stab}_K(A)$ *is the set* $\{x||A + xA| \leq K|A|\}$.

Lemma 3.2. *For* $a \in \mathrm{Stab}_K(A)$*, we also have* $a^{-1} \in \mathrm{Stab}_K(A)$.

Proof. If $a = 0$ this is trivial, otherwise by 1.2 we have $|A + a^{-1}A| = |a(A + a^{-1}A)| = |A + aA| \leq K|A|$. □

Lemma 3.3. *If* $A \neq \emptyset$ *and* $a \in \mathrm{Stab}_K(A)$ *then* $1 \leq K$.

Proof. Trivial. □

Lemma 3.4. *For* $a \in \mathrm{Stab}_K(A)$*, we also have* $a \in \mathrm{Stab}_{K^3}(A)$.

Proof. If $a = 0$ or $A = \emptyset$ this is trivial, otherwise by 1.1 and 1.2 we have

$$|A - aA| \leq \frac{|A + aA|^3}{|A||aA|} = \frac{|A + aA|^3}{|A|^2} \leq \frac{K^3|A|^3}{|A|^2} = K^3|A|$$

□

Lemma 3.5. *We have* $-\mathrm{Stab}_K(A) \subseteq \mathrm{Stab}_{K^3}(A)$.

Proof. Immediate from 3.4. □

Lemma 3.6. *For* $a \in \mathrm{Stab}_{K_1}(A), b \in \mathrm{Stab}_{K_2}(A)$*, we have* $a + b \in \mathrm{Stab}_{K_1^8 K_2}(A)$.

Proof. If $a = 0$ or $A = \emptyset$ this is trivial. Otherwise, we have $A + (a + b)A \subseteq A + aA + bA$, by 1.4, and by 1.7 and 1.2 we have $|A + aA + bA| \leq \frac{|A+bA||A+aA|^8}{|A|^8} \leq K_1^8 K_2|A|$. □

Lemma 3.7. *We have* $\mathrm{Stab}_{K_1}(A) + \mathrm{Stab}_{K_2}(A) \subseteq \mathrm{Stab}_{K_1^8 K_2}(A)$.

Proof. Immediate from 3.6. □

Lemma 3.8. *For* $n \in \mathbb{N}$ *we have* $(n + 1) \cdot \mathrm{Stab}_K(A) \subseteq \mathrm{Stab}_{K^{8n+1}}(A)$.

Proof. By induction with 3.7. □

Lemma 3.9. *We have* $\mathrm{Stab}_{K_1}(A) - \mathrm{Stab}_{K_2}(A) \subseteq \mathrm{Stab}_{K_1^8 K_2^3}(A)$.

Proof. Immediate from 3.7 and 3.5. □

Lemma 3.10. *For $a \in \operatorname{Stab}_{K_1}(A), b \in \operatorname{Stab}_{K_2}(A)$, we have $ab \in \operatorname{Stab}_{K_1K_2}(A)$.*

Proof. If $a = 0$ this is trivial with 3.3. Otherwise, we have, by 1.2 $|A + abA| = |a^{-1}A + bA|$. By the triangle inequality we have $|a^{-1}A + bA| \leq \frac{|A+a^{-1}A||A+bA|}{|A|}$, and using 3.2 we get that this is $\leq K_1K_2|A|$. □

Lemma 3.11. *We have $\operatorname{Stab}_{K_1}(A)\operatorname{Stab}_{K_2}(A) \subseteq \operatorname{Stab}_{K_1K_2}(A)$.*

Proof. Immediate from 3.10. □

Lemma 3.12. *If $a \in \operatorname{Stab}_K(A)$ and $K \leq K'$ then $a \in \operatorname{Stab}_{K'}(A)$.*

Proof. Trivial from the definition. □

Lemma 3.13. *If $K \leq K'$ then $\operatorname{Stab}_K(A) \subseteq \operatorname{Stab}_{K'}(A)$.*

Proof. Trivial from 3.12 □

Lemma 3.14. *If $1 \leq K$ implies $K \leq K'$ then $\operatorname{Stab}_K(A) \subseteq \operatorname{Stab}_{K'}(A)$.*

Proof. If $A = \emptyset$ this is trivial. Otherwise, if $K < 1$ then from 3.3 $\operatorname{Stab}_K(A) = \emptyset$ and this is trivial. Otherwise we get 3.13. □

Lemma 3.15. *We have $3\operatorname{Stab}_K(A)^2 - 3\operatorname{Stab}_K(A)^2 \subseteq \operatorname{Stab}_{K^{374}}(A)$.*

Proof. Immediate from 3.8, 3.9 and 3.11. □

Lemma 3.16. *We have $\frac{\min(|\operatorname{Stab}_K(A)|^2, p)}{2} \leq |\operatorname{Stab}_{K^{374}}(A)|$.*

Proof. Immediate from 3.15 and 2.2. □

Lemma 3.17. *If $4 \leq |\operatorname{Stab}_K(A)|$, then $\min(|\operatorname{Stab}_K(A)|^{\frac{3}{2}}, \frac{p}{2}) \leq |\operatorname{Stab}_{K^{374}}(A)|$.*

