Math threads

Contents

Introduction

The goal of this document is to

1. Keep track of my own thoughts about math, and in particular save partial progress.

2. Provide links to useful references.

3. Write up open-source notes about subjects that I learn.

1 Math thoughtstream

I'm going to catalogue all the math-related thoughts I have every day here (like a math thoughtstream `http://www.workflowy.com`). (This is inspired partly by Jacob Cole's idea of a "curiosity thread," `http://curiositythread.tk/`.) I find myself running into a few problems when I learn math:

1. I note interesting questions, and then forget about them if they don't seem pressing enough, or I misplace them.

2. I take down notes, and don't bring the notes when I need them (or spend too long looking for them).

3. There's lots of math topics, articles, blogs, etc. I want to read, but because of limited time, have to postpone, and I need a centralized place to keep the links so I can find them later.

4. Sometimes I read things, hold them in short-term memory, think I understand them, and then several months later I have to reread it to understand it. This is suboptimal—I want to force myself to write a summary, no matter how bare-bones, to save "partial progress in understanding," so if I work on something, going back to it I can pick up where I left off in understanding.

I've been "too busy" learning math to keep a blog, so this will be a substitute—I intend to write up the more interesting/important stuff in nicer form.

2 What's different

1. This is not a blog; it is a thoughtstream. (1) In a blog, I could write up math articles nicely, but it's harder to show/keep track of where they fit in my personal "big picture" of the math that I know. See my blog at `http://holdenlee.wordpress.com`. (2) I don't filter out material, other than using labels (see Organization, below), as I don't think there's harm in making this available.

2. It is not intended to stand on its own: I make copious references to books, articles, and websites. Part of it is notes made while reading books. (The idea is like in `http://mathbooknotes.wikia.com/wiki/Math_Book_Notes_Wiki`).

Why LaTeX/pdf? For me it is the fastest way to write math on the computer. Other formats don't allow LaTeX macros.

3 Organization

To help a reader navigate, I'll use the following labels. All numbers are rough guidelines only.

1. Readability: on the scale of 1-5, how easy it might be for someone else to read. 1 means not at all (probably lots of random notes I wrote up trying to understand something), 3 means somewhat comprehensible (but probably not finished, missing chunks, etc.), and 5 means "this could go in a book."

2. Precision: on the scale of 1-5, how much I explicitly go through the theorems and proofs. 1 means that I only try to write things in a big-picture kind of way (that may be misleading/inaccurate) so take these with a grain of salt.

3. Recommendations: [R] for books/references I highly recommend.

At the start of each section I'll (eventually) have a guide to that section, including: what I've learned and what I'm learning (in red), what I'd like to learn, and references/links.

4 Contact

I would love it if more people joined in! For a quick start, use the source code and delete the text (contact me if you need help); if enough people are interested we can start a group.

Email me at `mailto:holdenlee@alum.mit.edu` or `mailto:hl422@cam.ac.uk` to talk about math, or to talk about meta things like how to improve the organization of thoughtstreams, collaboration in math, etc.

Chapter 1

Threads organized by date

1 January 2014

27. (Analysis) Learned Fourier analysis (Computation) Read Ch. 9 of Quantum computing since Democritus (Aaronson).

28. (Computation) Learned how to use Isabelle. (Algebra) Chapter 4 of Schemes (Vakil). (Computation) Continued Aaronson. Notes. Did QComp problems 1 (Bernstein-Vazirani) and 3 (Simon). (Number theory) Went over Van der Corput lemma and corollary (equidistribution of $f(j)$ given by $\Delta_r f(j)$, notes). (Logic) Thought about Gödel Incompleteness. (Have lots of questions on this.)

29. Went over combo, percolation, distributions material. Read Ch. 11 of Aaronson. (Logic) Did exer. 27.

30. (Probability) Reading Ch. 4 of Probability on graphs. Wrote blog post on mathematical compression.

31. (Probability) Finish most of Ch. 4.

2 February 2014

1. (Analysis) Did distributions problems 1-7, parts of 11, 13. (Probability) Did problem 9 of percolation. (Algebra/geometry) Read Ch. 4 of Vakil and worked on exercises.

2. (Algebra/geometry) Worked through Ch. 5 (skimming parts) (Logic) Read part of “Reflection in probabilistic logic.”

3. (Computation) Essentially finish Quantum computation examples 1. (Algebraic geometry) Start writing summary. Notes.

4. (Combinatorics) Worked on Adam’s graph theory problem (without success). (Algebra/geometry) Start Ch. 8.

5. (Algebra) Polynomial method: cell decomposition, Szemeredi-Trotter, Bezout.

6. (Combinatorics) Solved Adam's graph theory problem.

7. -

8. -

9. (Combinatorics) Reading O'Donnell's thesis on noise sensitivity

10. (Analysis) Worked on distributions examples, typed (in distributions doc), read 3.1 of Stein-Shakarchi.

11. (Logic) Met with Prof. Forster to ask questions. (Percolation) Started examples sheet. (Computation) Worked on exercise for IFV.

12. (Combinatorics) Wrote up Bonami-Beckner. Read more on noise sensitivity. (Algebra) Started AMiIT problems.

13. (Analysis) Distributions: did most of examples. See distributions notes. `https://dl.dropboxusercontent.com/u/27883775/math%20notes/part_iii_distribution` `pdf` Read parts of Stein-Shakarchi Ch. 2 and 3 (Hilbert transforms, inequalities using convexity).

14. (Combinatorics) Wrote up Fourier spectrum small $\implies II \to 0$ argument, and iterated majority. (Computation) Wrote up QComp exercises and index-carded. (Question `http://tex.stackexchange.com/questions/160500/using-qasm2circ`)

15. (Combinatorics) Did most of Extremal combo sheet. See part iii combo `https://dl.dropboxusercontent.com/u/27883775/math%20notes/part_iii_combo.pdf`

16. (Probability) Percolation: worked on examples 1.

17. (Computation) Worked on IFV exercise.

18. ?

19. (Computation) Index-carded 18.404, read quantum computation

20. (Computation) Continued quantum computation

21. (Combinatorics) Worked on noise sensitivity.

22. -

23. TMS lecture—maths of climate, dependent type theory. (Computation) Index-carded quantum computation.

24. (Combinatorics) Did examples 1. See `https://dl.dropboxusercontent.com/u/27883775/math%20notes/part_iii_combo.pdf`

25. (Combinatorics) Skimmed some noise sensitivity (VI).

26. (Algebra) Polynomial method. (Analysis) Distributions

27. ?

28. (Computation) Caught up notes

3 March 2014

1. (Combinatorics) Noise sensitivity reading.

2. -

3. (Combinatorics, Computation) Noise sensitivity, boolean functions

4. (Combinatorics) Did Problem 1 in ES1. NS reading. (Algebra) Polymethod.

5. (Probability) Reviewed and index-carded percolation.

6. ?

7. (Combinatorics) Started examples sheet. Index-carded LLL and correlation inequalities.

8. (Analysis) Started ch. 3 of FAoNF, did some distribution examples. (Algebra) Polynomial method—read Ch. 2 of Dvir's notes. Read Terry Tao's blog entries on PM.

9. (Computation) Started Ch. 11 of Nature of Computation. (Combinatorics) Noise sensitivity, did exercises to understand simple examples.

10. (Combinatorics) Noise sensitivity. (Computation) Reading from NoC.

11. (Number theory) Analytic class number formula

12. Part III talks. (Number theory) Continue.

13. Part III talks. (Number theory) analytic class number formula writeup, $x^2 + x + p$ problem

14. (Number theory) Wrote up ACNF.

4 April 2014

5 May 2014

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12. Revise for Ramsey.
13. Revise for Elliptic Curves
14. Elliptic
15. Elliptic (formal groups, local fields, torsion group, Kummer thery, Galois cohomology)
16. Elliptic (Mordell-Weil with computation, heights)

Chapter 2

Analysis

1 Complex

Holomorphic functions with $\Re f \geq L$ (from Harvard quals): $g(e^{h(z)})$ where g sends $[0, \infty)$ into $[L, \infty)$ and $h(z)$ is arbitrary analytic.

Pf. Can take ln!

2 Fourier analysis

-29th Nov Given that $f \in C^1([0, 2\pi])$ and $f \sim \sum_n a_n e^{int}$, prove that $\sum_n |a_n|$ converges absolutely.

Initial idea: integration by parts. But this only gives a bound $a_n = O\left(\frac{1}{n}\right)$, not good enough.

Hint: Use the Cauchy-Schwarz inequality. Also recall the different notions of convergence: there is pointwise convergence but also L^2 convergence!

Solution.

$$\begin{aligned}\hat{f}(n) &= \int_0^{2\pi} f e^{-int}\, dt \\ &= \int_0^{2\pi} f' \frac{e^{-int}}{-in}\, dt \\ &= \frac{i}{n}\widehat{f'}(n)\end{aligned}$$

Now (exclude $n = 0$ for convenience)

$$\sum_n |\hat{f}(n)| = \sum_n \left|\frac{1}{n}\widehat{f'}(n)\right| \leq \sqrt{\sum_n \frac{1}{n^2} \sum_n |\widehat{f'}(n)|^2} \leq \left(\sum_n \frac{1}{n^2}\right)^{\frac{1}{2}} |f|_2$$

by Parseval.

3 Functional

3.1 Riesz Representation

(12:48pm–2:20pm)

Let's index-card Chapter 3.

[#partition of unity][#shrinkage lemma] Shrinkage lemma looks like partitions of unity. What is PoU? I keep forgetting. Need to index-card! Let me try to remember. A partition of unity with respect to $A \subset U$, is a sequence of continuous (C^∞, if so desired) functions satisfying the following. (Exist for U open in $\mathbb{R}^n$, A compact.)

1. For any x, there exists a neighborhood U_x such that $\sum_i f_i(y)$ is finite sum on U_x, equal to 1 on A.

OK, you fail. We define partitions of unity not with respect to one set but to *a collection of open sets.*

Definition 2.3.1: (Munkres p. 139, theorem 16.3) [1] A **partition of unity** wrt U is a sequence ϕ_i of continuous functions $\phi_i : \mathbb{R}^n \to \mathbb{R}$ such that

1. (Nonnegativity) $\phi_i(x) \ge 0$ for all x.
2. (Support in U) $S_i := \operatorname{Supp} \phi_i \subseteq U$.
3. (We only have to deal with a finite number of the ϕ_i at a time.) Each point has a neighborhood that intersects only finitely many of the S_i.

[2] We typically want extra conditions. Let $\mathcal{A}$ be a collection of open sets in $\mathbb{R}^n$, and let $U = \bigcup \mathcal{A}$. A **partition of unity** compactly supported, of class C^∞, dominated by $\mathcal{A}$ is a sequence ϕ_i of continuous functions $\phi_i : \mathbb{R}^n \to \mathbb{R}$ such that

1. (Nonnegativity) $\phi_i(x) \ge 0$ for all x.
2. (Compact support contained in elements of $\mathcal{A}$) $S_i := \operatorname{Supp} \phi_i \subset\subset A$ for some $A \in \mathcal{A}$.
3. (We only have to deal with a finite number of the ϕ_i at a time.) Each point has a neighborhood that intersects only finitely many of the S_i.
4. (C^∞) $\phi_i \in C^\infty$.

Theorem 2.3.2: There exist partitions of unity with respect to $\mathcal{A}$, with all the above conditions.

Proof.

1. Find a nice C^∞ function with compact support–such as $f(x)g(1-x)$, $f(x) = e^{-1/x}1_{x>0}$. Use as building blocks for functions on rectangles.
2. There exists an exhaustion of $\mathcal{A}$ by rectangles: Q_i such that Q_i° cover U, each Q_i is in an element of $\mathcal{A}$ (cf. 2), and each point of A has a neighborhood intersecting finitely many Q_i (cf. 3).

3. Define functions like in (1) on rectangles in (2). The key is normalizing the right way: $\phi_i(x) = \psi_i(x)/\sum_{n=1}^{\infty} \psi_n(x)$.

□

Query: do certain things not extend to complex theory because we can't define a nonzero analytic function with compact support?

What is this good for?

1. Defining Riemann integration over non-compact sets. Remember it's convenient to first define for compact sets because we can divide into smaller and smaller rectangles. We define $\int f = \sum \int \phi_i f$.

2. See HW3 `C:\Users\Owner\Documents\Holden\Math\CollegeMath\Analysis\RealAnalysis\18.101`

3. Existence of bump functions: Given compact A in open U, there exists a C^∞ function $\rho : \mathbb{R}^n \to \mathbb{R}$ such that ρ is 1 on A and $\text{Supp}(\rho) \subseteq U$.

   Important conceptual question: in the theorem we seem tohave $\sum \phi_i = 1$ everywhere. How to get something that vanishes outside some set? Answer: a finite number of opens cover K, *throw away* the rest of the sets and functions.

Shrinkage lemma is the same argument as PoU, with 2 differences.

1. **We shrink the sets V_i, an easy use of normality.**

2. **We're dealing with topological spaces not $\mathbb{R}^n$, so the explicit construction of the function is replaced by Urysohn's lemma.**

Review of measure theory: why is regularity defined the way it is?
What's an example of an outer measure that's not a measure?
(See `https://www.sharelatex.com/project/51fe1979db89c3c351050572` for some motivations/applications.)

Fixed a lot of typos. (This takes sooo long. Maybe delegate to other people in the future?)

12th Nov: From Big Rudin, note convergence is a requirement in the countable additivity (in the real case, the sum would be finite or ∞; definability was not an issue).

For the real case, it was immediately apparent that if A has finite measure and f is bounded, $\int_A f < \infty$. This is not clear for the complex case! There could be places where the measure is positive/negative/pointing in some other direction and so cause cancellation when calculating $\mu(A)$, but conceivably "multiplying by f" makes it all positive, and $\int_A f$ could diverge. But this actually doesn't happen! Want μ to be majorized in absolute value by λ, so define a

3.2 Weak topologies

15th Nov

Remark after 4.4.4:

- Understand ℓ_∞ and why it's such a good counterexample for things.

- Proof of X w-sep implies sep?

4.4.5 (pr:f4-15). Standard: we want to produce a countable set whose closed linear span is the whole space, then use Riesz. Our distance function should give good approximations to every point. But the distance function is not in X^*! How to relate stuff in X^*? Definition of metrization: that balls contain open sets (and vice versa)—and the open sets are where a finite number of x^* are less than something. Thus take these x^* for the radius of the ball going to 0.

(What prevented w from being metrizable usually? There not being a countable number of seminorms. Metrizability gives us a countable number of x^* which really capture the topology, in the sense of being dense in the space.)

Given arbitrary x^*, we want to approximate it, Riesz-style: find z^* small so $x^* - z^*$ is in the span. Equivalently, we want $\ker(x^* - z^*) \supseteq \bigcap \ker x^*_{ni}$ some finite intersection; we need x^*, z^* to coincide on the intersection of some kernels—but this is fine since by metrizability the intersection of those kernels is in a ball, where x^* is small, and by Hahn-Banach extension we can make z^* small as needed.

4.4.6 Why is X sep implying X^* w^*-sep? Again,

> 🔑 Show topologies are the same by showing the identity is a continuous bijection from a compact to a Hausdorff.

4.4.7 (lem:f4-17) I'm confused about the application of the Open Mapping Theorem here. OK: open map when restricted to X, enough.

We're applying HB separation with A and $(x^{**}(x_1^*), \ldots)$.

Note that ε is not independent of x (i.e., there may not be x with $\|x\| = \|x^{**}\|$ because we don't have completeness. Sup is important, it's not necessarily a max.

(I don't understand this deeply.)

4.4.8 (thm:goldstine) It seems that HB separation is often used for balls and points. To prove a point is in a ball, assume it is not, and use HB to derive an inequality; but we can characterize the sup over the ball in terms of norm, and get a contradiction. Why would this be difficult without HB separation? If we don't know it, it's perfectly fine for us not to be able to separate things by looking at functions on them... Note we needed compactness here! We need the strict inequality.

The nice thing about w^* topology is that it's "like" a product topology... in that you look at finitely many things at a time... It makes a lot of proofs work. w^* neighborhoods involve finitely many things, why we could do 4.4.7. I don't get the second proof.

4.4.9 (4-19) Why is Y closed subspace imply Y reflexive? Reflexivity is powerful: often you can argue on X^* more easily... but then you end up getting results on X^{**} instead of X, but for reflexive spaces $X^{**} = X$!

(2) is really suggested by Goldstine!

(1) $\implies$ (3) bootstraps using (2).

(3) $\implies$ (1) bootstraps using everything!

How to read w, w^*: one is using the functionals, one is using evaluations.

Why is B_X norm-closed in X^{**}?

4.4.11 cf. proof of uncountability? This lemma is really weird. Think about it! Do the natural thing to prove.

4.4.10 proof: Use $X \hookrightarrow C(K) \hookrightarrow C(\Delta) \hookrightarrow C[0,1]$. Spaces of functions easier to analyze because they "come from" something?

17th Nov:

1. Pr. 4.2.4 $\sigma(X, X^*)$: Why not metrizable?

2. See proof of PUB and Banach–Steinhaus

3. Completeness: why is X complete under w-topology? (Need in order to conclude Pr 4.2.8 from 4.2.7.)

4. Cor. 4.4.2 cf. Fourier series weakly converging. cf. in the approx problem (Weyl), we only need weakly conv.

5. Why do we need Banach in 4.4.9?

Index-carded Ch. 4.

11/18/13

1. Why does B weakly* bounded imply norm bounded need completeness?

   For all x, $\{x^*(x) : x^* \in A\}$ is bounded. (How to remember definition? Note that can't vary over x inside.) Now use Hahn-Banach for Banach spaces to express in terms of norm. $|x^*(x)| < M$.

3.3 Spectra

Warm-up: Let p be an analytic function and A a Banach algebra. Under what conditions is

$$\mathrm{sp}(p(a)) = p(\mathrm{sp}(a))?$$

Initial thoughts:

1. Need $r(a) <$radius of convergence of p. So CONDITION: **Suppose that the radius R of convergence for p satisfies $R > r(a)$, and $R > \|a\|$.** (Second automatically implies the first, by submultiplicativity.)

WHAT WE NEED TO SHOW:

$$\left\{\lambda \in \mathbb{C} : \lambda 1_A - p(a) \notin A^\times\right\} = \left\{p(\lambda) : \lambda 1_A - a \notin A^\times : .\right\}$$

PROOF IDEA: If $p(a) = 0$ then $p(x) = (x-a)q(x)$. Difficulty: we're not over $\mathbb{C}$. Actually: this doesn't matter so much.

EASY CASE: Let's consider polynomials first. Can we write

$$p(\lambda)1_A - p(a) = (\lambda 1_A - a)q(\lambda)?$$

Then LHS not invertible implies RHS not invertible. Refinement: we want

$$p(\lambda)1_A - p(a) = (\lambda 1_A - a)^n q(\lambda)$$

with $q(\lambda) \neq 0$. Why does this hold? Just some abstract algebra: in $R[t]$ we can divide polynomials when the leading term of the divisor is a unit; here, it's 1_A. Think of q above as in $A[t]$. Then we are done: if there's an inverse for $p(\lambda)1_A - p(a)$ we get an inverse for $(\lambda 1_A - a)$. If there's an inverse for $(\lambda 1_A - a)$, then because there is an inverse for $q(\lambda)$, we are done.

Now let's GENERALIZE. By division in $R[[t]]$ there is a power series

$$p(T) - p(a) = (T - a)q(T).$$

Need convergence properties of $q(T)$. This is messy but elementary in the sense of an intro analysis course, the key being that the coefficients of $p(T)$ grow like $\left(\frac{1}{R}\right)^n$ at most. The proof is same as for power series, using submultiplicativity and triangle inequality.

Of course, it would be nice to just have general lemmas on holomorphic functions on A so we don't have to repeat "using the same argument as in complex analysis."

So let's see what's done in the course.

Spectral mapping theorem for polynomials: note (6.1) implying what we want: it's not trivial, we can't just choose Λ such that $|\Lambda(x^n)| = \|x^n\|$! Because we're taking $n \to \infty$.

3.3.1 The case of $\mathcal{B}(X)$

How to prove the following: Any basis of a complete space X in the functional analysis sense has the same cardinality.

Q: Why aren't compact operators the same as finite-rank operators?

A: It's not just the dimension of the image that matters, it's how you map onto it. Consider $T : x_n \mapsto \frac{1}{n}x_n$.

Q: how to relate the spectral theorem in the course with more intuitive results, and concrete things like Schrödinger's equation?

Browsing wikipedia

1. http://en.wikipedia.org/wiki/Compact_operator_on_Hilbert_space

2. http://en.wikipedia.org/wiki/Spectral_theory_of_compact_operators

3. http://en.wikipedia.org/wiki/Almost_periodic_function

4. http://en.wikipedia.org/wiki/Decomposition_of_spectrum_(functional_analysis)

3.4 Holomorphic functional calculus, spectral theorem

Understand how complex analysis works on complex spaces!

Q. How do we rephrase Cauchy's Theorem?

Theorem 2.3.3 (Rudin, 3.31)**:** Ω be open, X complex Frèchet space (why need Fréchet space? Why don't you need Banach space (norms)?), and assume $f : \Omega \to X$ is weakly holomorphic. Then

1. f is strongly continuous—what does this mean?

2. (Cauchy's Theorem) If Γ is a closed path with $\mathrm{Ind}_\Gamma(w) = 0$ for $w \notin \Omega$, then $\int_\Gamma f(\zeta)\, d\zeta = 0$ and $f(z) = \frac{1}{2\pi i}\int_\Gamma (\zeta - z)^{-1} f(\zeta)\, d\zeta$ if $z \in \Omega$ and $\mathrm{Ind}_\Gamma(z) = 1$. (...)

3. f is strongly holomorphic.

Q. Proof? Copying or using case for $\mathbb{C}$?

Idea: reduce to $\mathbb{C}$ by looking at Γf. Now use Γf being holomorphic. (a) is hardest it seems.

Q. What is this distinction between weakly and strongly holomorphic?

1. (We can't work on X right now, so use functionals!) weak: Λf is holomorphic for every Λ.

2. (We copy the definition for holomorphic) strong: $\lim_{w \to z} \frac{f(w)-f(z)}{w-z}$.

What is NOT clear: that weakly holomorphic implies continuous! Need facts about how weak topology relates to strong topology.

Rudin says 3.18 is important: In a LCS, every weakly bounded set is originally bounded, and vice versa. (See Prop. 4.2.6 in functional notes. Note we assume Banach there. Exercise: prove for LCS. We can probably use HB for LCS.) So? Recall the definition of derivative where we think of it like $f(z) + f'(z-w)(z-w) + o(z-w)$.

Get back to this later.

7.3 in Graham Allan: "f-d spectral theorem for normal T is another name for diagonalization." Compact normal T in Hilbert space. (Note compact implies 0 is in spectrum.) (If infinite number of eigenvalues, go to 0. Why?) ! Symbolically, $T = \int_{\sigma(T)} \lambda\, dE_\lambda$. This is calculus. For the **functional** calculus part, $f(T) = \int_{\sigma(T)} f(\lambda)\, dE_\lambda$. ($f$ holomorphic) Allen uses Daniell integration, which creates measures from functionals.

Now I understand the statement in lecture notes. Think of θ like an integral, then it corresponds with the statement above. We sidestep the issue of having to define a measure this way. Commuting with φ is the commuting with f above. We actually define θ_x first and THEN prove the spectral theorem. So this chapter is not the final word—but we a sort-of intermediate theorem to where we eventually want to go (spectral theorem).

To resolve: how is θ_x related to the spectral measure?

Chapter 7 in notes. Consider the case $A = \mathcal{M}_{n\times n}(\mathbb{C})$. NO WE CAN'T because this is not commutative! So instead restrict to $\overline{\mathbb{C}[M]}$ for $M \in \mathcal{M}_{n\times n}(\mathbb{C})$. (We only care about 1 operator at a time anyways.) (For noncommutative we're in representation theory.) Then $\theta_x : \mathcal{O}(U) \to M_{n\times n}, u \mapsto M$. Here characters are replacing M by an eigenvalue.

Holomorphic functional calculus says that we can define holomorphic functions on A. We can take holomorphic functions over $\mathbb{C}$ and evaluate them at things in A. Moreover, it interacts nicely with characters—we want this because this is our natural way of getting something in $\mathbb{C}$ from something in A, $\varphi : A \to \mathbb{C}$, and somehow characters capture the complete structure of A.

Technical condition: we need convergence. To ensure convergence we need our holomorphic functions to converge at the spectrum (eigenvalues) (think about matrices. in order for $f(A)$ to converge we need f to converge at eigenvalues of f).

Really, think of $\theta_x(f)$ as "$f(x)$." Now we're just saying $\varphi(f(x)) = f(\varphi(x))$, i.e., f commutes with characters. (What's the point of writing it as θ_x? To emphasize that it's continuous with respect to $f \in \mathcal{O}(U)$.)

More generally, if we think of a 1-parameter subgroup of $\mathcal{M}_{n\times n}(\mathbb{C})$, then characters correspond to eigenspaces.

How to show this? Looks like developing the theory of holomorphic functions all over again... what do we need to look out for?

7.1.2 (Runge) *What is the obstruction to approximation by polynomials?* It's Cauchy's integral formula. Consider $\frac{1}{x}$ defined in an annulus. Taking an integral around the circle once gives $2\pi i$. It's 0 for any polynomial.

What goes wrong in Stone-Weierstrass? We need the algebra to be *self-adjoint*, and the conjugate of a holomorphic function is typically not a holomorphic function! ($\overline{z}$ is not. only constants are?) Stone-Weierstrass takes us out of the analytic world.

Notation: $[\Gamma]$ is set of points on the paths.

We define Riemann integration on Banach spaces. (I guess we don't care about Lebesgue integration because we deal mainly with holomorphic functions?) Define relative to path, too.

7.1.5 see stuff before on different notions of "analyticity." (If we prove weak analytic implies analytic, we have less work on our hands in showing things are analytic.) Getting Cauchy's theorem directly, without repeating the argument: use the φ!

7.1.6 We want to define $f(x)$. One approach is to expand f in power series and check convergence... but note in complex analysis, every function can be written in terms of an integral using Cauchy, and we can also check analyticity this way. To evaluate at x, we circle x.

Proof. What's the corollary ?? Checking θ_x continuous—pretty trivial, recall that the seminorms are max on a compact set.

Additions:

1. By Cauchy's Theorem, since 1 is defined not just on U but the whole space, we can change the contour to a circle, which also winds around each point of $\sigma(x)$ once.

2. This is just term-by-term integration. (Classic proof of Cauchy. Note here x is in the algebra, which is why we had to expand first.)

3. Note we are using the fact that the power series of the reciprocal converges in A—proof transfers over to A. Why don't we just look at power series in A?—Try this and look

at obstacles. Note s_k, t_k have no poles, though they might have zeros. What was the point of all this? We want to eval $\int r(z)(...)$; we really want it to be $r(x)$, so let's decomp it like that...

4. Part (3): just do it... we basically use the fact that φ is an algebra homomorphism. We can commute it with the integral (shown before). Why is the last equality $= f(\varphi(x))$ true? f might have poles inside... NO: because f could only have poles outside of U, and we assumed Γ winds 0 times around anything in U. (condition of lemma 7.1.6)

Why are we NOT done after Lemma 7.1.6? We need

1. θ_x is algebra hom.

(Note φ characterization of σ is very useful!)

Where did we need semisimple in the remark? Added.

Proof of Runge. We know the image of θ_x is inside $A = R(K)$. The proof of 7.1.6 was exactly this approximation process with rational functions. We're doing two things:

1. We're saying $\theta_x(f) = f$, where θ_x is defined as this integral, chosen with our goal $\theta_x(f) = f$ in mind.

2. We're saying $\theta_x(f)$ is in our algebra, because it is defined as an integral in our algebra.

We're really sending a function to itself here... sort-of a trivial case of 7.1.6 for analytic functions.

(29 Nov material) Take as black box the Theorem ??. Review. What are we proving??

3.5 C^*-algebras

What is good to know before starting?

1. Hermitian, unitary, normal operators

2. Positive definite operators, square roots.

Q: Why is G-N useful? Our spaces are actually spaces of functions

Q: Is $C(K)$ a subalgebra of $\mathcal{B}(H)$ for some H? Clearly, consider $\mathcal{B}(C(K))$.

The condition $\|xx^*\|$, with the normal, etc. conditions, mesh very nicely with the formula for the spectral radius. Cor??

Remark before 8.1.8??

Lem 8.1.8 proof: h acts like a real element, so consider $\|h + it\|^2$. But on the other hand look at $\varphi(h)$; h acting real forces $\varphi(h)$ to act real.

Why is $|\varphi(a)| < \|a\|$?

!!!! G-N is from the Gelfand transform! A is a set of functions on its character.

Rem after cor 8.1.10 (8-3) Note $\mathbb{T}, \mathbb{R}$ closed, 1-D.

2. Why $=$? Why holds for normal x?

Commuting thing: a common inverse if $a^{-1}b^{-1} = b^{-1}a^{-1}$? Can there be different left/right inverses???

3. Note commutative implies semisimple.
Can do stuff on noncommutative if take a commutative subalgebra.
cf. This is how we prove square roots in the finite-dimensional case too!!!
PD: same idea: look at TT^*, use approximate spectrum to make work in f.a.

3.6 Spectral theorem

3.6.1 Figuring things out

12/12/13: Read over spectral theory notes.

Need an example! What is this operator-valued measure? Why do we need to talk about operator-valued measures rather than normal measures? Why is P not necessarily countably additive?

Example: $H = L_2[0,1]$, $K = [0,1]$, $P(E)f = 1_E \cdot f$. Then $P_{f,g}(E) = \int_E f\overline{g}\, d\mu$. (Check convention with conjugation.) Finite-dimensional case: H is $n \times n$ diagonal matrices, $K = \{1, \ldots, n\}$. (Why am I thinking about finite-dimensional case? Because one goal of functional analysis is to use intuition from finite-dimensional algebra and prove structure theorems about function spaces.)

Q: It seems often H is a space of functions over K? Is there an example where this isn't the case?

Q: What about this example? $H = L^2[0,1]$, $K = \mathbb{Z}$, $P(\{n\})$ is projection to nth Fourier coefficient. Note K is not compact though! (it is locally compact...)

Note 9.1(v) says

$$\sum_i \langle P(E_i)x, y\rangle = \left\langle P\left(\bigcup_i E_i\right) x, y\right\rangle.$$

But how do we know

$$\sum_i \langle P(E_i)x, y\rangle = \left\langle \sum_i P(E_i)x, y\right\rangle?$$

We need this to conclude $P\left(\bigcup_i E_i\right) x = \sum_i P(E_i)x$ for all x.

Example: $A = L^2[0,1]$, $H = L^2[0,1]$. Note Φ_A is NOT evaluation. Claim: $\Phi_A = \left\{\int f(t)e^{-2\pi ikt}\, dt : k \in \mathbb{Z}\right\}$? Then 9.8 is just $f = \sum \widehat{f}(n)e^{2\pi int}$?

Note we make A into a function on Φ_A by the Gelfand transform $A \to C(\Phi_A)$. $T \mapsto \hat{T}$. Q: it seems like Φ_A is NOT compact! What's wrong? This doesn't seem to be right... Wiener algebra: the maximal ideals are f such that $f(x) = 0$, varying over x. This isn't what I'd expect over some space like L^2 where changing a function on a set of measure 0 doesn't do anything...

Resolution: If we use convolution, then there isn't an identity! (There are only almost identities.)

Example: Consider $T = \int$. We get $\int f = \sum_n \frac{1}{2\pi in}\hat{f}(n)e^{2\pi int}$. Integration is decomposable.

3.6.2 Summary of chapter

Before reading this chapter, it's good to recall facts about finite-dimensional linear operators. This is because the spectral theorem will be a generalization of the spectral theorem from linear algebra (although at first glance there seems to be so much measure-theoretic notation that this is not clear). In general, in functional analysis we draw intuition from finite-dimensional linear algebra and prove structure theorems about function spaces.