Proof. From direct calculation using 3.16. □

Lemma 3.18. *If $4 \leq |\operatorname{Stab}_K(A)|$ for all $n \in \mathbb{N}$, $\min(|\operatorname{Stab}_K(A)|^{\left(\frac{3}{2}\right)^n}, \frac{p}{2}) \leq |\operatorname{Stab}_{K^{374^n}}(A)|$.*

Proof. By induction on 3.17. □

Definition 3.19. $\operatorname{StabC}_2(\beta) = 374^{\lceil \log_{\frac{3}{2}}(1/\beta) \rceil}$

Lemma 3.20. *If $4 \leq |\operatorname{Stab}_K(A)|$ and $p^\beta \leq |\operatorname{Stab}_K(A)|$, then $\frac{p}{2} \leq |\operatorname{Stab}_{K^{\operatorname{StabC}_2(\beta)}}(A)|$.*

Proof. By setting $n = \operatorname{StabC}_2(\beta)$ at 3.18. □

Definition 3.21. $\operatorname{StabC}(\beta) = 9\operatorname{StabC}_2(\beta)$

Lemma 3.22. *If $4 \leq |\operatorname{Stab}_K(A)|$ and $p^\beta \leq |\operatorname{Stab}_K(A)|$, then $\operatorname{Stab}_{K^{\operatorname{StabC}(\beta)}}(A) = \mathbb{F}$.*

Proof. By Cauchy-Davenport and 3.7 after **??**. □

Lemma 3.23. *If $p^\beta \leq |A| \leq p^{1-\beta}$ and $K < \frac{p^\beta}{2}$, then $\operatorname{Stab}_K(A) \neq \mathbb{F}$.*

Proof. 2.1 gives a value a which by direct computation we can show isn't in $\operatorname{Stab}_K(A)$. □

Lemma 3.24. *If $4 \leq |\operatorname{Stab}_K(A)|, p^\beta \leq |\operatorname{Stab}_K(A)|, p^\gamma \leq |A| \leq p^{1-\gamma}$ then $\frac{p^\gamma}{2} \leq K^{\operatorname{StabC}(\beta)}$*

Proof. By applying 3.22 and 3.23. □

Chapter 4

Energy Growth

Theorem 4.1. *Let $S_1, S_2, \ldots, S_k \subseteq S$ be finite sets with $|S_i| \geq \delta|S|$ for all i. Then, there exists i such that $|\{j||S_j \cap S_i| \geq (\delta^2/2)k\}| \geq (\delta^2/2)k$*

Proof. This is exactly Claim 3.3.6 in [Dvi12]. □

Theorem 4.2. *Let A, T be finite sets with $Q(A, \lambda A) \geq \frac{|A|^3}{K}$ for all $\lambda \in T$. Then there exist sets A', T' with $\frac{|A|}{16K} \leq |A'|$ and $\frac{|T|}{2^{17}K^4} \leq |T'|$, such that $T' \subseteq \mathrm{Stab}_{2^{110}K^{42}}(A')$.*

Proof. This is exactly Theorem 3.3.5 in [Dvi12], using BSG from LeanAPAP. □

[Dvi12]: Dvir, Zeev. Incidence Theorems and Their Applications , now, 2012, doi: 10.1561/0400000056.

Chapter 5

Lines

TOOD: Figure out how to write blueprints about definitions

Definition 5.1. *A line over a field* $\mathbb{F}$ *is a linear subspace of* $\mathbb{F}^3$ *of dimension 2.*

Definition 5.2. *A point* $(x, y) \in \mathbb{F}^2$ *is in a line* L *iff* $(x, y, 1) \in L$.

Definition 5.3. *Given a linear isomorphism* P *and a line* L*, we have a line* PL.

Proof. This is a valid line because linear isomorphism preserves dimension. □

Lemma 5.4. *For any linear equivalence, applying it to lines is injective.*

Proof. From the injectivity of linear isomorphisms. □

Theorem 5.5. *Given a set* P *of points and a set* L *of lines, the number of incidences is at most* $\sqrt{|L||P|(|P| + |L|)}$.

TODO2

Chapter 6

Projective Transformations

TOOD: Figure out how to write blueprints about definitions

Definition 6.1. *Given two different values,* $(x_1, y_1), (x_2, y_2) \in \mathbb{F}^2, (x_1, y_1) \neq (x_2, y_2)$*, we get a linear isomorphism* A *such that* $A(x_1, y_1, 1) = (1, 0, 0)$ *and* $A(x_2, y_2, 1) = (0, 1, 0)$.