Problem 2.3.4: Do the following. (If you prefer, think of T as a matrix.) Everything is over $\mathbb{C}$.

1. (The spectral theorem) State the spectral theorem for normal operators on a finite-dimensional vector space.

   (a) Be sure to state the entire thing—i.e., with the "resolution of the identity."

   (b) What are some important classes of normal operators, and what happens in those cases?

2. (Operators as functions on their spectra)

   (a) Let T be a finite-dimensional diagonalizable linear operator. Consider the algebra $\mathbb{C}[T, T^*]$. Describe $\hat{T}$.

   (b) Let A be the algebra of linear operators on a finite-dimensional V that are diagonalizable with respect to a fixed basis. Describe the Gelfand transform $\hat{\bullet}$.

3. (Commuting linear operators) When do two diagonalizable linear operators commute? Prove this.

4. (Defining functions on linear operators) Let T be normal, and f be a function.

   (a) When does it make sense to define $f(T)$? How do we define it?

   (b) Why do we restrict to T normal?

1. The most compact version of the spectral theorem is probably the following.

   Theorem 2.3.5 (Spectral theorem, I)**:** Let T be a normal operator on a finite-dimensional Hilbert space H (vector space with inner product). Then T is unitarily diagonalizable, i.e., there exist U unitary and D diagonal so that

   $$T = UDU^{-1}.$$

   If T is unitary, then T and hence D has eigenvalues on the unit circle $\mathbb{T}$. If T is hermitian, then T and hence D has real eigenvalues.

   The "expanded" version of the spectral theorem involves several more statements—all of which are relatively easy to derive from the above, so that we often forget about them. But they are important because they will suggest the right way to state the spectral theorem in the infinite-dimensional case.

Theorem 2.3.6 (Spectral theorem, II)**:** Let T be a normal operator on a finite-dimensional Hilbert space H. Let $\sigma(T)$ denote the eigenvalues of T. Let E_λ be the eigenspace of T with eigenvalue λ, and P_λ be the orthogonal projection onto E_λ (so that $P_{\lambda_1}P_{\lambda_2} = 0$ for $\lambda_1 \neq \lambda_2$). Then the following hold.

(a) (Diagonalizability) $H = \bigoplus_{\lambda\in\sigma(T)} E_\lambda$, where the eigenspaces E_λ are mutually orthogonal.

(b) (Resolution of the identity) $I = \sum_{\lambda\in\sigma(T)} P_\lambda$

(c) (Spectral decomposition of T) $T = \sum_{\lambda\in\sigma(T)} \lambda P_\lambda$

It is not hard to see that in this finite-dimensional case, (a), (b), and (c) are just different ways of saying the same thing.

2. The characters correspond to eigenspaces E of T: $\varphi_E(T')$ is the eigenvalue of T' on E. Thus $\hat{T} : \Phi_A \to \mathbb{C}$ is simply the function sending the character corresponding to E_λ, to λ:
$$\hat{T}(\varphi_{E_\lambda}) = \lambda.$$
For (b), the φ correspond to basis elements v; $\hat{T}$ is the function sending φ_v to the eigenvalue of v.

3. A, B commute when they are simultaneously diagonalizable. One way is to find a simultaneous eigenbasis step by step. Another is to write the spectral decomposition as in (1) and see that B has to commute with the projections to the eigenspaces of A. (This is actually the criteria we'll use in the infinite-dimensional case.)

4. f needs to be defined at the eigenvalues of T. Writing $T = UDU^{-1}$, we define $f(T) = Uf(D)U^{-1}$. In other words, if the spectral decomposition of T is $\sum_{\lambda\in\sigma(T)} \lambda P_\lambda$, we define
$$f(T) := \sum_{\lambda\in\sigma(T)} f(\lambda)P_\lambda.$$
cf. (b) and (c) in (1), where $f(x) = 1, x$ respectively. We restrict to T normal so that we have a spectral decomposition of T. (Nothing really goes wrong if T is diagonalizable but not normal.)

   Note that $f(T)g(T) = (fg)(T)$: this is since we multiply termwise
$$\sum_{\lambda\in\sigma(T)} f(\lambda)P_\lambda \sum_{\lambda\in\sigma(T)} g(\lambda)P_\lambda = \sum_{\lambda\in\sigma(T)} (fg)(\lambda)P_\lambda,$$
using $P_{\lambda_1}P_{\lambda_2} = 0$ for $\lambda_1 \neq \lambda_2$.

Combining (1) and (2), we can write the spectral decomposition in a fancy way:
$$T = \sum_{\lambda\in\sigma(T)} \hat{T}(\varphi_{E_\lambda})P_\lambda.$$

Or identifying φ_{E_λ} with λ,

$$\text{eq:f9b-1} T = \sum_{\lambda \in \sigma(T)} \hat{T}(\lambda) P_\lambda. \tag{2.1}$$

(We wouldn't actually want to do this, but stretching your brain for what's coming up...)

3.6.3 Preparing for infinite dimensions

Things we have to consider:

1. There may be an infinite number of eigenspaces. Everything seems to fall apart: how do we write our space as a direct sum of eigenspaces? How do we write I as a sum of projections? How do we write T as a sum of functions that are nonzero only on eigenspaces?

2. In the finite-dimensional case, an eigenspace is λ such that $T - \lambda I$ is not invertible, or equivalently, it's not injective. In the infinite-dimensional case, $T - \lambda I$ may be not invertible, and still injective. difference something to do with discrete/continuous spectrum?

To solve (1), we have to take an integral rather than a sum!

3. How do we take an integral of *operators*? What is the measure space?

We'll have to address these questions!

3.6.4 Reading guide

As a quick example, consider $H = C[0,1]$, continuous functions on $[0,1]$. Given f, consider the linear operator on H that is simply multiplication by f. Can you "see" that f is like a diagonal matrix? Think of functions on $[0,1]$ as functions with an infinite number of components, one for each $x \in [0,1]$; multiplication by f multiplies the x-component by $f(x)$.[1] Then $\sigma(f)$ is simply the image of f.

When we have a sum it makes sense to isolate points, but when we have an integral it doesn't—so we don't really want to just define $P_\lambda = P_{E_\lambda}$ for $\lambda \in \sigma(T)$. We want to define $P(E)$ where E is a *subset* of $\sigma(T)$.

Thus we define resolution of the identity (9.1) where (iii)-(v) describe how the different $P(E)$ relate to one another. Think of K as being $\sigma(T)$; the formulation here is more general. Now we want to be able to say that P is a measure in some sense; however P is a function with image $\mathcal{B}(H)$; thus instead we say $P_{x,y}$ is a regular complex Borel measure for all K.

Returning to our example, see (9.2).

(9.3) Note (i) is by 9.1(iii), (ii) is by 9.1(ii) and (iv), (iii) is by taking $x = y$ in 9.1(v) and noting $P(K) = I$. Still haven't resolved 9.3(iv)-(v). (iii) is important: we don't just have a complex measure here, we have a positive measure.

(9.4) Compare this with the notation $L_\infty(\mu)$ for a measure μ. The only difference is we're dealing with P which is an "operator-valued measure."

[1] What if $H = L^2[0,1]$? We aren't allowed to evaluate at a point anymore.

(9.5) Given f, $\int_K f\,dP_{x,y}$ looks like it should be bilinear in x, y, so we should be able to write it as $\langle\Phi(f)x, y\rangle$. This gives us a different way to express the integral. (For the proof, we will actually show how to "calculate" what $\Phi(f)$ is, as opposed to just saying it exists.)

Proof: Try to define Φ for simple functions first. It is easy to show that Φ is a *unital* $*$*-homomorphism* on simple functions using the properties of P, since we are only dealing with finite sums.

In order to pass from the finite to the infinite case, we need to deal with convergence, i.e., we need a bound on $\|\Phi(s)\|$. We find we actually have an equality $\|\Phi(s)\| = \|s\|_\infty$, so Φ is isometric on simple functions. Now knowing how Φ respects norms for simple functions, we find $\Phi(s_n)$ is Cauchy for s_n Cauchy, and extend the definition in a straightforward way to all f. (iii) is a again a "true for simple functions, hence true for all functions" argument.

Important remark (9.6): given P we can determing Φ. Φ is such that (i) holds. We have $\langle\Phi(1_E)x, y\rangle = \int_K 1_E\,dP_{x,y} = P_{x,y}(E)$, so $\Phi(1_E) = P(E)$. Φ as an extension of P to non-simple functions, in the way that an integral generalizes a measure in a unique way.

(9.8) Stare at (2.1) for a few seconds, and this will make sense.

Think of $\hat{T}$ as crystallizing what T does on various eigenspaces E_λ, as separating T along its various components; we just have to combine them with an integral to get T.

Proof:

1. Our main tool for dealing with the integral is 9.5(i). 9.5(i) tells us that given a resolution of the identity there is Ψ such that

   $$\Psi(\hat{T}) = \int_K \hat{T}\,dP;$$

   actually, 9.5(i) defines T for *all* $f \in L_\infty(P)$, not just $C(\Psi_A) \cong A$:

   $$\Psi(f) = \int_K f\,dP.$$

   Summarizing, $\hat{\bullet} : A \xrightarrow{\cong} C(\Phi_A)$, and we'd like $\Psi : L^\infty \to A$. We want $\Psi(\hat{T}) = T$, Ψ is like an inverse Gelfand transform.

   Note here, however, we don't know what P is yet. (The whole point of the spectral theorem is to get a resolution of the identity!) So we'd like to define Ψ such that $\Psi(\hat{T}) = T$, and then get P out of it. We'd like to reverse 9.5. The key to getting a measure from a functional is the Riesz Representation Theorem; we get a family $P_{x,y}$, and then check these come from a single P.

   That's the motivation. Let's do everything in order now: in order to define Ψ on $L^\infty(K)$ extending $\hat{T} \mapsto T$, i.e. define a nice map when we know the map for continuous functions,

   (a) we use RRT to express $\hat{T} \mapsto \langle Tx, y\rangle$ as an integral wrt $\mu_{x,y}$,

   (b) then define $\Psi(f)$ using the integral (using sesquilinearity).

   We make sure Ψ is well-behaved by looking at norms. (Review chapter 3 if you need help on the total variation norm.) (Some comments here: the norm of $(x, y) \mapsto \int_K f\,d\mu_{x,y}$ is by definition $\max\left(\frac{\int_K f\,d\mu_{x,y}}{\|x\|\|y\|}\right)$.

We have defined Ψ now.

2. We show that $\Psi(fg) = \Psi(f)\Psi(g)$. We think about what this is saying in terms of measures:

$$\langle \Psi(fg)x, y\rangle = \int fg\, d\mu_{x,y}$$
$$\langle \Psi(f)\Psi(g)x, y\rangle = \langle \Psi(g)x, \Psi(f)^* y\rangle = \int g\, d\mu_{x,\Psi(f)^*y}$$

   (I'm trusting that it's easier to move the $\Psi(f)$ first. Or maybe it doesn't matter.) So we need $f\, d\mu_{x,y} = d\mu_{x,\Psi(f)^*y}$. To test equality of measures, by uniqueness in RRT it suffices to test equality of measures by looking at integrals of continuous functions; $\hat{T}$ are all the continuous functions on Φ_A so we test using those. This is the 2 lines of calculations on the bottom of page 3. (We're basically trying to take $\widehat{ST} = \widehat{S}\widehat{T}$ and turn it into $\Phi(fg) = \Phi(f)\Phi(g)$.)

3. Define P from Ψ. As remarked in 9.6 above, we should have $P(E) = \Psi(1_E)$. We do need to verify P is a resolution of the identity (because we're going the opposite way around from 9.5); this is straightforward. Now 9.5 applies immediately.

4. Uniqueness: simple RRT.

5. Moreover: Use Urysohn. Note $\hat{T}$ is real (i.e., T is Hermitian). (This is an example of when it's easier to look at the Gelfand transform—we can treat T like a function!)

6. (ii) Two options: use 9.5(iii), and uniqueness in RRT, or do it directly by calculating $\langle STx, y\rangle$ and using uniqueness in RRT.

(9.10) Note $\lambda x^* - \overline{\lambda} x$ is has $\sigma() \subseteq i\mathbb{R}$ because $a\bar{b} - \bar{a}b \in i\mathbb{R}$. Why is f bounded analytic? Idea: "complete" into 1-parameter group.

(9.11) Proof: We want to apply 9.8. The difference is that the integral is over $\sigma(T)$ not K. The thing to note is that Φ_A is homeomorphic to $\sigma(T)$: we have

$$\{\varphi(T) : \varphi \in \Phi_A\} = \sigma(T)$$

so consider the map $\varphi \mapsto \varphi(T)$. Since Φ_A separates points of $\overline{\mathbb{C}[T, T^*]}$, this is a bijection; since it is a continuous map between compact Hausdorffs, it is a homeomorphism. (Note that for normal operators, $\sigma(T)$ doesn't get bigger when we restrict the algebra.)

Uniqueness: use uniqueness in RRT and Stone-Weierstrass.

Commutating: use the lemma.

9.12 cf. Problem 4. Note that for normal operators, we can define $f(T)$ for f not necessarily analytic! Before, we could only define it for f analytic.

(iv) follows from Lemma 1(iii). Why do we have equality in (ii)?

9.13 This is ingenious! From the fact for $\mathbb{C}$, and noting we have multiplicativity in the integral just like in Problem 4, the result follows immediately.

9.14 Unitary is e^{iH}: Apply the functional calculus with the logarithm, remembering to show that $e^{\ln}$ converges.

9.15 Connectedness of $G(\mathcal{B}(H))$: find a path to the identity.

Thinking about Schrödinger's equation: it's complicated because you have to use the spectral theorem for unbounded operators. See p. 348 of Rudin. Stop here for today but look at SE in Physics notebook, the 18.102 derivation, and the last page in analysis in the Cambridge notebook.

3.7 Problems

-30th Nov Example sheet 2 (4 Dec: writing up solutions nicely)

Chapter 3

Combinatorics

1 Ramsey theory

12-13-13

http://qchu.wordpress.com/2010/11/22/boolean-rings-ultrafilters-and-stone

1. Idempotents.

> Central idempotents are important because every idempotent gives a decomposition
>
> $$\begin{aligned} M &= M_0 \oplus M_1 \\ m &= rm + (1-r)m \end{aligned}$$
>
> where r projects to the first summand and $(1-r)$ projects to the second summand. (Where does centrality come in? The action of R respects the decomposition, i.e., $M_0 = rM$ and $M_1 = (1-r)M$ are actually modules.)

For example, $\frac{1}{|G|}\sum_{g\in G} g$ gives a decomposition where M_0 is the invariant subspace. More generally if χ si the character for irreducible V, $\frac{1}{|G|}\sum_{g\in G} g$ gives a decomposition where M_0 is the sum of summands isomorphic to V.

2. Boolean rings

Definition 3.1.1: A **Boolean ring** is a ring satisfying $b^2 = b$ for all $b \in B$.

I.e., every element is idempotent. Boolean rings have characteristic 2 and are commutative. They are the same as Boolean algebras, with $\cdot \leftrightarrow \wedge$ and $+ \leftrightarrow \triangle$ (symmetric difference). (For a Boolean algebra, the picture is subsets under inclusion.) All finite Boolean rings look like this, i.e., $\mathrm{Hom}(\{1,\ldots,n\},\mathbb{F}_2)$, i.e. subsets, by a simple induction argument.

3. Spectra

"Whenever we meet a commutative ring, we should ask what its spectrum is." The only prime ideal are the maximal ideals. (Proof: $B/\mathfrak{p}$ must be an integral domain; in the quotient $b(1-b) = 0$ so $b = 0$ or 1.) A homomorphism $B \to \mathbb{F}_2$ is the same as a consistent assignment of truth values (i.e., if $a, b \mapsto 1$, then $ab \mapsto 1$, since we're thinking of it as $a \wedge b$).

Boolean rings correspond to Boolean algebras. Think of $B \to \mathbb{F}_2$ as assignments of truth values.