Lemma 6.2. *Given a point* p *not on the line between* $(x_1, y_1), (x_2, y_2)$*, the projective transformation defined by those points doesn't move it to infinity.*

Proof. Direct calculation. □

Chapter 7

Incidence

Definition 7.1. $C = C_2 + 1$

Definition 7.2. $\varepsilon(\beta) = \varepsilon_2(\beta)/3$

Theorem 7.3. *Let there be a set P of points and a set L of lines over a prime field, with $|P| \leq n, |L| \leq n$ and $p^{\beta} \leq n \leq p^{2-\beta}$. Then the number of intersections is at most $Cn^{\frac{3}{2}-\varepsilon(\beta)}$.*

Proof. We reduce this to 7.5, by removing all points contained in at most $n^{\frac{1}{2}-\varepsilon(\beta)}$ lines. This removes at most $n^{\frac{3}{2}-\varepsilon(\beta)}$ points, which is corrected for with $C = C_2 + 1$. □

Definition 7.4. $C_2 = \sqrt{2(C_3 + \frac{\sqrt{2}}{4})}$

Theorem 7.5. *Let there be a set P of points and a set L of lines over a prime field, with $|P| \leq n, |L| \leq n$ and $p^{\beta} \leq n \leq p^{2-\beta}$, and each point intersecting with at least $n^{\frac{1}{2}-\varepsilon(\beta)}$ lines. Then the number of intersections is at most $C_2 n^{\frac{3}{2}-\varepsilon(\beta)}$.*

Proof. We reduce this to 7.6, by removing all points contained in more than $4n^{\frac{1}{2}+\varepsilon(\beta)}$ lines. There can be at most $n^{1-2\,\varepsilon(\beta)}\frac{\sqrt{2}}{4}$ such points, by 5.5. Therefore, there are still many remaining points, and because each point has at least $n^{\frac{1}{2}-\varepsilon(\beta)}$ lines there are still many intersections. □

Theorem 7.6. *Let there be a set P of points and a set L of lines over a prime field, with $|P| \leq n, |L| \leq n$ and $p^{\beta} \leq n \leq p^{2-\beta}$, and each point contained in at least $n^{\frac{1}{2}-\varepsilon(\beta)}$ lines and at most $4n^{\frac{1}{2}+\varepsilon(\beta)}$. Then the number of intersections is at most $C_3 n^{\frac{3}{2}-\varepsilon_2(\beta)}$.*

Proof. We use **??** to claim that there exist two points, a, b such that for a large number of points they are both on a line from a and a line from b. We only keep those, and because all points are contained in $n^{\frac{1}{2}-\varepsilon(\beta)}$ lines there are still many intersections. Then we remove all points on the line between a and b. Because all lines, expect maybe one, intersect at most one such point, this step doesn't remove many intersections. Now we can apply 7.7. □

Theorem 7.7. *Let there be a set P of points and a set L of lines over a prime field, with $|P| \leq n, |L| \leq n$ and $p^{\beta} \leq n \leq p^{2-\beta}$, two different points p_1, p_2, which are both contained in at most $4n^{\frac{1}{2}+\varepsilon(\beta)}$ lines, with no points in P on the line p_1p_2, and all points in P on an intersection of some line from p_1 and some line from p_2. Then the number of intersections is at most $C'n^{\frac{3}{2}-\varepsilon'(\beta)}$.*

Proof. By 6.1 we can reduce this to 7.8. TODO. □

Theorem 7.8. *Let there be two sets* A, B *and a set* L *of lines over a prime field, with* $|A| \leq 4n^{\frac{1}{2}+2\,\varepsilon(\beta)}, |B| \leq 4n^{\frac{1}{2}+2\,\varepsilon(\beta)}, |L| \leq n$ *and* $p^{\beta} \leq n \leq p^{2-\beta}$*. Then the number of intersections is at most* $C'n^{\frac{3}{2}-\varepsilon\text{'}(\beta)}$*.*

Proof. We reduce to 7.9 by removing all lines which contain too few points. □

Theorem 7.9. *Let there be two sets* A, B *and a set* L *of lines over a prime field, with* $|A| \leq 4n^{\frac{1}{2}+2\,\varepsilon(\beta)}, |B| \leq 4n^{\frac{1}{2}+2\,\varepsilon(\beta)}, |L| \leq n$ *and* $p^{\beta} \leq n \leq p^{2-\beta}$*. Additionally, suppose there are at least* $n^{\frac{1}{2}-\varepsilon\text{'}(\beta)}$ *points on each line. Then the number of intersections is at most* $C_2'n^{\frac{3}{2}-\varepsilon\text{'}(\beta)}$*.*

Proof. We now remove all horizontal lines, to reduce to 7.10. This doesn't remove many intersections because each point can intersect at most one horizontal line. □

Theorem 7.10. *Let there be two sets* A, B *and a set* L *of non-horizontal lines over a prime field, with* $|A| \leq 4n^{\frac{1}{2}+2\,\varepsilon(\beta)}, |B| \leq 4n^{\frac{1}{2}+2\,\varepsilon(\beta)}, |L| \leq n$ *and* $p^{\beta} \leq n \leq p^{2-\beta}$*. Additionally, suppose there are at least* $n^{\frac{1}{2}-\varepsilon\text{'}(\beta)}$ *points on each line. Then the number of intersections is at most* $C_2'n^{\frac{3}{2}-\varepsilon\text{'}(\beta)}$*.*