Key result: The maximal ideals of $\mathrm{Hom}(\{1,\dots,n\},\mathbb{F}_2)$ are exactly those that are 1 on some s. I.e., they correspond to sets containing s. $\operatorname{Spec} B$ is $\{1,\dots,n\}$ with the discrete topology. Q: What happens if B is infinite? Craziness!

`http://en.wikipedia.org/wiki/Stone_functor` Sends a topological space T to the Boolean ring of clopen subsets of T.

Theorem 3.1.2: $\mathrm{Hom}_{\mathrm{Top}}(-,\mathbb{F}_2)$ and Spec are adjoint.

Skip proof.

Spec sends colimits to limits. Write Spec of a Boolean ring as the Spec of $\varprojlim B_i$ for B_i finite subrings. Why can we do this? We get it's $\varinjlim \operatorname{Spec} B_i$, a profinite set. It's automatically compact, Hausdorff, and totally disconnected (Stone space). It is the Stone-Čech compactification βS!

Make this concrete: $2^{\mathbb{N}}$ is a profinite set, as an limit of $2^{[n]}$.

See the 2 functors above? We actually have $\operatorname{Spec}\mathrm{Hom}_{\mathrm{Top}}(T,\mathbb{F}_2)$ for all Stone spaces T.

Skip proof again.

4. Ultrafilters.

Let's refine what we mean by Boolean rings are the same as Boolean algebras. What do ideals correspond to? A subset of the poset that is a lower set ($y \le x, x \in I \implies y \in I$) and a directed set (existence of upper bounds for 2 elements.). This is called an ideal in a poset. `http://en.wikipedia.org/wiki/Ideal_(order_theory)`

Maximal ideals are exactly those such that for every b, $b \in \mathfrak{m}$ xor $1-b \in \mathfrak{m}$. Ultrafilters correspond to maximally consistent deductively closed sets.

Skip the rest.

Todd Trimble: I think there is a psychological tendency to think of ultrafilters as somehow "big": a really big collection of subsets hard to comprehend (at least in the case of a non-principal ultrafilter). And its not that thats wrong exactly. But considered topologically, one can consider an ultrafilter as a process of zeroing in on an ideal point, hence something that gets smaller and smaller (or more and more precise)... What makes the ultrafilter "big" is the upward closure condition, but somehow you dont care about all that surrounding fluff, you just care about how the smaller and smaller subsets you can identify as being within U.

`http://terrytao.wordpress.com/2007/06/25/ultrafilters-nonstandard-analysi`

`http://marker.to/307MY4`

Tao starts off with some metamath remarks on epsilon management.

Nonstandard analysis is interesting!

The "voting" analogy is very good. A voting system, i.e., an ultrafilter, is a system (satisfying basic properties) to assign limits to any sequence.

I initially thought we had to define an ultrafilter p for $K^{\mathbb{N}}$, but it turns out we only need to define an ultrafilter on $\{0,1\}^{\mathbb{N}}$, because everything else can be reduced to true-false statements. Let the p-limit be the infimum x such that for $y > x$, $x_n > y$ is not p-true, and $x_n < y$ is p-true (or equivalently the supremum x such that for $y < x$...). Exercise: check this is well-defined.

The proof with $\beta\mathbb{N}$ is nice.

http://en.wikipedia.org/wiki/Non-standard_analysis

http://qchu.wordpress.com/2010/12/09/ultrafilters-in-topology/

http://qchu.wordpress.com/2010/12/14/ultrafilters-in-ramsey-theory/

Q's: Is there an ultrafilter p such that $p - \lim x_n = q$ when the density of $x_n = 1$ is q and the rest are 0? Probably there are multiple such p.

Back to course material:

Note very dependent on 0's and 1's: 0 and 1 do not occupy symmetric places.

Compare $*$-topology with w^* topology? (specifically, the topology induced by the w^* topology on ℓ_∞.)

1.1 Examples

1.1.1 Examples 2

2 Graph theory

2.1 Ramanujan graphs

Reading Ram Murty's article on Ramanjan graphs.

- Eigenvalues determine growth and randomness. The largest eigenvalue determines the exponential rate of growth and the rest determine how close it sticks to that growth. Growth of what? A matrix repeatedly applied to a vector, or powers of a matrix.

  Some questions about graphs can naturally be put in the language of matrices by looking at the adjacency matrix: the number of paths from i to j corresponds to A_{ij}. We will find that λ_2 is connected to...

  - the diameter of the graph
  - how much an arbitrary subset of vertices "expands" under taking its neighbors.

  So why should the second eigenvalue matter? Its size plays a large role in how "random" the graph appears to be, and when it is larger, "growth" is more regular in various senses (to be made precise).

Lemma 3.2.1 (The largest eigenvalue)**:** Let G be a graph. Let

$$\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_n$$

be the eigenvalues of its adjacency matrix. If G has maximum degree k, then $|\lambda_i| \le k$ for all i.

If G is k-regular, then $\lambda_1 = k$.

Proof. The Perron-Frobenius Theorem states that a matrix with nonnegative entries has as its largest-absolute-value eigenvalue a positive λ with $\min_i \sum a_{ij} \le \lambda \le \max_i \sum a_{ij} = k$.

If G is k-regular, then all row sums are k. Explicitly, the all 1's eigenvector has eigenvalue k.

A purely combinatorial proof is the following: the number of paths of length n is at most nk^n. □

Problem 3.2.2: For a k-regular graph, does λ_1 have absolute value strictly larger than all other eigenvalues?

Lemma 3.2.3: Suppose G is connected.

1. Then $k = \lambda_1 > \lambda_2$.

2. If G is bipartite, then $\lambda_n = -k$; otherwise, λ_1 is the eigenvalue strictly largest in absolute value.

Proof. Note the all 1's vector has eigenvalue k.

1. Blah.

2. BIPARTITE

   If G is not bipartite, then given any i, j, there are paths of different parities between i, j, so for large enough m there is a path of length m between i and j. Take m large enough for all (i, j); then A^m is positive. Apply the Perron-Frobenius Theorem to get that $\lambda_1 = k$ is the unique eigenvalue with largest absolute value.

□

Problem 3.2.4: Find an upper bound for the diameter of the graph the second largest vector in absolute value λ. (Hint: What does this translate to in terms of the adjacency matrix?)

Lemma 3.2.5 (Small λ means small diameter)**:** Suppose G is k-regular and not bipartite. Then

$$\operatorname{diam}(G) \le \frac{\ln(n-1)}{\ln(k/\lambda)} + 1.$$

Proof. We translate the problem to a statement about the adjacency matrix. It suffices to show every entry of A^d is positive when $d > \frac{\ln(n-1)}{\ln(k/\lambda)}$, because $(A^d)_{ij}$ is the number of paths from i to j of length d. Note $(A^d)_{ij} = (A^d e_j)_i$. Decompose e_j in terms of eigenvectors

$e_j = \frac{1}{n}u_1 + a_2u_2 + \cdots + a_nu_n$. Then

$$\begin{aligned}(A^de_j)_i &= (\frac{1}{n}\lambda_1^n u_1 + a_2\lambda_1^n u_2 + \cdots + a_n\lambda_1^n u_n)_i \\ &\geq \frac{1}{n}k^n - (|a_1| + \cdots + |a_n|)\lambda \\ &\geq \frac{1}{n}k^n - \frac{n-1}{n}\lambda\end{aligned}$$

where we used

$$|a_2| + \cdots + |a_n| \leq (|a_2|^2 + \cdots + |a_n|^2)^{\frac{1}{2}} \leq |e_j| - \frac{1}{n} = \frac{n-1}{n}.$$

This is greater than 0 when $d > \frac{\ln(n-1)}{\ln(k/\lambda)}$, as needed. □

Lemma 3.2.6 (Lower bound on λ)**:** $\lambda \geq \sqrt{\frac{k(n-k)}{n-1}}$.

Proof. We have

$$\begin{aligned}&\operatorname{tr}(AA^T) = kn \\ &\operatorname{tr}(AA^T) = \lambda_1^2 + \cdots + \lambda_n^2 \leq k^2 + (n-1)\lambda^2.\end{aligned}$$

Solving for λ gives the result. □

Definition 3.2.7: A graph is a **Ramanujan graph** when $\lambda(G) \leq 2\sqrt{k-1}$.

Theorem 3.2.8: Let G be a finite abelian group and S a subset of G of size k that generates G. Then the eigenvalues of the Cayley graph $X(G,S)$ are

$$\lambda_\chi = \sum_{s\in S}\chi(s)$$

where χ ranges over irreducible characters of G.

The eigenvalues of the graph $Y(G,S)$ where (x,y) is an edge iff $xy \in S$ is multiset are also

$$\lambda_\chi = \sum_{s\in S}\chi(s)$$

Proof. The eigenvalues are the eigenvalues of multiplication by $\sum_{s\in S} s$ in $\mathbb{C}[G]$. Since we have the decomposition $\mathbb{C}[G] = \bigoplus V_\chi$, where g acts on V_χ as $\chi(g)$, we get the result. □

How can we get this sum to be small for all χ except the trivial one? Let S to the multiset of squares; we get a Gauss sum with absolute value $\sqrt{p}$.

Theorem 3.2.9: Consider $\mathbb{F}_q$, and let S be the multiset of roots of a polynomial of degree 2 or 3. Then $Y(G,S)$ is Ramanujan.

Proof. This follows from the Riemann hypothesis for zeta functions of curves over finite fields. (Actually, just from Hasse's Theorem!) □

In the non-abelian case:

1. the eigenvalues are $\lambda_X = \frac{1}{\chi(1)} \sum_{s\in S} \chi(s)$, with multiplicity $\chi(1)^2$.

Thinking of Av as v dilated along the directions of the eigenvectors, we see (Rayleigh-Ritz)

$$\lambda_{\max} = \max_{v\neq 0} \frac{(Av, v)}{(v, v)}$$

and similarly for $\lambda_{\min}$.

For subsets $B, C \subseteq V$ let $c(B, C)$ be the number of ordered pairs $(b, c) \in B \times C$ which are edges.

Theorem 3.2.10: For every partition $V = B \cup C$, $e(B, C) \geq \frac{(d-\lambda)|B||C|}{n}$.

If random, would expect around $\frac{d|B||C|}{n}$.

Proof. Let $|V| = n$, $b = |B|$, and $c = |K| = n - b$. Let $D = dI$. Consider

$$\begin{aligned}\langle (D-A)x, x\rangle &= \sum_{u\in V} \left(d(x(u))^2 - \sum_{v\in N(u)} x(u)x(v) \right) \\ &= d \sum_{u\in V} x(v)^2 - \sum_{uv\in E} x(u)x(v) \\ &= \sum_{uv\in E} (x(u) - x(v))^2.\end{aligned}$$

Note the similarity to the integration by parts formula $\int u\Delta u = \int |\operatorname{grad} u|^2$. Define x by $x(v) = -c$ for all $v \in B$, $x(v) = b$ for all $v \in C$, and $x(v) = 0$ for all other values. Note $\sum_{v\in V} x(v) = 0$. We detect edges between B and C by making the terms in the sum 0 only for u, v in different sets B, C!

(tl;dr): eigenvalues $\lambda \mapsto d - \lambda$ We claim that A and $D - A$ have the same eigenvalues. Note if μ is an eigenvalue of A then $d - \mu$ is an eigenvalue of $D - A$. Note x is orthogonal to the (constant) eigenvector corresponding to the smallest eigenvalue 0 of $D - A$. The eigenvectors of $D - A$ are orthogonal and form a basis for $\mathbb{R}^n$. Now x is a linear combination of the other eigenvectors. Since $d - \lambda$ is the second smallest smallest eigenvalue of $D - A$,

$$\langle (D-A)x, x\rangle \geq (d-\lambda)\langle x, x\rangle = (d-\lambda)(bc^2 + cb^2) = (d-\lambda)bcn.$$

But choosing x as mentioned, the LHS is $e(B, C)(b + c)^2$; divide by $(b + c)^2$. □

Corollary 3.2.11 (Small λ implies good expansion)**:** Keeping the same assumptions, G is a (n, d, c)-expander with

$$c = \frac{d-\lambda}{2d}.$$

Proof. Let $|B| \leq \frac{n}{2}$. Let $C = \overline{B}$. The above shows that $e(B, C) \geq \frac{(d-\lambda)|B||C|}{n} \geq \frac{(d-\lambda)|B|}{2}$. Since G is d-regular,

$$|N(B)| \geq \frac{(d-\lambda)|B|}{2d}.$$

□

Alon improved this to $c = \frac{2(d-\lambda)}{3d-2\lambda}$.

Theorem 3.2.12: If G is a (n, d, c)-expander then $\lambda \le d - \frac{d^2}{4+2c^2}$.

How small can λ be?

Theorem 3.2.13 (Alon Nilli)**:**

$$\lambda \ge 2\sqrt{d-1}\left(1 - O\left(\frac{1}{\operatorname{diam} k}\right)\right).$$

(Alon Nilli is a pseudonym of Noga Alon.)

> I don't understand this, but there's something deep going on in defining zeta functions. `http://en.wikipedia.org/wiki/Selberg_zeta_function` What was the lesson to learn from the success of the zeta function? Why do products of this type inherently contain interesting information?

Number of proper walks A_r. Note $A_1 A_r = A_{r+1} + (k-1)A_{r-1}$, so we get prop 11.

1! A closed geodesic which is not the power of another one is a prime geodesic. Equivalent only if cycle.

Definition 3.2.14: Ihara zeta function

$$Z_X(s) = \prod_p (1 - q^{-s\ell(p)})^{-1}$$

satisfies Riemann hypothesis iff X is Ramanujan graph!

?? "These constructions raise the intriguing question of whether there is a generalization of the notion of a graph to that of a supergraph' whose zeta function would (in some cases) coincide with those higher dimensional zeta functions of varieties.

3 Techniques

3.1 LLL

3.2 Techniques

Lovasz Local Lemma.

Understanding 18.997 notes.

Partial motivations? When 12 and 23 are edges, but not 13, need $(1-p_1)(1-p_3)+p_1+p_2 > 1$.

Idea: induction on number of vertices. For each new edge, somehow treat the neighbors and non-neighbors differently. We expand as a product:

$$P\left(\bigwedge_{i=1}^{n} \overline{A_i}\right) = \prod_{i=1}^{n}\left(1 - P\left(A_i | \bigwedge_{k=1}^{i-1} \overline{A_k}\right)\right) \ge (1-x_1)\cdots(1-x_n).$$

To get this we want to bound each $P\left(A_i|\bigwedge_{k=1}^{i-1}\overline{A_k}\right)$ away from 1, say it's less than x.

SUBPROBLEM: *Bound each* $P\left(A_i|\bigwedge_{k=1}^{i-1}\overline{A_k}\right)\le\bullet$. *This is where induction actually take place.* Note for each A_i it's natural to split the rest of the set into 2 parts, they'll somehow contribute differently; S_1, the dependent stuff, and S_2, the independent stuff. (We bound trivially)

$$P\left(A_i|\bigwedge_{k=1}^{i-1}\overline{A_k}\right)\le P\left(A_i|\bigwedge_{k\ne i}\overline{A_k}\right).$$

We should somehow be able to get rid of the independent stuff but we have to be careful because S_1 could depend on S_2. So we consider $P(A|B\wedge C)$, B is not for S_1 and C is S_2. Then bound ABOVE by

$$P(A|B\wedge C)\le\frac{P(A)}{P(B|C)}.$$

Does this make sense? We need to use independence of A and C somewhere, to decouple A from C; we "throw away" B (how optimal is this?). Bottom just need to bound BELOW, this is INDUCTION HYPOTHESIS. Again break up as product, want $P(\overline{A_j}|\bullet)$ bounded from ABOVE, which matches IH.