Proof. We apply **??** to get two values $b_1, b_2 \in B$ such that many lines pass through these rows. Because there are many points on each line, only keeping those still gives many incidences. Now, a line can be described as two points a_1, a_2, and the line would be the line passing through $(a_1, b_1), (a_2, b_2)$. Suppose it passes through a given point (a, b). This gives $a = \frac{b_2-b}{b_2-b_1}a_1 + \frac{b-b_1}{b_2-b_1}a_2$, so $\frac{b_2-b}{b_2-b_1}a_1 + \frac{b-b_1}{b_2-b_1}a_2 \in A$. Equivalently, there are many $(N^{3/2-\epsilon})$ triplets $(b, a_1, a_2) \in B \times A \times A$ such that $\frac{b_2-b}{b_2-b_1}a_1 + \frac{b-b_1}{b_2-b_1}a_2 \in A$. This implies that there must be many $(N^{1/2-\epsilon})$ values of b such that there is a large number of pairs (a_1, a_2) with this property. Now we can only keep those, remove b_1, b_2, and apply 7.11 □

Theorem 7.11. *Let there be two sets* A, B *and a set* L *of non-horizontal lines over a prime field, with* $|A| \leq 4n^{\frac{1}{2}+2\,\varepsilon(\beta)}, |B| \leq 4n^{\frac{1}{2}+2\,\varepsilon(\beta)}, |L| \leq n$ *and* $p^{\beta} \leq n \leq p^{2-\beta}$*. Suppose there are at least* $n^{\frac{1}{2}-\varepsilon\text{'}(\beta)}$ *points on each line, and lastly, suppose there are two values* $b_1, b_2 \notin B$*, TODO. Then* $|B|$ *is at most* $C_5'n^{1/2-\varepsilon\text{'}_2(\beta)-\varepsilon\text{'}(\beta)-4\,\varepsilon(\beta)}$*.*

Proof. TODO □

Chapter 8

Transfer operator

Definition 8.1. *For $f : A \to B, G : A \to C$ we have $f\#g$ is a function $B \to C$ defined by $f\#g(x) = \sum_{f(y)=x} g(y)$.*

Proposition 8.2. *We have $f\#(g+h) = f\#g + f\#h$.*

Proposition 8.3. *We have $f\#(g-h) = f\#g - f\#h$.*

Proposition 8.4. *If h is an additive homomorphism we have $h \circ (f\#g) = f\#(g \circ h)$.*

Proposition 8.5. *If f is a bijection we have $(f\#g)(x) = g(f^{-1}(x))$.*

Lemma 8.6. *We have $h\#(f\#g) = (h \circ f)\#g$.*

Proof.

$$\sum_{y \in h^{-1}(x)} \sum_{z \in f^{-1}(y)} g(z) = \sum_{z} \sum_{y \in h^{-1}(x), z \in f^{-1}(y)} g(z) = \sum_{z} [h(f(z)) = x] g(z) = \sum_{z \in (h \circ f)^{-1}(x)} g(z) = ((h \circ f)\#g)(x)$$

□

Proposition 8.7. $\mathrm{id}\#f = f$

Proposition 8.8.

$$\sum_{x} (f\#g)(x)h(x) = \sum_{x} g(x)h(f(x))$$

Lemma 8.9.

$$E[(f\#g)(x)h(x)] = \frac{|A|}{|B|} E[g(x)h(f(x))]$$

Proof. By unfolding the expectation and using 8.8. □

Proposition 8.10. *if $(f\#g)(x) \neq 0$ then $\exists y, f(y) = x$.*

Chapter 9

Finite Probability Distributions

Definition 9.1. *A finite probability distribution is a function $f : A \to \mathbb{R}$ from a finite type A, such that f is nonnegative and the sum of f is 1.*

Definition 9.2. *The uniform distribution on a nonempty set A, $\text{Uniform}(A)$, assigns $\frac{1}{|A|}$ to all values in A and 0 to other values.*

Definition 9.3. *Given two finite probability distributions $f : A \to \mathbb{R}, g : B \to \mathbb{R}$, we have a probability distribution from $A \times B$ defines as $(f \times g)(x, y) = f(x)g(y)$.*

Definition 9.4. *Given a finite probability distribution $f : A \to \mathbb{R}$ and a function $g : A \to B$, we can apply g to the random variable represented by f. This gives the distribution $g\#f$.*

We can directly transfer all theorems on $f\#g$ to finite PMFs.