3.3 Entropy

Comments

References:

- Probabilistic method, Ch. 15
- Some intersection theorems for ordered sets and graphs, F. Chung and R. Graham. (Original application. Nice proof that any system of graphs with $F\cap F'$ connected has at most $2^{\binom{n}{2}-\frac{n}{2}}$ elements.)
- Hypergraphs, entropy, and inequalities, E. Friedgut. (in AMM)

Nice translation between picture and inequalities like

$$\int f(x,y)g(y,z)h(z,x)\,dxdydz\le\sqrt{\int\int f^2(x,y)\,dxdy\int g^2(y,z)\,dydz\int h^2(x,z)\,dxdz}.$$

(Note: it's easier to think about Shearer's entropy lemma first. Prove it in the natural way. The difficulty is in: how to divide into the individual elements without destroying the inequality? Solution: don't use the inequality $H(X_1,X_2,\ldots)\le H(X_1)+H(X_2)+\cdots$ but rather equality $H(X_1,X_2,\ldots)=H(X_1)+H(X_2|X_1)+\cdots$. Is there some duality between that and the inequality in the problem below?)

MOVED to blog post!

4 Extremal combinatorics

2-15-14 Examples MOVED to combo notes.

Chapter 4

Computation

1 QIT

1.1 Questions

See paper for a prelim web for QIT.

Insights and questions

1. What is the relationship of the Bloch sphere to the map $SU_2 = \mathbb{S}^3 \overset{\cong}{\to} SO_3$? Note that $s = (0,0,1)$ corresponds to the kernel $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $(1,0,0)$ to $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$, $(0,1,0)$ to $\begin{pmatrix} 1 \\ -i \end{pmatrix}$; they correspond to I, i, $-k$ in SU_2 (sort-of). cf. p. 105 (2.72) in NC. There seems to be an angle-halving thing going on.

   It seems SO_3 is acting on the Bloch-sphere through SU_2-conjugation.

2. The relative trace map is the dual of the inversion map. Note a space of linear operators on a finite-dimensional space (i.e. matrices) is naturally self-dual, $A^* \otimes A$. Downloaded a paper on Stinespring.

3. What is the basis-less way to define the trace?

4. Proving Stinespring using $B(H_A)$ as the ancilla. (Ask functional analyst about significance of Stinespring)

1.2 Quantum entropy

1. Quantum teleportation: Alice and Bob share a maximally entangled 2-qubit state. Alice wants to send a qubit without a quantum channel. How?

   Clarification: it's a different qubit, and she wants Bob to have a copy of it at the end. (She doesn't need to keep her qubit.)

   How might we discover this? We want something that takes the information in C and somehow transfers it to B.

Nice way to think about; the change-of-basis matrix from $|00\rangle\rangle, |01\rangle\rangle, |10\rangle\rangle, |11\rangle\rangle$ to the Bell states is ...

2. Shannon entropy: "It quantifies the minimal physical resources (i.e., the minumum number of bits) needed to store information emitted per use of a classical information source. It provides a limit to which data can be compressed reliably, i.e., in a manner which allows the recovery of the original data with a low probability of error." For quantum source, **von Neumann entropy** $S(\rho) = -\text{tr}(\rho \lg \rho)$.

   TODO: prove concavity.

Proof of properties of entropy follows from an important inequality.

Theorem 4.1.1 (Klein)**:** Define the **quantum relative entropy** of a state $\rho \in \mathcal{D}(H)$ and a positive semi-definite $\sigma \in \mathcal{B}(H)$ by

$$D(\rho|q) = \text{tr}(\rho(\lg \rho - \lg \sigma)).$$

We require $\text{Supp}(\rho) \subseteq \text{Supp}(\sigma)$.

Then

$$D(\rho|\sigma) \geq 0,$$

equality iff $\rho = \sigma$.

Proof. Intimidated by the fact they aren't simultaneously diagonalizable. No fear, just follow the math: write out the spectral decompositions, note that we get dot products between the eigenvectors (coefficients may be less than 1, this looks good), we get coefficients elements of doubly stochastic P. Now use concavity of log, get in terms of classic relative entropy with probabilities $\sum_\alpha p_{i\alpha} q_\alpha$.

(Can probably be written better with matrices.) □

Define quantum joint entropy, conditional entropy, mutual information. What makes these different from classical?

! Quantum conditional entropy can be negative, $S(Y) \geq S(X, Y)$. Less disorder when you look at a larger system.
Example: Bell state, ρ_A is completely mixed, but $S(A, B) = 0$.

1. How does tensoring affect entropy? Additivity $S(\rho_A \otimes \rho_A) = S(\rho_A) + S(\rho_B)$. Just like proof with independents adding.

2. Subadditivity: use $D(\rho|\sigma) \geq 0$ on $\sigma = \rho_A \otimes \rho_B$.

3. If composite system is in a pure state, then entropies of subsystems equal. (Pf. Schmidt decomposition—symmetric.)

4. Triangle inequality.

   $$S(\rho_{AB}) \geq |S(\rho_A) - S(\rho_B)|.$$

   Introduce reference system purifying. (Philosophically, why does this work?)

5. Strong subadditivity. $S(\rho_{ABC}) + S(\rho_B) \le S(\rho_{AB}) + S(\rho_{BC})$.

   (a) Further conditioning reduces entropy: $S(A|BC) \le S(A|B)$. (We already get $S(A|B) \le S(A)$ by subadditivity.)

   (b) Discarding quantum systems never increases mutual information.

   (c) Quantum operations (CPTP) *on one subsystem* don't increase mutual information.

   Pf. (Note that $I_A \otimes$ disappears under partial trace.) Key: Stinespring dilation applied to ρ_{AB}. Note the mutual info is the same in the larger system by the way we defined it $I(A:B) = I(A:BC)$. No information loss in the larger system $I(A:BC) = I(A':B'C')$ (note that operating on one part of the system doesn't change the partial trace to the other part—checkme. Unitary transformation preserves entropy, because trace preserved under conjugation). Adding C doesn't change I, tossing away this part can only decrease it.

1.3 Problems

1.3.1 Examples 2

Examples class

1. (a) We have $\lambda \langle \varphi|\psi\rangle = \langle \varphi|A|\psi\rangle = \mu \langle \varphi|\psi\rangle$.

   (b) Note $A - A^\dagger$ is normal, so is diagonalizable. We have $v^\dagger A v = 0$ for all v. Thus A must be 0.

   (c) Look at an eigenspace of A. On that eigenspace, $A(Bv) = BAv = \lambda(Bv)$, so B takes the eigenspace to itself.

2. Hermitian matrices are of the form $\begin{pmatrix} a & c+di \\ c-di & b \end{pmatrix}$. Density matrices have trace 1 so $a + b = 1$. We can write it as

$$\frac{1}{2}(\underbrace{(a+b)}_{1} I + c\sigma_1 + d\sigma_2 + (a-b)\sigma_3).$$

   The north/south pole are $\frac{1}{2}(I \pm \sigma_z) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

   Pure states are in the form $\frac{1}{2}\begin{pmatrix} 1+a & b-ci \\ b+ci & 1-a \end{pmatrix}$; their determinant is 0: $1 - a^2 - b^2 - c^2 = 0$, so $a^2 + b^2 + c^2 = 0$.

   Now consider $\frac{1}{2}(1 + d\vec{s} \cdot \vec{\sigma})$ for $\|\vec{s}\| = 1$ and $d \ge 0$; for $d = 0$ eigenvalues are 1, for $d = 1$ one eigenvalue is 0, so for $d \le 1$ it is positive, for $d > 1$ it is not. Alternatively use the criterion that a matrix is positive (sd) if all principal minors are positive (nonnegative); the determinants of the minors are $1 + a$, $1 - \|s^2\|$. (Alternatively, $\mathrm{tr}(\sigma_k \rho) = s_k$—the σ_k

are orthogonal wrt the trace inner norm. The sum of these coefficients sqaured must be at most 1, for a density matrix they are 1.)

The completely mixed state is the center.

3. We have

$$s_x = \operatorname{tr}\left(\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\rho\right) = \frac{1}{2}$$
$$s_y = \operatorname{tr}\left(\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\rho\right) = \frac{1}{3}$$
$$s_z = \operatorname{tr}\left(\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\rho\right) = \frac{1}{5}$$

This is a mixed state because the sum of these squared is less than 1. There is $\operatorname{tr}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\rho = \frac{3}{5}$ chance of it being 1.

4. Use the representation in 2 and note that the unit ball $B \in \mathbb{R}^3$ is convex.

5. The state is maximally entangled with the partial trace is I/d. Let M be the matrix of coefficients. $\operatorname{tr}_A(|M\rangle\rangle\langle\langle M|) = MM^\dagger = I/d$; the columns are orthogonal with norm $\frac{1}{\sqrt{d}}$.

6. Note that $A \otimes B|\rho\rangle\rangle = |A\rho B^\dagger\rangle\rangle$. Thus, identifying $B(H)$ with $H \otimes H$ via $|\bullet\rangle\rangle$, Kraus representation reads as

$$|\Phi(\rho)\rangle\rangle = \sum_i A_i \otimes A_i |\rho\rangle\rangle$$

Now consider the map $B(H)\otimes B(H) \overset{\cong}{\to} B(H\otimes H)$, $\sum_i A_i \otimes A_i$ is mapped to $\sum_i |A_i\rangle\rangle\langle\langle A_i|$. This is a positive semidefinite quadratic form on $H \otimes H$ so it can be written as a sum of at most d^2 terms.

Motivation: d^2 suggests a linear dependence argument. The initial attempt fails, because note the function seems quadratic. This leads naturally to:can we describe the problem using quadratic forms? I was confused for a time about the right way to make the isomorphism (lots of tensor products and duals...), but the lemma on the vector-matrix correspondence fit perfectly. It's not quadratic forms after all, it's just tensor product. I wonder if we can proved d^2 in Stinespring dilation with Kraus's d^2?

7.

Revisit Ex. 4, 9, 10, 13, 14 once solutions are up.

1.3.2 Examples 3

Example sheet 29th Nov

1. We have

$$\begin{aligned}\operatorname{tr}(\rho_{AB}T) &= \operatorname{tr}_A(\operatorname{tr}_B(\rho_{AB}(T_A \otimes I_B))) \\ &= \operatorname{tr}_A(\operatorname{tr}_B(\rho_{AB})T_A) \\ &= \operatorname{tr}_A(\rho_A T_A).\end{aligned}$$

   From first to second line—can just write out.

   We use $\log(\rho_A \otimes \rho_B) = \log \rho_A \otimes I_B + I_A \otimes \rho_B$. (Take the spectral decomposition, for instance. Alternatively, use the fact that if $[A, B] = 0$, then $\log(AB) = \log A + \log B$. This is from $e^X e^Y = e^{X+Y}$ iff $[X, Y] = 0$.)

   Then

$$\begin{aligned}-\operatorname{tr}(\rho_{AB}\log(\rho_A \otimes \rho_B)) &= -\operatorname{tr}(\rho_{AB}(\log \rho_A \otimes I_B + \log I_A \otimes \rho_B)) \\ &= -\operatorname{tr}_A(\rho_A \log \rho_A) - \operatorname{tr}_B(\rho_B \log \rho_B) \\ &= S(\rho_A) + S(\rho_B).\end{aligned}$$

2. Let $\sigma_{AB} = \sum_i p_i \rho_i \otimes |i\rangle\langle i|$. Then

$$\sigma_{AB} = H(p) + \sum_i p_i S(\rho_i).$$

   We have (note additivity under tensor product gives $S(\rho_i \otimes |i\rangle\langle i|) = S(\rho_i) + \underbrace{S(|i\rangle\langle i|)}_{0} = S(\rho_i)$)

$$\begin{aligned}S(\sigma_A) &= S(\sum_i p_i \rho_i) \\ S(\sigma_B) &= S(p_i \underbrace{\operatorname{tr}(\rho_i)}_{1} |i\rangle\langle i|) \\ &= H(p).\end{aligned}$$

   Then subadditivity $S(\sigma_{AB}) \leq S(\sigma_A) + S(\sigma_B)$ gives

$$S\left(\sum_{i=1}^r p_i \rho_i\right) \geq \sum_{i=1}^r p_i S(\rho_i).$$

3. The U_i are simultaneously diagonalizable.

$$\begin{aligned}S(\sum_i p_i U D_i U^\dagger) &= S((\sum_i p_i U D_i U^\dagger)(\log \sum_i p_i U D_i U^\dagger)) \\ &= -\operatorname{tr}(\sum_i p_i D_i \log(p_i D_i)) \\ &= -\operatorname{tr}(\sum_i p_i D_i (\log(p_i) I + \log D_i)) \\ &= -\sum_i p_i \log p_i \underbrace{\operatorname{tr}(D_i)}_{1} + \sum p_i S(\rho_i)\end{aligned}$$

4. Recall we had something like $\sum p_i \log p_i \geq \sum_{i,j} p_i \log q_j \langle v_i | w_i \rangle^2$ which is like $p^t \log p \geq p^t \ln Aq \geq p^t A \lg q$ for a doubly stochastic matrix A. Since $-\log$ is strictly convex, for equality in the first we must have the Aq distribution being p, in the second we must have $q = Aq$. (Note: what if $p_i = 0$? A is allowed to act however on $(\operatorname{Supp} \rho)^\perp$, however Aq must still be p.)

   Alternatively, write as $D(\{\lambda_i\} || \{\sum_\alpha p_{i\alpha} q_\alpha\}) \geq 0$, with equality only if distributions the same.

   (b) When they commute, there is a mutual basis of eigenvectors. $D(\mu||\sigma) = D(\{\lambda_i\}||\{\mu_i\})$. When they don't commute, we can only write $D(\{\lambda_i\}||\{\sum_\alpha p_{i\alpha} q_\alpha\})$.

   (c) Look at $D(\rho||\sigma) \geq 0$ where σ is completely mixed.

5. Note

$$D(\rho||\sigma) = \sum_i p_i D(\rho_i||\sigma_i)$$

   by Exercise 3. Let Λ send ρ to $\sum |0\rangle\langle 0| \otimes p_i \rho_i$. (To see we can choose Λ CPTP, note it's $\Lambda(\rho) = \sum A_i \rho A_i^\dagger$ where

$$A_i = |0\rangle\langle i|$$

   sends $|i\rangle$ to $|0\rangle$ and is 0 on $|0\rangle^\perp$.) Now use Problem 11.

   Actually easier: use ULM directly. LHS is $D(\rho_A||\sigma_A)$.

6. Let $\rho' = \sum p_i \rho^i_{AB}$. We need to show

$$S(A|B)_{\sum p_i \rho^i_{AB}} \geq \sum_i p_i S(A|B)_\rho.$$

   The LHS is

$$\begin{aligned} S(\sum_i p_i \rho^i_{AB}) - S(\operatorname{tr}_A \sum p_i \rho^i_{AB}) &= -\operatorname{tr}_B(\operatorname{tr}_A((\sum \rho_i \rho^i_{AB}) \log(\sum_i \rho_i \rho^i_{AB}))) \\ &\quad - [-\operatorname{tr}_B(\operatorname{tr}_A(\sum \rho_i \rho^i_{AB}) \log \operatorname{tr}_A(\sum_i \rho^i_{AB}))] \\ &= -\operatorname{tr}_B \operatorname{tr}_A(\rho' \log \rho' - \rho' I_A \otimes \log \operatorname{tr}_A \rho') \\ &= -D(\rho'||I_A \otimes \operatorname{tr}_A \rho'). \end{aligned}$$

   Instead of I_A adjoin a random $|0\rangle\langle 0|$. The RHS is

$$\begin{aligned} \sum_i p_i(S(\rho^i_{AB}) - S(\operatorname{tr}_A(\rho^i_{AB}))) &= -\sum_i p_i \operatorname{tr}_B(\operatorname{tr}_A(\rho^i_{AB} \log \rho^i_{AB}) - \operatorname{tr}_A(\rho^i_{AB} \operatorname{tr}_A \log \rho^i_{AB})) \\ &= -\sum_i p_i D(\rho^i_{AB}||I_A \otimes \operatorname{tr}_A \rho^i_{AB}). \end{aligned}$$

   Now use problem 5.

7. We have

$$S(A|B)_{\rho_{AB}} = S(A|BC)_{\rho_{ABC}} = S(A|B'C)_{\sigma_{AB'C}} \leq S(A|B')_{\sigma_{AB'}},$$

the second equality by fact the unitary operation is independent of A (does not impinge on it), the inequality by "conditioning decreases relative entropy."