Definition 9.5. *Given two finite probability distributions $f : A \to \mathbb{R}, g : A \to \mathbb{R}$, we have a probability distribution defines as $f - g = s\#(f \times g)$ with $s(x, y) = x - y$.*

Definition 9.6. *Given two finite probability distributions $f : A \to \mathbb{R}, g : A \to \mathbb{R}$, we have a probability distribution defines as $f + g = a\#(f \times g)$ with $a(x, y) = x + y$.*

Definition 9.7. *Given a finite probability distribution $f : A \to \mathbb{R}$, we have a probability distribution defines as $-f = n\#f$ with $n(x) = -x$.*

Proposition 9.8. *These operations define a commutative monoid.*

Lemma 9.9. *We have $(f\#a) \times (g\#b) = h\#(a \times b)$, with $h(x, y) = (f(x), g(y))$.*

Proof. By calculation. □

Lemma 9.10. *We have $f\#(a \times b) = b \times a$ for $f(x, y) = (y, x)$.*

Proof. Simple application of 8.5 □

Lemma 9.11. *We have $(f\#a) + (g\#b) = h\#(a \times b)$, with $h(x, y) = f(x) + g(y)$.*

Proof. By simplification after 9.9. □

Definition 9.12. *Given a finite probability distribution $f : A \to \mathbb{R}$ and a list of finite probability distributions on B, indexed by elements of A, g, we can define $g(f)$ as the probability distribution obtained by sampling an element from f, and then sampling an elemente from the corresponding distribution in g.*

Lemma 9.13. *We have $f(g(a)) = h(a)$ with $h(x) = g(f(x))$.*

Proof. By calculation. □

Lemma 9.14. *We have $g\#f(a) = h(a)$ with $h(x) = g\#f(x)$.*

Proof. By calculation. □

Definition 9.15. *We say that a distribution a is ε-close to N entropy if for all sets $|A| \leq N$, $\sum_{x\in A} a(x) \leq \varepsilon$. Note that this is a bit different than the usual definition.*

Proposition 9.16. *If a is ε-close to $\lfloor n \rfloor$ entropy it's also ε-close to n entropy.*

Proposition 9.17. *If a is ε_1-close to n entropy and $\varepsilon_1 \leq \varepsilon_2$ it's also ε_2-close to n entropy.*

Lemma 9.18. *If e is an isomorphism and a is ε-close to n entropy, $e\#a$ is also ε-close to n entropy.*

Proof. By definition, after using 8.5. □

Lemma 9.19. *If a is ε-close to n entropy, then for any PMF b, $a+b$ is also ε-close to n entropy.*

Proof.

$$\sum_{x\in H}(a+b)(x) = \sum_{x\in H}\sum_{v} b(v)a(x-v) = \sum_{v} b(v)\sum_{x\in H} a(x-v) = \sum_{v} b(v)\sum_{x\in H-v} a(x) \leq \sum_{v} b(v)\varepsilon = \varepsilon$$

□

Proposition 9.20. *If, for all x such that $0 < f(x)$, we have that $g(x)$ is ε-close to n entropy, then $g(f)$ is ε-close to n entropy.*

Proposition 9.21. *For any probability distribution a, there are at most n values such that $a(x) > 1/n$.*

Chapter 10

Lemmas about LP Norm

Theorem 10.1. *For a function f with domain A*

$$\|f\|_{\ell^1} \leq \sqrt{|A|}\|f\|_{\ell^2}$$

Proof. This is a particular case of the Cauchy-Schwartz inequality. □

Lemma 10.2. *For a function f with domain A*

$$\|f\|_{\ell^p} = |A|^{1/p}\|f\|_{L^p}$$

Proof. Trivial from the definition of $\|\cdot\|_{L^p}$. □

Lemma 10.3.

$$\|f\|_{\ell^p} \leq |A|^{1/p}\|f\|_{\ell^\infty}$$

Proof.

$$(\sum_x |f(x)|^p)^{1/p} \leq (\sum_x \|f\|_{\ell^\infty}^p)^{1/p} = (|A|\|f\|_{\ell^\infty}^p)^{1/p} = |A|^{1/p}\|f\|_{\ell^\infty}$$

. □

Lemma 10.4. *Note that in this lemma $\langle f, g\rangle$ is $\sum_x f(\bar{x})g(x)$.*

$$|\langle f, g\rangle| \leq \|f\|_{\ell^1}\|g\|_{\ell^\infty}$$

Proof.

$$|\sum_x f(\bar{x})g(x)| \leq \sum_x |f(\bar{x})g(x)| \leq \sum_x |f(x)|\|g\|_{\ell^\infty} = \|f\|_{\ell^1}\|g\|_{\ell^\infty}$$

□

Lemma 10.5.

$$\|a\|_{\ell^2} \leq \sqrt{\|a\|_{\ell^1}\|a\|_{\ell^\infty}}$$

Proof. Trivial with 10.4 and $\|a\|_{\ell^2} = \sqrt{\langle a, a\rangle}$ □

Chapter 11

XOR Lemma

Most of the material in here was taken from [Rao07].