Felix: $\omega_{AB'C} = (1_A \otimes U)\rho_{AB} \otimes \rho_\varphi (1_A \otimes U^\dagger)$.

8. What is this good for?

   (a)

$$\frac{1}{2}I(A:B)+\frac{1}{2}I(A:E) = \frac{1}{2}(-AB+A+B-AE+A+E) = \frac{1}{2}(B+E-AB-AE)+A = A.$$

   (b)

$$\frac{1}{2}(A:B-A:E) = \frac{1}{2}(-AB+A+B+AE-A-E) = \frac{1}{2}(2B-2AB) = I_c^{A>B}.$$

9. I'm confused about question 9. We clearly have $\mathcal{B}(\mathcal{H}_A)\otimes\mathcal{B}(\mathcal{H}_B) \cong \mathcal{B}(H_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}})$. So $\sigma_A \otimes \tau_B$ clearly span the whole space. Do we want the σ_A, τ_B to be *density* matrices?

10. For convenience, extend definition of S to all diagonalizable matrices.

$$\begin{aligned} S(\rho') = S(\sum_i P_i\rho P_i) &= -\sum \operatorname{tr}(P_i\rho P_i \log(P_i\rho P_i)) \\ &\geq -\sum \operatorname{tr}(\rho \log \rho P_i) \\ &= S(\rho). \end{aligned}$$

Felix: $[P_i, \rho'] = 0$ implies $[P_i, \log\rho'] = 0$ either by simultaneous diagonalizability, or analyticity of log. (Holds for arbitary operators?) Is log well defined for Jordan matrix with positive eigenvalues?

OR: measurement is CPTP.

11. Lindblad-Uhlmann Monotonicity says

$$D(\rho_A||\sigma_A) \leq D(\rho_{AB}||\sigma_{AB}).$$

We use Stinespring dilation, adjoining B, conjugating by unitary, taking trace.

$$D(\rho_A||\sigma_A) = D(\rho_{AB}||\sigma_{AB}) = D(\rho'_{AB}||\sigma'_{AB}) \geq D(\Lambda(\rho_A)||\Lambda(\sigma_A)),$$

the first is that adjoining a pure state doesn't change entropy, the middle is invariance under unitary, the last by monotonicity.

(Details. $\Lambda\rho = \operatorname{tr}_B(U(\rho\otimes|\varphi\rangle\langle\varphi|)U^\dagger)$.

Why invariant under unitary? Eigenvalues and inner products don't change under unitary transformations. Or: trace is cyclic.)

"Data processing inequality." Can prove lots of data processing inequalities. Instead of taking an ancilla, take an isometry $U: \mathcal{H}_A \to \mathcal{H}_B$, $\Lambda(\rho) = \operatorname{tr}_E(U\rho U^\dagger)$ (note $U^\dagger U = 1_A$, $UU^\dagger = \pi_{U(\mathcal{H}_A)} : \mathcal{H}_{AE} \to \mathcal{H}_{AE}$.

1.3.3 Examples 4

1. The HSW theorem gives the product state capacity in terms of a maximum of the Holevo χ quantity, cf. how the classical noisy coding theorem gives the capacity in terms of the mutual information. Letting $\rho = \sum p_i \rho_i$,

$$\text{eq:qitex4-1}C_{\text{cl}}^{(1)}(\Lambda) = \max_{\{p_i,\rho_i\}} \chi(\{p_i, \Lambda(p_i)\}) = \underbrace{\max_{\{p_i,\rho_i\}} S(\Lambda(\rho))}_{(b)} - \underbrace{\sum_i p_i S(\Lambda(\rho_i))}_{(a)}. \tag{4.1}$$

   We can maximize over pure states $p_i = |\psi_i\rangle\langle\psi_i|$, in which case

$$\Lambda(p) = p|\psi_i\rangle\langle\psi_i| + (1-p)\frac{I}{2}.$$

   (a) In a basis where ψ_i is one of the vectors, we have that the matrix for $\Lambda(p)$ is $p\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right) + (1-p)\left(\begin{smallmatrix}\frac12&0\\0&\frac12\end{smallmatrix}\right) = \left(\begin{smallmatrix}\frac{1+p}{2}&0\\0&\frac{1-p}{2}\end{smallmatrix}\right)$. Hence

$$\text{eq:qitex4-1}\sum_i p_i S(\Lambda(\rho_i)) = H\left(\frac{1+p}{2}\right). \tag{4.2}$$

   This is independent of the ensemble.

   We expect this as it is symmetric; it treats every pure state ρ equally.

   (b) We are hence reduced to maximizing (b). Noting Λ is convex-linear, we get (b) equals

$$S\left(p\rho + (1-p)\frac{I}{2}\right).$$

   Diagonalizing $\rho = \left(\begin{smallmatrix}\lambda&0\\0&1-\lambda\end{smallmatrix}\right)$, we find that

$$S\left(p\rho + (1-p)\frac{I}{2}\right) = S\begin{pmatrix}p\lambda+\frac{1-p}{2}&0\\0&-p\lambda+\frac{1+p}{2}\end{pmatrix} = H\left(p\lambda + \frac{1-p}{2}\right)$$

   This is maximized when $\lambda = \frac12$, and equals $h\left(\frac12\right) = 1$.

   The capacity is $\boxed{1 - h\left(\frac{p+1}{2}\right)}$, achieved by any ensemble whose density matrix $\sigma = \frac{I}{2}$ is the completely mixed state. (For example, take $\rho_1 = |0\rangle\langle 0|, \rho_2 = |1\rangle\langle 1|$.)

2. Abbreviate $s = \sin\theta$ and $c = \cos\theta$. We have

$$\rho_1 = \begin{pmatrix}0&0\\0&1\end{pmatrix}$$
$$\rho_2 = \begin{pmatrix}s^2&sc\\sc&c^2\end{pmatrix}$$
$$\rho = \frac12\rho_1 + \frac12\rho_2 = \begin{pmatrix}s^2/2&sc/2\\sc/2&(1+c^2)/2\end{pmatrix}.$$

By calculation, the eigenvalues are $\frac{1\pm c}{2}$. Thus

$$\chi\left(\left\{\frac{1}{2}, \Lambda(p_i)\right\}\right) = H\left(p\left(\frac{1+c}{2}\right) + \frac{1-p}{2}\right) - H\left(\frac{1+p}{2}\right),$$

maximized when $\theta = \pm 90^\circ$, $c = 1$, and this equals $1 - H\left(\frac{1+p}{2}\right)$, as in Exercise 1 (which shows a way to attain the bound in exercise 1).

3. The answer is n, as $S(\Lambda(\rho)) \le n$ (using $H(J) \le n$ when J attains at most n values), and $S(\Lambda(\rho_i)) \ge 0$.

4. (a) We check

$$\begin{aligned}\operatorname{tr}_B|\Psi\rangle\langle\Psi| &= \operatorname{tr}\left(\sum \rho^{\frac{1}{2}}|e_i\rangle \otimes |e_i\rangle\right)\left(\langle e_i|\rho^{\frac{1}{2}} \otimes \langle e_i|\right) \\ &= \operatorname{tr}\sum \rho^{\frac{1}{2}}|e_i\rangle\langle e_i| \otimes |e_i\rangle\langle e_i| \\ &= \sum \rho^{\frac{1}{2}}|e_i\rangle\langle e_i|\rho^{\frac{1}{2}} = \rho.\end{aligned}$$

Letting $\rho = \sum p_i|i\rangle\langle i|$, the Schmidt purification is

$$|\Phi\rangle = \sum \sqrt{p_i}|i\rangle|e_i\rangle$$

while

$$|\Psi\rangle = \sum \sqrt{p_i}|i\rangle\langle i|e_i\rangle \otimes |e_i\rangle.$$

(b)

$$\operatorname{tr}(AB^T) = \langle\langle I|AB^T\rangle\rangle = \langle\langle I|A \otimes B|I\rangle\rangle = \langle\Omega|A \otimes B|\Omega\rangle.$$

5. We use the fact that fidelity is equal to the maximum dot product over purifications. This is so we can work with pure states.

$$F(\rho,\sigma) = \max|\langle\psi_\rho^{AB}|\psi_\sigma^{AB}\rangle|.$$

Let ψ, ϕ denote these purifications. Diagonalize so that $|\psi\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, $|\phi\rangle = \begin{pmatrix}a\\b\end{pmatrix}$, $|\psi\rangle\langle\psi| = \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$, $|\phi\rangle\langle\phi| = \left(\begin{smallmatrix}\overline{a}a&\overline{a}b\\\overline{b}a&\overline{b}b\end{smallmatrix}\right)$. We have

$$\begin{aligned}1 - F(\rho,\sigma) &= 1 - |a| \\ \sqrt{1 - F(\rho,\sigma)^2} &= \sqrt{1 - |a|^2} \\ \|\rho - \sigma\|_1 &\le \max_P \operatorname{tr}(P \otimes I(|\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|)) \\ &\le \max_P \ldots = F(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = \sqrt{1 - |a|^2}.\end{aligned}$$

6. (a) Since P is a projection, the vector $|\phi\rangle$ can be written as a weighted sum of two orthogonal vectors $|\alpha\rangle$ and $|\beta\rangle$, $|\phi\rangle = a|\alpha\rangle + b|\beta\rangle$, for $a, b \ge 0$, such that $P|\alpha\rangle$ and

$P|\beta\rangle = 0$. Then

$$\begin{aligned}
\rho &= a^2|\alpha\rangle\langle\alpha| + ab(|\alpha\rangle\langle\beta| + |\beta\rangle\langle\alpha|) + b^2|\beta\rangle\langle\beta| \\
\overline{\rho} &= |\beta\rangle\langle\beta|\rho|\beta\rangle\langle\beta| = b^2|\beta\rangle\langle\beta| \\
\|\rho - \overline{\rho}\|_1 &= \left\| \begin{pmatrix} 0 & ab \\ ab & b^2 \end{pmatrix} \right\|_1 \\
&= \frac{b^2 + \sqrt{b^4 + 4a^2b^2}}{2} + \frac{-b^2 + \sqrt{b^4 - 4a^2b^2}}{2} \\
&= b\sqrt{b^2 + 4a^2} \\
&\leq 2\sqrt{1 - a^2}
\end{aligned}$$

(b) We have

$$\begin{aligned}
\|\rho - \overline{\rho}\|_1 &= \left\| \sum \lambda_i(\rho_i - \overline{\rho_i}) \right\|_1 \\
&\leq \sum \lambda_i \left\|(\rho_i - \overline{\rho_i})\right\|_1 \leq 2\sum_i^d \lambda_i\sqrt{1 - \mathrm{tr}(\overline{\rho_i})}.
\end{aligned}$$

(c) By Jensen, since $\sqrt{}$ is concave, $\sum \lambda_i \sqrt{x_i} \leq \sqrt{\sum x_i}$. Thus

$$\|\rho - \overline{\rho}\|_1 \leq 2\sqrt{1 - \mathrm{tr}(\overline{\rho})}.$$

Alternate solution:

$$\begin{aligned}
\|P\rho P\|_1 &= \|(I - P + P)\rho - P\rho P\|_1 \\
&\leq \|(I - \rho)\rho\|_1 + \|P\rho(I - P)\|_1 \\
&= \mathrm{tr}((1 - \rho)\sqrt{\rho}\sqrt{\rho}) + \mathrm{tr}|P\sqrt{\rho}\sqrt{\rho}(I - \rho)| \\
&\leq \sqrt{\mathrm{tr}((I - \rho)^2\rho)\,\underbrace{\mathrm{tr}\rho}_{1}} + \sqrt{\underbrace{\mathrm{tr}(P^2\rho)}_{\mathrm{tr}(P\rho)\leq 1}\,\mathrm{tr}(\rho(I - P))} \\
&\leq \sqrt{\mathrm{tr}((I - P)\rho)} + \sqrt{\mathrm{tr}((I - P)\rho)} \\
&= 2\sqrt{1 - \mathrm{tr}(P\rho)} = 2\sqrt{1 - \mathrm{tr}(\overline{\rho})}.
\end{aligned}$$

using Cauchy-Schwarz with the trace norm. This doesn't use the fact that ρ is pure.

7. (a) $\langle\psi_i|\psi_j\rangle = -\frac{1}{2}$ for $i \neq j$.

(b) (i) 0 (ii) $\frac{2}{3}\left(I - \frac{1}{2}|\psi_x\rangle \underbrace{\langle\psi_x|\psi_y\rangle}_{-\frac{1}{2}}\langle\psi_y| \right) = \frac{1}{2}$.

(c) $I(X : Y) = H(X) - H(Y|X) = \log_2 3 - 1 \approx 0.585$.

(d) By calculation (see Mathematica notebook) $\rho = \begin{pmatrix} 3/8 & 0 & 0 & 1/8 \\ 0 & 1/8 & 1/8 & 0 \\ 0 & 1/8 & 1/8 & 0 \\ 1/8 & 0 & 0 & 3/8 \end{pmatrix}$ with eigenvalues $\frac{1}{2}, \frac{1}{4}, \frac{1}{4}$ so with entropy 1.5, or .75 per bit. (Note $\sum p_i S(\rho_i) = 0$ as each ρ_i has rank 1.)

(e) We actually need another E_z to form the POVM, since $\sum E_x$ has rank 3, is diag(1,1,1,0) in some basis. Now we get .9714, .0143.

(f)

$$\frac{1}{2}(\log_2(3) - (H(.9714, .0143, .0143))) \approx .685.$$

8. (a) We have that ρ'_{RQE} is a pure state, since ψ^ρ_{RQ} is a purification, so is ψ^ρ_{RQ}, and tensoring by $|0_E\rangle\langle 0_E|$ doesn't change this. Thus

$$S(\rho, \Lambda) = S(\rho'_{RQ}) = S(\rho'_E).$$

Note $S(\rho, \Lambda)$ is well-defined as we can change the purification by a unitary; just check that this doesn't change the trace.

(b) Let the Kraus representation be $\Lambda(\rho) = \sum_i A_i \rho A_i^\dagger$, $\sum_i A_i^\dagger A_i = I$. Extend $|0\rangle$ to $\{|i\rangle\}$. Then

$$U(|\psi_Q\rangle \otimes |0_E\rangle) = \sum_i A_i |\psi_Q\rangle \otimes |i_E\rangle.$$

and

$$\langle\psi|\langle 0|U^\dagger U|\varphi\rangle|0\rangle = \sum_k A_k^\dagger A_k \langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle.$$

This is the unitary appearing in Stinespring dilation.

$$\begin{aligned} \mathrm{tr}_E U(\rho \otimes |0\rangle\langle 0|)U^\dagger &= \sum_{i,j} A_i \rho A_j^\dagger \mathrm{tr}|i\rangle\langle j| = \Lambda(\rho) \\ \mathrm{tr}_{RQ} U(\rho \otimes |0\rangle\langle 0|)U^\dagger &= \sum_{i,j} \mathrm{tr}(A_i \rho A_j^\dagger)|i\rangle\langle j|. \end{aligned}$$

Then $S(\Lambda, \rho) = S(\rho'_{RQ}) - S(\rho'_E) = -\mathrm{tr} W \lg W$ with $W_{ij} = \mathrm{tr}(A_i \rho A_j)$.