Theorem 11.1. *For a function f with domain A,*

$$\|f\|_{\ell^1} \le |A|^{3/2} \|\hat{f}\|_{\ell^\infty}$$

Proof. By 10.1 we have $\|f\|_{\ell^1} \le \sqrt{|A|}\|f\|_{\ell^2}$. Then using 10.2 this is $|A|\|f\|_{L^2}$. By Parseval's theorem, this is $|A|\|\hat{f}\|_{\ell^2}$. By 10.3, we have $\|\hat{f}\|_{\ell^2} \le \sqrt{|A|}\|\hat{f}\|_{\ell^\infty}$, which combines to the desired conclusion. □

Lemma 11.2. *This is a very slight generalization of Lemma 4.3 in [Rao07]:*

Let G, H be finite abelian groups. Let X be a function $G \to \mathbb{R}$ such that for every nontrivial character χ, $\hat{X}(\chi) \le \frac{\varepsilon}{|G|}$ and let U be the function with constant value $E_x[X(x)]$. Let $\sigma : G \to H$ be a function such that for every character ϕ, we have $\|\widehat{\phi \circ \sigma}\|_{\ell^1} \le \tau$. Then $\|\sigma\#X - \sigma\#U\|_{\ell^1} \le \tau\varepsilon\sqrt{|H|}$

Proof. The proof is identical to the proof in [Rao07], using 11.1. □

Lemma 11.3. *If a, b, n are reals, b, n are positive, and $\frac{a}{b} \le n$, then $\frac{a}{b} \le \frac{a+1}{b+1/n}$.*

Proof. By direct calculation (alternatively, this can be seen as an instance of the mediant inequality). □

Lemma 11.4. *For a real x, we have $2 - |4x - 2| \le |e^{x2\pi i} - 1|$.*

Proof. We have $|e^{x2\pi i} - 1| = |\cos(2\pi x) - 1 + i\sin(2\pi x)| = \sqrt{(\cos(2\pi x) - 1)^2 + \sin^2(2\pi x)} = \sqrt{2 - 2\cos(2\pi x)}$. WLOG, it's sufficient to consider the range $0 \le x \le \frac{1}{2}$. In this range, we have the inequality $\cos(2\pi x) \le 1 - \frac{2}{\pi^2}(2\pi x)^2 = 1 - 8x^2$, from which the result quickly follows. □

In the following, we consider $\sigma : \mathbb{Z}_N \to \mathbb{Z}_M$ defined as $\sigma(x) = x \bmod M$.

Lemma 11.5. *We have $\|\sigma\#U - U\|_{\ell^1} \le \frac{n}{m}$.*

Proof. We can easily bound each difference by $\frac{1}{n}$ using $(\sigma\#U)(x) = \frac{\lceil \frac{N-(x \bmod M)}{M} \rceil}{N}$ and $U(x) = \frac{\frac{N}{M}}{N}$. □

Theorem 11.6. *This is Lemma 4.4 in [Rao07] with explicit constants:*
For any character χ *of* $\mathbb{Z}_M$, $\|\widehat{\chi \circ \sigma}\|_{\ell^1} \leq 6\ln(N) + 6$

Proof. Let $\rho(x) = e^{x2\pi i}$. We can find a value w such that $\chi(x) = \rho(wx/M)$. Then $\chi(\tau(x)) = \rho(wx/M)$. Now we have

$$\|\widehat{\chi \circ \sigma}\|_{\ell^1} = \frac{1}{N}\sum_{t\in\mathbb{Z}_N} |\sum_{x\in\mathbb{Z}_N} \rho(wx/M)\rho(-tx/N)| = \frac{1}{N}\sum_{t\in\mathbb{Z}_N} |\sum_{x\in\mathbb{Z}_N} \rho(\frac{wN-tM}{NM})^x|$$

We now want to claim $|\sum_{x\in\mathbb{Z}_N} \rho(\frac{wN-tM}{NM})^x| \leq \frac{|\rho(\frac{wN-tM}{NM})^N-1|+1}{|\rho(\frac{wN-tM}{NM})-1|+1/N}$ If $\rho(\frac{wN-tM}{NM}) = 1$, this is trivially correct. Otherwise, this is a geometric sum, and then we can use 11.3. We easily have $|\rho(\frac{wN-tM}{NM})^N - 1| + 1 \leq 3$, and now we need to bound $\frac{1}{N}\sum_{t\in\mathbb{Z}_N} \frac{1}{|\rho(\frac{wN-tM}{NM})-1|+1/N} = \frac{1}{N}\sum_{t\in\mathbb{Z}_N} \frac{1}{|\rho(\langle\frac{wN/M-t}{N}\rangle)-1|+1/N}$. We can use 11.4 to bound this as $\frac{1}{N}\sum_{t\in\mathbb{Z}_N} \frac{1}{(2-|4(\langle\frac{wN/M-t}{N}\rangle)-2|)+1/N}$ By writing $wN/M = \lfloor wN/M \rfloor + \langle wN/M\rangle$, this is equal to $\sum_{t\in\mathbb{Z}_N} \frac{1}{2N-|4(\langle wN/M\rangle+t)-2N|+1}$ Now by splitting to cases and calculating we can see that $\frac{1}{2N-|4(\langle wN/M\rangle+t)-2N|+1} \leq \frac{1}{4t+1} + \frac{1}{4(n-1-t)+1}$. Applying bonuds on the harmonic sum, we get the desired result. ☐

Theorem 11.7. *Let* X *be a distribution* $\mathbb{Z}_N$ *such that for every nontrivial character* χ, $\hat{X}(\chi) \leq \frac{\varepsilon}{|G|}$. *Then* $\mathrm{SD}(\sigma\#X, U) \leq \varepsilon\sqrt{M}(3\ln(N)+3) + \frac{M}{2N}$.

Proof. Trivial with $\mathrm{SD}(A,B) = \|A-B\|_{\ell^1}$, the triangle inequality with 11.5, 11.2 and 11.6. ☐

[Rao07]: Rao, Anup. "An Exposition of Bourgain's 2-Source Extractor." Electron. Colloquium Comput. Complex. TR07 (2007): n. pag.

Chapter 12

Lemmas about the Inner Product Extractor

Proposition 12.1. *For a character χ, $\chi(a) = \chi(b)$ iff $\chi(a-b) = 1$.*

Proposition 12.2. *The inner product is commutitive.*

Lemma 12.3. *If χ is a non-trivial character of a field $\mathbb{F}$, then there is an injective function from elements of $\mathbb{F}^2$ (generalize this to any dimension) to characters of it, defined by $f(x)(y) = \chi(x \cdot y)$.*

Proof. It's easy to see this maps values to additive characters. For injectivity, we have some value x such that $\chi(x) \neq 1$. Now if $f((a_1, a_2)) = f((b_1, b_2))$, if they aren't equal, we can apply either $\frac{x}{a_1 - b_1}$ or $\frac{x}{a_2 - b_2}$, and then we get $\chi(x) = 1$ by 12.1, a contradiction. □

Lemma 12.4. *The function in the previous lemma is actually a bijection.*

Proof. By 12.3 and the cardinality being equal. □

Theorem 12.5.

Note: the inner product and DFT here aren't normalized.

$$\sum_x a(x) \sum_y b(y)\chi(x \cdot y) = \langle a, P(\hat{b}) \rangle$$

where P reorders $\hat{b}$ based on 12.4

Proof. TODO □

Theorem 12.6.

$$|\sum_x a(x) \sum_y b(y)\chi(x \cdot y)|^2 \leq |A|^2 \|a\|_{\ell^2}^2 \|b\|_{\ell^2}^2$$

Proof. We use 12.5 to rewrite the sum, and then use Cauchy-Schwartz. Then we can undo the reordering and use Parseval's theorem to get the desired result. □

Theorem 12.7.

$$|\sum_x a(x) \sum_y b(y)\chi(x \cdot y)| \leq |A| \|a\|_{\ell^2} \|b\|_{\ell^2}$$

Proof. Simplying apply a square root to 12.6. □

Theorem 12.8. *For any bilinear form F and character χ,*

$$|\sum_x a(x) \sum_y b(y)\chi(F(x,y))|^2 \leq |\sum_x a(x) \sum_y (b-b)(y)\chi(F(x,y))|$$

Proof.

$$\begin{aligned}
|\sum_x a(x) \sum_y b(y)\chi(F(x,y))|^2 \leq & \quad (\sum_x a(x)|\sum_y b(y)\chi(F(x,y))|)^2 && (12.1)\\
\leq & \quad \sum_x a(x)|\sum_y b(y)\chi(F(x,y))|^2 && (12.2)\\
= & \quad \sum_x a(x)(\sum_y b(y)\chi(F(x,y)))(\sum_y b(y)\bar{\chi}(F(x,y))) && (12.3)\\
= & \quad \sum_x a(x) \sum_y \sum_{y'} b(y)b(y')\chi(F(x,y))\chi(-F(x,y')) && (12.4)\\
= & \quad \sum_x a(x) \sum_y \sum_{y'} b(y)b(y')\chi(F(x,y-y')) && (12.5)\\
= & \quad \sum_x a(x) \sum_y (b-b)(y)\chi(F(x,y)) && (12.6)\\
& && (12.7)
\end{aligned}$$

□

Theorem 12.9. *For any bilinear form F and character χ,*

$$|\sum_x a(x) \sum_y b(y)\chi(F(x,y))| \leq \sqrt{|\sum_x a(x) \sum_y (b-b)(y)\chi(F(x,y))|}$$

Proof. Trivial from 12.8. □

Theorem 12.10. *If a and b are ε-close to N entropy, then*

$$|\sum_x a(x) \sum_y b(y)\chi(F(x,y))| \leq \frac{|A|}{N} + 2\varepsilon$$

Proof. From the hypothesis and 9.21 we can look at $a'(x) = \begin{cases} a(x) & a(x) \leq \frac{1}{N} \\ 0 & \frac{1}{N} < a(x) \end{cases}$, and similarly for b', and the difference would be at most 2ε. Then we can apply 12.7 to get the result. □