9. Let $A = (\mathrm{id}_R \otimes \Lambda)|\Psi^\rho_{RQ}\rangle\langle\Psi^\rho_{RQ}|$ and $\lambda_1, \ldots, \lambda_{d^2}$ be its eigenvalues. Then

$$\begin{aligned} S(\rho, \Lambda) &= -\mathrm{tr}(A \lg A) \\ &= H(\{\lambda_j\}) \\ F_e(\rho, \Lambda) &= \langle\psi^\rho_{RQ}|A|\psi^\rho_{RQ}\rangle \\ &\le \max \lambda_j. \end{aligned}$$

Then using classical Fano,

$$\begin{aligned} S(\rho, \Lambda) &= H(\{\lambda_j\}) \\ &\le h(\lambda_{\max}) + [1 - h(\lambda_{\max})] \lg(d^2 - 1) \\ &\le h(F_e(\rho, \Lambda)) + [1 - F_e(\rho, \Lambda)] \lg(d^2 - 1) \end{aligned}$$

10. Choose $p_i, \rho_i, p'_i, \rho'_i$ the maximum for χ for Λ_1, Λ_2. Then

$$\begin{aligned}\chi^*(\Lambda_1) + \chi^*(\Lambda_2) &= \chi(\{p_i, \Lambda(\rho_i)\}) + \chi(\{p'_i, \Lambda(\rho'_i)\}) \\ &= \chi(\{p_i p'_j, \Lambda_1 \otimes \Lambda_2(\rho_i \otimes \rho'_j)\}) \\ &\le \chi^*(\Lambda_1 \otimes \Lambda_2).\end{aligned}$$

(Basically, write out in terms of S's, and use the fact that S of product states is the sum of the S's.)

11.

12. (a) First, letting $\omega = |w\rangle\langle w|$, $\omega = \sum_{i,j} \sqrt{\lambda_i}\sqrt{\lambda_j}|i\rangle\langle j| \otimes |i\rangle\langle j|$. $(I \otimes \Lambda)(\omega)$. See that linear, show for pure state, use spectral decomposition.

    Then $\omega = \sum w_n |\psi^n\rangle\langle\psi^n|$, put the second in.

    (b) Use the Choi-Jamilkowski isomorphism. Can take rank 1 operators.

$$\begin{aligned}|\widetilde{\Phi}\rangle\langle\widetilde{\Phi}| &= \frac{1}{d}\sum_{i,d} |i\rangle\langle j| \otimes |i\rangle\langle j| \\ (I \otimes \Lambda)(|\widetilde{\Phi}\rangle\langle\widetilde{\Phi}|) &= \frac{1}{d}\sum_{i,j} |i\rangle\langle j| \otimes \Lambda(|i\rangle\langle j|) \\ &= \sum_m p_m |u_m\rangle\langle u_m| \otimes |v_m\rangle\langle v_m|\end{aligned}$$

    (by separability assumption.) We want to show that

$$\begin{aligned}\Lambda(\rho) &= d\sum_m |v_m\rangle\langle v_m| \mathrm{tr}(\rho p_m |u_m\rangle\langle\rangle)| \\ \Lambda(|\widetilde{\Phi}\rangle\langle\widetilde{\Phi}|) &= \sum_{m,j,k} |v_m\rangle\langle v_m| \mathrm{tr}(|j\rangle\langle k| p_m |u_m\rangle\langle u_m|).\end{aligned}$$

2 Quantum computation

2.1 Quantum computing since Democritus

[Read:2, Prec:1]

Outline of Aaronson's book.

10 Quantum computing To define BQP, we need 4 conditions.

1. Initialization

2. Transformations: use a simple set of quantum gates. To learn about—

    - Toffoli and Hadamard are universal. `http://www.arxiv.org/abs/quant-ph/0205115`

- Solovay-Kitaev: any universal set efficiently simulates any other http://www.arxiv.org/abs/quant-ph/0505030
- Gottesman-Knill: Hadamard and CNOT can be classically simulated efficiently http://www.arxiv.org/abs/quant-ph/9807006

3. Measurement: can simulate measurement using quantum gate by CNOT

4. Uniformity: classical algorithm to make circuit. Exercise. ?? Is this meant to be recursive?

Uncomputing: $BQP^{BQP} = BQP$. Bennett (1980s): run subroutine, copy answer (why does no-cloning not apply here? because it's a pure state?), run backwards.

Inclusions:

$$BPP \subseteq BQP \subseteq PP$$

1. BPP in BQP because flipping coin is $H|0\rangle$.

2. BQP in EXP by simulation. In PP by Adleman, DeMarrais, Huang. Idea: Feynman path integral. p_{accept}: sum over all computational paths that lead to an accepting basis state. Determining whether $p_{accept} \geq \frac{1}{3}$ is a PP problem.

Suspect: BPP≠BQP because Shor's algorithm factors. http://www.scottaaronson.com/blog/?p=208

Simon's algorithm "secret XOR-mask." Idea; use fourier transform for $(\mathbb{Z}/2)^N$ to extract hidden periodicity info. There is an oracle relative to which BPP≠BQP. Understand this.

Recursive Fourier sampling. Given $f(x) = \langle s, x\rangle$, prep $2^{-n/2}\sum(-1)^{f(x)}|x\rangle$, apply H, get $|s\rangle$ checkme. Recurse. Quantum algorithm can do with 2^d queries, 2 b/c uncompute.

Is BQP in PH? Fourier checking as candidate problem for oracle separation http://www.scottaaronson.com/papers/bqpph.pdf.

BBBV: Oracle where NP$\not\subseteq BQP$. Quantum search needs $2^{n/2}$ times, because quantum mechanics is based on 2-norm. After T queries, approximately $\frac{1}{T}\sqrt{N}$ amplitude of guessing correctly.

Deutsch: Computational resources come from multiverse (145), cf. consciousness computing in Anathem. For this interpretation to work, different branches of the multiverse have to interfere. http://www.scottaaronson.com/papers/philos.pdf

3 Pset 1

1. (Bernstein-Vazirani problem)

   (a) Note $B_n \twoheadrightarrow B_1$ is a surjective group homomorphism, so it has kernel $\frac{|B_n|}{|B_1|} = \frac{|B_n|}{2}$.

   (b) Given k queries, the algorithm can differentiate at most 2^k possibilities.

Understanding H: we have

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

and $H = ((-1)^{xy})_{0\le x,y\le 1}$ in matrix form.

Hence

$$H_n|a\rangle = \bigotimes_n \sum_{y_i=0}^{1} (-1)^{x_i y_i}|y_i\rangle = \boxed{\sum_y (-1)^{x\cdot y}|y\rangle}.$$

(c)

$$\begin{array}{ccc} & U_f & H \\ & | & \\ \times \quad H & | & \end{array}$$

U_f gives $(-1)^{f_a(x)}|x\rangle(|0\rangle - |1\rangle)$, Hadamarding by H_n gives $|a\rangle(|0\rangle - |1\rangle)$ since $H^2 = I$.

2. Double-and-add. (See 18.783)

3. (Simon's algorithm)

(a)

$$\begin{array}{ccccc} \text{input} & H & U_f & & H \\ \text{input} & H & | & & H \\ 0 & - & | & \text{measure} & \\ 0 & - & | & \text{measure} & \end{array}$$

Applying H to each qubit gives $\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n}$. Applying U_f gives $\frac{1}{2^{n/2}} \sum_{a\in B^n} |a\rangle|f(a)\rangle$. Measuring the output register gives

$$\left(\sum_{b\in f^{-1}(a)} |b\rangle\right)|a\rangle = (|b+\xi\rangle + |b\rangle)|a\rangle$$

where $b \in f^{-1}(a)$ arbitary. This does not give information.

(b) We have

$$H_n(|b+\xi\rangle + |b\rangle) = \sum_y (-1)^{(b+\xi)\cdot y}|y\rangle + (-1)^{b\cdot y}|y\rangle = 2\sum_{y,\xi\cdot y=0} |y\rangle;$$

the solutions to $\xi \cdot y = 0$ constructively interfered. They all have equal probability, $\frac{1}{2^{n-1}}$.

(c) The probability that a $(n-1)$ vectors span a $(n-1)$-dimensional subspace is $(1-\frac{1}{2^{n-1}})\cdots(1-\frac{1}{2}) \ge \frac{3}{8}(1-\frac{1}{8}-\frac{1}{16}-\cdots) = \frac{3}{8}\frac{3}{4} = \frac{9}{32} \ge \frac{1}{4}$.

(d) The probability of not winning after n runs is at most $(1-\frac{1}{4})^n$. If we want this to be at most p, then we want

$$\begin{aligned}\left(1-\frac{1}{4}\right)^n &\le p\\ n\ln\frac{3}{4} &= \ln p\\ n &= \frac{\ln p}{\ln\frac{3}{4}} = O(\ln p).\end{aligned}$$

(e) Just query a constant number of times.

4. THIS IS NOT ACTUALLY NECESSARY: [Applying CX to a unentangled vector $(\alpha|0\rangle+\beta|1\rangle)\otimes(\gamma|0\rangle+\delta|1\rangle) \in \mathbb{C}^2\otimes\mathbb{C}^2$ (represented by matrix $\left(\begin{smallmatrix}\alpha\gamma & \alpha\delta\\ \beta\gamma & \beta\delta\end{smallmatrix}\right)$) gives $\left(\begin{smallmatrix}\alpha\gamma & \alpha\delta\\ -\beta\delta & -\beta\gamma\end{smallmatrix}\right)$. This is separable iff the matrix has rank 1, iff the determinant is 0, i.e., $\alpha\beta(\delta^2-\gamma^2)=0$, iff either

(a) the first vector is a multiple of $|0\rangle$ or $|1\rangle$, or

(b) $\gamma = \pm\delta$, the second vector is in the Hadamard basis (or a multiple thereof).]

We claim (by induction) that given a time and a register there are ≤ 2 possibilities for what the qubit there could be (it makes sense to say this since it's unentangled). At each CX there are 4 possibilities going in, and 4 possibilities going out. We can represent these by 0's and 1's, and replace the CX's with classical gates.

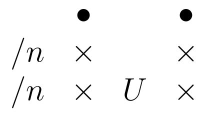
5. (a) This is clear as an unitary transformation can be defined by sending an ONB to an ONB.

(b) No, if we only operate on the parts individually it must remain a product state.

(c) By changing basis it suffices to show we can manufacture $\lambda|0\rangle|0\rangle+\mu|1\rangle|1\rangle$. Apply $|0\rangle \mapsto \lambda|0\rangle+\mu|1\rangle$ to the first gate and then CX.

6. (a) It sends an ONB to an ONB.

(b)



If the control bit is 0, no swaps occur and we just get the original input out. If the control bit is 1, the input gets routed to the bottom register, where U is applied, then it gets routed back to the original register. (Written out: $\sum a\otimes v_1\otimes v_2$ goes to $\sum(a=0)|0\rangle\otimes v_1\otimes v_2+(a=1)|1\rangle\otimes v_2\otimes v_1$ goes to $\sum(a=0)|0\rangle\otimes v_1\otimes v_2+(a=1)|1\rangle\otimes v_2\otimes Uv_1$ goes to $\sum(a=0)|0\rangle\otimes v_1\otimes v_2+(a=1)|1\rangle\otimes Uv_1\otimes v_2$.

(c) Replace U by U_f with $n+m$.

7. We reduce this problem to the problem of finding the period of a function. Construct $f : B_{n+1} \to B_{n+1}$ where $f(0, x) = (0, f_0(x))$ and $f(1, x) = (1, f_1(x))$. The period of f is exactly $(1, u)$. f can be computed by the technique in problem 6.

$$\begin{array}{ccc} \bullet & & \bullet \\ \times & U_{f_0} & \times \\ \times & U_{f_1} & \times \end{array}$$

   where the middle and bottom registers each contain $m+n$ qubits, and the input is the first $n+1$ lines.

   Now apply Simon's algorithm to f. This finds u.

8. Easy.

9. (a) We need $\lceil \log_2 39^2 \rceil = 11$ qubits.

   (b) $N = 39$, $a = 5$, we get the period is 4. It is exactly periodic as $4 \mid 2048$.

   (c) We get $512k$ each with probability $\frac{1}{4}$. We have $\frac{1}{2}$ chance of getting the period unambiguously.

10. (a) $\lceil \log_2 21^2 \rceil = 9$.

    (b) $\frac{c}{2^m} = \frac{427}{512} = \frac{1}{1+}\frac{85}{512} = \frac{1}{1+}\frac{1}{6+}\frac{2}{85}$. $\frac{6}{7}$?

4 Unsorted

[Read: 1, Prec: 1]

Q: for what kind of existence questions is it true that either "A exists" or "A doesn't exist" consistently in all axiom systems (that include ZF)?

I.e., "P=NP" under one axiom system and not under another is impossible, right? Try to enumerate all programs, and try to write proofs that a program solves 3-SAT... what if a program solves 3-SAT but it is unprovable that it does? Well, still it either has to solve it or not solve it, and the existence of one under any axiom system gives a program that works under any axiom system, right? (Do I have my logic right?) If P=NP is there necessarily a certificate?

On the other hand, it is possible that P≠NP and there is no way to prove it, i.e., it's undecidable.

Chapter 5

Geometry

0.1 Riemannian geometry

From Gromov's book. [R:1, P:1]

Conditions we impose on distance (which gives some limitations)

1. Symmetric

2. Nondegeneracy (Kobayashi, Hofer metrics are problemsome)

Euclidean embeddings hide rather than reveal the true metric structure of Riemannian manifolds due to uncontrolled distortion.

Power of Riemannian geometry depends on elliptic Riemannian equations (Laplace-Hodge, Dirac, Yang-Mills), coming with Riemannian tensor but invisible on embedding.

$\mathbb{R}^n$ is not the best example: Tradition of homogeneous spaces where isometry group acts transitively. But hard evaluate metric invariants in terms of $g(x, y)$. $\mathbb{R}^n$ is the only self-similar space in the Riemannian category.

$K \le 0$: thinner geodesic triangles. Geometry of symmetric spaces, $S^n, \mathbb{CP}^n$ (positive curvature), $\mathrm{SL}_n \mathbb{R}/SO(n)$, $K \le 0$.

1. complex manifolds—bounded

2. symplectic—lagrangian submanifolds

3. homotopy category "continuous maps between spaces transform to distance decreasing maps between polyhedra"

4. discrete group

Mediate between extremes of isometric and continuous to get distance decreasing maps and λ-Lipschitz maps.

Interesting: metric behavior of sequences of compact spaces. (ex. a noncompact space)

Several notions of distance between metric spaces. "Metric convergence."

Convergence of spaces modulo $\mu = 0$. Ex. unit spheres S^i converge to single atom of unit mass.

Local to global: Lower bound on Ricci curvature of X implies measure doubling property.

Singular fractal spaces and maps.

Definition 5.0.1: dilatation

$$\mathrm{dil}(f) = \sup_{x,x'\in X, x\neq x'} \frac{d(f(x),f(x'))}{d(x,x')}.$$

Lipschitz: $\mathrm{dil}(f) < \infty$.

Length defined in terms of dilatation $\ell(f) \int_a^b \mathrm{dil}_t(f)\,dt$. (For continuous, define as sup of sum.)

Definition 5.0.2: Length structure: $C(I)$ of $f : I \to X$ with sheaf structure. ℓ satisfies (a) positivity, (b) restriction, juxtaposition, (c) invariance under parameter change (d) continuity.

Define metric $d_\ell(x, y) = \inf \ell(f)$.

Ex. Metric space. C continuous mappings, ℓ as above. In general $d_\ell \neq d$, with different topologies.

Can we use a metric on S^{n-1} to get metric on $\mathbb{R}^n$? Yes apparently. $|r_1 - r_2| + r \|s_1 - s_2\|^{\frac{1}{2}}$. d_ℓ is weird! Checkme. Koch snowflake.

Topologies for d, d_ℓ coincide iff for each $x \in X$ and $\varepsilon > 0$ there's a d-neighborhood of x in which each point is connected to x by curve of length at most ε.

When X is Riemannian manifold and f is differentiable, local dilatation at x is norm of derivative.

Induced length structures

1 Algebraic geometry

geo/ag/summary

1.1 Sheaves

Define a sheaf and morphism between sheaves. Phrase this in terms of exact sequences. Define a stalk. How is the morphism related to the morphisms on stalks?

- A presheaf of [category $\mathcal{C}$] is a contravariant functor from $\mathrm{Top}(X)$ (open subsets under inclusion) to $\mathcal{C}$. $\mathcal{C}$ can be abelian group, ring, algebra, etc. A morphism of sheaves corresponds to a natural transformation. Define subsheaf by requiring the maps $\mathscr{F}(U) \to \mathscr{G}(U)$ to be injective; define quotient sheaf on the sections as well.