Chapter 13

Bourgain Extractor

Definition 13.1. *Given a distribution A on $\mathbb{F}$, and a distribution B on $\mathbb{F}^3$, we define a distribution $L(A, B)$ by sampling x from A, sampling (y, z, w) from B, and outputting $(x+y, z(x+y)+w)$.*

Lemma 13.2. *We have $L(f(A), g(B)) = L'(A \times B)$ with $L'(x, y) = L(f(x), g(y))$.*

Proof. Trivial with **??** and 9.14. ☐

Theorem 13.3. *Given an integer N and a real number β such that $p^\beta \leq N \leq p^{2-\beta}$, and two nonempty sets $A' \subseteq \mathbb{F}, B' \subseteq \mathbb{F}^3$, such that $|B'| \leq N$ and the last two values in every element of B' are unique, then $L(\text{Uniform}(A'), \text{Uniform}(B'))$ is $\frac{C}{|A'||B'|} N^{3/2-\varepsilon(\beta)}$-close to N entropy.*

Proof. TODO ☐

Theorem 13.4. *TODO*

Proof. TODO ☐

Theorem 13.5. *TODO*

Proof. TODO ☐

Definition 13.6. $M(x, y) = (x + y, 2(x + y), -((x + y)^2 + x^2 + y^2))$

Definition 13.7. $D(x, y) = (x, x^2 - y)$.

Lemma 13.8. $f\#(b \times b \times b) = D\#L(b, M\#(b \times b))$*, with* $f(x, y, z) = (x + y + z, x^2 + y^2 + z^2)$.

Proof. By direct calculation with 9.9, 8.6, 9.10. ☐

Lemma 13.9. *If the maximum value of a is ε, the maximum value of $M\#(a \times a)$ is at most $2\varepsilon^2$.*

Proof. It suffices to show that every value can be obtained at most twice as an output of M. Because the first value determines the second one, we can drop it, and then if want to get (x_1, x_2) we need $y_1 + y_2 = x_1, y_1 y_2 = x_1^2 + x_2/2$ (by calculation). A calculation can further show that $(x_1, x_2) \to -x_1$ is a bijection from this to the set of roots of $y^2 + x_1 y + (x_1^2 + x_2/2)$, which is easily of size at most 2. ☐

Definition 13.10. $\beta = \frac{35686629198734976}{35686629198734977}$.

Definition 13.11. $\alpha = \varepsilon(\beta)$

Lemma 13.12. $\alpha = \frac{11}{2}(1 - \beta)$.

Proof. By calculation. □

Lemma 13.13. *For any source a with maximum value at most $p^{-1/2+2/11\alpha}$, $D\#L(a, M\#(a\times a))$ is $8Cp^{-2/11\alpha}$-close to $p^{1+2/11\alpha}$ entropy.*

Proof. First, by 9.18, we can get rid of the D. Now we want to apply 13.5. We already have a bound for the maximum value of a, and using 13.9 we get a bound for the maximum value of $M\#(a \times a)$. The last two values of a triple in the support $M\#(a \times a)$ is an injective function by 8.10, as the first value is half of the second value for triples in the domain of M. □

Definition 13.14. $C_b = \sqrt[64]{16C + 1}$.

Theorem 13.15. *For any two sources a, b with maximum value at most $p^{-1/2+2/11\alpha}$, and any non-trivial character χ,*

$$|\sum_x a(x) \sum_y b(y)\chi(xy + x^2y^2)| \leq C_b p^{-1/352\alpha}$$

Proof. First define $a' = f\#a, b' = f\#b$ for $f(x) = (x, x^2)$, then this is $|\sum_x a'(x) \sum_y b'(y)\chi(x \cdot y)|$ Applying 12.9 3 times, then swapping x, y and doing it three more times, we can bound this by $|\sum_x(b' + b' + b' + (b' - b' - b' - b' - b'))(x) \sum_y(a' + a' + a' + (a' - a' - a' - a' - a'))(y)\chi(x \cdot y)|^{1/64}$ Now we want to use 12.10. By 9.19, it suffices to show that $b' + b' + b'$ and $a' + a' + a'$ are close to high entropy. First, we can rewrite this by unfolding a' and b', using 9.11 and then 13.8. Finally, what we want is 13.13. □

Theorem 13.16. *For any positive integer m and two sources a, b with maximum value at most $p^{-1/2+2/11\alpha}$, the statistical distance of $f\#(a \times b)$ with $f(x, y) = (xy + x^2y^2 \bmod p) \bmod m$ to the uniform distribution is at most $\varepsilon = C_b p^{-1/352\alpha}\sqrt{m}(3\ln(p) + 3) + \frac{m}{2p}$.*

Proof. This is a simple application of 11.7 with 13.15 □

Theorem 13.17. *For any positive integer m, the function $f(x, y) = (xy + x^2y^2 \bmod p) \bmod m$ is a two source extractor, with $k = (1/2 - 2/11\alpha)\log(p), \varepsilon = C_b p^{-1/352\alpha}\sqrt{m}(3\ln(p) + 3) + \frac{m}{2p}$.*

Proof. This is a simple restatement of 13.16 □