- A sheaf satisfies uniqueness and existence of gluings.

- That is, the following is exact:

$$0 \to \mathcal{O}(U) \to \prod_{V\subseteq U} \mathcal{O}(V) \to \prod_{V\cap W} \mathcal{O}(V \cap W)$$

  where the last map is $(f \in \mathcal{O}(V), g \in \mathcal{O}(W)) \to (f - g \in \mathcal{O}(V \cap W))$.

- A stalk is a direct limit $\varprojlim \mathscr{F}(U)$. φ is an isomorphism iff every φ_P is an isomorphism. [Proof? not hard]
- The picture to have in mind is functions (algebraic, analytic, etc.) on a space.

Define kernels, cokernels, and images. How do these behave under stalks? What requires sheafification and why? What is the universal property of sheafification?

- Define them by $U \mapsto \bullet(\varphi(U))$ where $\bullet$ is kernel, cokernel, or image.
- Universal property of sheafification: $\exists! \mathscr{F}^+$:

$$\begin{tikzcd}
\mathscr{F}^+ \arrow[dr, dotted] & \\
\mathscr{F} \arrow[u] \arrow[r] & \mathscr{G}.
\end{tikzcd}$$

  [Define it as functions on U to the union $\cup_{P \in U} \mathscr{F}_P$ that are locally consistent. This adds in everything required by gluing.] Why do the cokernel and image require sheafification, but not the kernel?

- We show taking ker and im commute with stalking, and injectivity and surjectivity are preserved under stalking. (Hartshorne exer. II.1.2, 18.725.2.1) (To show this, use lemma: if $\varphi_P(s_P) = t_P$ then this is true for some open W. I.e., image presheaf is same as image when looking at small enough opens.)
- Left exactness of global sections. Note this will be important for cohomology later on. (Hartshorne exer. II.1.8, 18.725.2.2)

How do you transfer a sheaf between topological spaces?

- Given $f : X \to Y$, we define pushforward or direct image by $(f_* \mathscr{F})(V) = \mathscr{F}(f^{-1}(V))$. Pushforward is easier because inverse image of an open is open. The image of an open is not necessarily open, so we have to take a direct limit $(f^{-1}\mathscr{G})(U) = \lim_{f(U) \subseteq V} \mathscr{G}(V)$.

Is it sufficient to define sheaves over a base of the topology? How? Yes, idea of B-sheaves.

What are some common constructions, and why are they useful? Skyscraper sheaf, extending by zero.

How can we think of sections as functions?

1. A function vanishes at a point if $f_x \in \mathfrak{m}_x$. This is closed.

1.2 Schemes

Define schemes and scheme morphisms. Why do we require them to be morphisms of locally ringed spaces?

Describe schemes and morphisms on Spec A, Proj A. Show that the concept of scheme/-morphism captures the classical notion. What further information does it give?

What are scheme points?

What are functions on schemes, and what does it mean to evaluate at a point? Evaluation at a point is evaluation modulo a prime ideal.

What do open sets in schemes look like? They are dense when X is irreducible. In this case think of them as containing most points, i.e., the intersection of any two open sets is *large* and one minus the other is *small*, and closed sets are small (of lower dimension!). (This is different from the picture you get in topology and differential geometry!) Thus a "partition of unity" consists of functions summing to 1, each of which vanishes on a (small) closed set, and is nonzero most places.

1.3 Properties of schemes

How do you use the affine communication lemma? Which properties are affine local?

What are topological properties and their scheme analogues?

Discuss: finiteness conditions: (locally) noetherian, (locally) finite (type),

- Locally noetherian: covered by affine noetherians. Noetherian: +qc, equivalently, finite cover by affine noetherians. (pf) Local property—explain—H.II.3.2

- Locally of finite type: Cover $Y = \bigcup \operatorname{Spec} B_i$, $f^{-1}(V_i) = \bigcup \operatorname{Spec} A_{ij}$, finitely generated B_i-algebra. Finite type if each $f^{-1}(V_i)$ has *finite* affine cover, finite can choose $f^{-1}(V_i) = \operatorname{Spec} A_i$ *(affine, not just affine cover)*, with A_i *fg module.*

Discuss: irreducible, reduced, and integral.

- **Irreducible**: can't be written as a proper union of 2 closed subsets. "1 piece."
  - Every two opens intersect. Every open is dense. There is a generic point for the whole space.
  - In affine scheme, irreducible subsets↔prime ideals.

- **Reduced**: $\mathcal{O}(U)$ has no nilpotents for any U. "No fuzz."
  - For $\operatorname{Spec} A$, iff A has no nilpotents. (See V for how to think about nilpotent points.)
  - Equivalently, $\mathcal{O}_P$ have no nilpotents (H Ex. II.2.3).
  - Nilpotency can cause a function to vanish at all stalks.

- **Integral**: each $\mathcal{O}(U)$ is an integral domain.
  - For $\operatorname{Spec} A$, iff A is integral. (V 5.2G)
  - Integral iff reduced and irreducible. (H Pr. II.3.1, V 5.2G, Pf. $\Longrightarrow$ If reducible, get disjoint opens, $\mathcal{O}(U_1 \cup U_2) = \mathcal{O}(U_1) \times \mathcal{O}(U_2)$.

    $\Leftarrow$ If $fg = 0$, note that their vanishing sets $f_x \notin \mathfrak{m}_x$ are closed. By irreducibility, one of them vanishes at all stalks, so is nilpotent, so 0.)

Discuss: normal, factorial

-

Discuss: X-valued points. What is the relation to Yoneda's Lemma?

1.4 Properties of morphisms

Discuss: how do we think of properties of objects as properties of morphisms? Why is this useful?

- $\pi : X \to Y$ has P iff for every affine open $U \subseteq Y$, $\pi^{-1}(U)$ has P.
- "Fibers all have P." (Not just fiber-by-fiber, but behaves well as the fiber varies.)

Generalities about morphism. What makes a reasonable class of morphisms?

- (V 7.1.1) (1) Local on the target: π in the class means $\pi^{-1}(V) \to V$ in the class. True on open cover means tryue. (2) closed under composition. (3) Closed under base change, pullback, fiber product. *Always ask whether these hold!*
- (Affine-)Local on the source: check on (affine) open cover of X. [ex. open embedding is not local on the source: you can't check injectivity on the source! (V.7.1D)]

  1. How to prove affine-locality?

-

Discuss: primes in rings, and how it applies to AG. What is the significance of Nakayama's Lemma?

- $B \to A$ integral, integral extension, as generalization of field extensions. This can be checked locally, i.e., by localizing at b_j with $(b_1, \ldots, b_n) = 1$ (V7.2A PoU)

  What about integrality is preserved by quotients and localization?

  - integral: localization and quotient of B, quotient of A, NOT localization of A.
  - integral extension: NOT loc/quo of A, quo B. (V7.2B)

- How to conclude integrality? If A is finite B-algebra, then ϕ is integral. Pf. use the equivalence a is integral iff contained in subalgebra that is fg B-module. (V7.2.1-2)
- Lying over theorem: For integral extension, map on prime ideals (Spec) is surjective. (Noetherian, fg not needed.) V7.2.5. sketch proof

  Going-up for integral homomorphism. Chain $\mathfrak{p}_i$ lying over $\mathfrak{q}_i$, then second chain can be exteneded.

- NAK

Discuss: morphisms

- Affine: For every affine open $U \subseteq Y$, $\pi^{-1}(U)$ is affine. (V7.3.3) Affine-local on target. (7.3.4—not easy!)

Discuss: open immersions.

- Open embedding as ringed spaces. "Open subschemes."

Discuss: closed immersions. What makes them harder than open immersions? How can we begin to classify them?

1. Motivation: $\operatorname{Spec} A/I \to \operatorname{Spec} A$, $A \twoheadrightarrow A/I$. (Holds with H def by checking on stalks. H II.3.2.3, V8.1E)
2. Complication: A closed subset has many subscheme structures, $\mathfrak{a}$ for which $V(\mathfrak{a}) = Y$. (Ex. take $\mathfrak{p}^n$.)
3. 2 definitions. H p. 85: closed imbedding of topological spaces, and $f^\#$ surjective. V8.1.1 affine, for every π-open affine pair ($\pi^{-1}(\operatorname{Spec} B) \cong \operatorname{Spec} A$), $B \to B/I$ surjective. [motivation: reduce to affine case]

   Equivalence: V $\implies$ H. *We can detect closedness with an open cover. The property of being open/closed is local.* On the π-oaps we get $\operatorname{Spec} B/I \to \operatorname{Spec} B$, image $V(I)$. Surjectivity can be checked locally. (V 8.1A) H $\implies$ V.
4. Basic properties: finite, because B/I finite over B trivially. Closed under composition, because affine is, and successive quotient. (V 8.1B, 8.1C)
5. We want to generalize the idea that there's an I corresponding to $\operatorname{Spec} A \to \operatorname{Spec} B$. Because we need to glue affine sets, we want not an ideal but an **ideal sheaf**, defined to agree with the expected. Example, if $V = \operatorname{Spec} B$ we want to get out $I = \ker(B \to A) = \ker(\mathscr{O}_Y(V) \to \mathscr{O}_X(U)) = \ker \mathscr{O}_Y(U) \to \pi_* \mathscr{O}_Y(V)$. Define

   $$\mathscr{I}_{X/Y} := \ker \mathscr{O}_Y \to \pi_* \mathscr{O}_X.$$

   By definition,

   $$0 \to \mathscr{I}_{X/Y} \to \mathscr{O}_Y \to \pi_* \mathscr{O}_X \to 0.$$

   When do ideals in affine open sets define closed subscheme? 8.1F, 8.1G, 8.1H. Need to behave under localization. Review H II.3.11

Chapter 6

Probability

1 Probability

Resources:

1. Durrett, Probability
2. Scott Sheffield 18.175 `http://math.mit.edu/~sheffield/fall2012math175.html` and 18.177 `http://math.mit.edu/~sheffield/2011math177.html`
3. David Williams, Probability with martingales

Plan:

1. Review and index-card measure theory. (Spread this out because need to go forward with other stuff; take the big theorems for granted now.)
2. Understand PGF's and other basic tools.
3. Understand the central limit theorem.
4. Start on martingales, etc. (Do lots of problems.)

1.1 Measure theory review and basic probability

1.1.1 Measure theory

From measure theory:

1. Bounded convergence theorem (for finite measures)—convergence *in probability*. Idea: ε_1 for space where $> \varepsilon$, ε_2 for rest.
2. Fatou's lemma (idea: reduce to f_n increasing. Truncate. Take the inf inside decreases the expression, use BCT.)
3. Dominated convergence theorem (Fatou).

4. Monotone convergence theorem (Fatou for $g \pm f_n$).

5. Change of variables (prove for simple, nonnegative, integrable).

1. Types of convergence (in order of strongest to weakest):

   Definition 6.1.1: We say $X_n \to X$

   (a) **almost surely** if $P(X_n \to X) = 1$. For example, the proportion of heads goes to $\frac{1}{2}$.
   (b) **in probability** if $P(|X_n - X| > \varepsilon) \to 0$. For example, the probability of bulls-eye goes to 1 (if the probability after n steps is $1 - \frac{1}{n}$, from experience).
   (c) **in distribution** if $P(X_n \le t) \to P(X \le t)$.

   We have see old notebook

   (a) Almost sure implies in probability
   (b) L^2 convergence implies in probability (Markov)
   (c) In probability and continuity at t implies in distribution at t.

2. Product measure. Q1: Under what conditions can we define $\mu = \mu_1 \otimes \mu_2$? σ-finite is enough. Q2: when is $\int d\mu$ a double integral? When f is integrable. (It suffices to get the μ_2-integrable for μ_1-almost all x_1.)

Questions

1. Q: Given f is an increasing function, what is the distribution of $f(M)$ based on M?

   First Q: How do we think about a distribution? Several ways.

   (a) As a measure μ: $P(x \in I) = \int_I dP$.
   (b) As a function (if it's continuous!) $P(a \le x < b) = \int_a^b p(x)\,dx$; p is the distribution function.

   [Riemann-Steltjes?]

   Original Q: We want $\int_{f(a)}^{f(b)} dP_{f(M)} = \int_a^b dP$, so letting q, p be distribution functions,

   $$\int_{f(a)}^{f(b)} q(x)\,dx = \int_a^b p(x)\,dx.$$

   By change-of-variables, $p(x) = f'(x)q(x)$.

   Q: What are the precise conditions?

Sheffield's slides

1. Why can't σ-algebra be all subsets of Ω? It's inconsistent with translation invariance: take one point from each rational equivalence class. 3 ways to get around this:

(a) Remove the axiom of choice. (ex. use the axiom of determinacy)

(b) Replace countable additivity with finite additivity (Banach-Tarski).

(c) Don't define probability for all sets. (the usual approach. Price: we'll have to worry about what the σ-algebra might be!)

2. Classifying probability measures on $\mathbb{R}$.

   Theorem 6.1.2: thm:F-P The probability measures on $\mathbb{R}$ are in 1-1 correspondence with the right-continuous, non-decreasing functions F tending to 0 at $-\infty$ and 1 at ∞, by

$$P((a,b]) = F(b) - F(a).$$

   Extension to $\mathbb{R}^d$: take $F(x) = \mu((-\infty, x_1] \times \cdots \times (-\infty, x_n])$.

3. How do we define measures? Use extension theorems. For theorem above, are we confident we can extend the definition to all Borel measurable sets in a consistent way?

   Define **algebra** (collection of sets closed under finite unions/complementation), **semialgebra** (closed under intersection, and such that S^c is finite disjoint union, cf. a subbase)

   Theorem 6.1.3 (Caratheéodory extension theorem)**:** If μ is a σ-finite measure on an algebra $\mathcal{A}$ then μ has a unique extension to the σ-algebra generated by $\mathcal{A}$.

   (If S is a semialgebra, $\mu(\phi) = 0$, μ is finitely additive and countably subadditive, then μ has a unique extension on $\overline{S}$; if it is σ-finite, the above applies.

For random variables: If $X^{-1}(A) \in \mathcal{F}$ for all $A \in \mathcal{A}$ and $\mathcal{A}$ generates $\mathcal{S}$, then X is measurable.

Basic properties: Suppose r.v.'s converge to an event; it's also measurable.

Lebesgue: if you can measure, you can integrate. Verify linearity and positivity for:

1. finitely many values
2. bounded
3. nonnegative
4. measurable

Define expectation, as long as integrals of $\min(X,0), \max(X,0)$ aren't both infinite. *We can interpret our basic properties of integrals as properties of expectation.*

Counterexamples to bounded convergence theorem by fat rectangles, to Fatou by thin rectangles.

What does the strong law mean?

Problem 6.1.4:

1. Okay, but what does independent mean in this context?
2. And how do you even define an infinite sequence of independent random variables? Is that even possible? It's kind of an empty theorem if it turns out that the hypotheses are never satisfied.
3. And by the way, what measure space and σ-algebra are we using? And is the event that the limit exists even measurable in this σ-algebra? Because if it's not, what does it mean to say it has probability one?
4. Also, why do they call it the strong law? Is there also a weak law?

On independence:

1. Pairwise independence implies independence.
2. π-systems $\mathcal{A}_i$ independent implies $\sigma(\mathcal{A}_i)$ independent by π-λ theorem.
3. $(X_1, \ldots, X_n)$ has distribution $\mu_1 \times \cdots \times \mu_n$.
4. Expected values multiply (need $X_i \geq 0$ for all i or $\mathbb{E}|X_i| < \infty$).

Make sense of me! Let Ω be the set of all countable sequences $\omega = (\omega_1, \omega_2, \omega_3, \ldots)$ of real numbers. Let $\mathcal{F}$ be the smallest σ-algebra that makes the maps $\omega \to \omega_i$ measurable. Let P be the probability measure that makes the ω_i independent identically distributed normals with a certain distribution.

Let $\mathcal{F}$ be the natural product σ-algebra. (cf. topological products)

Theorem 6.1.5 (Kolmogorov extension)**:** If we have consistent probability measures on $(\mathbb{R}^n, \mathcal{R}^n)$, then we can extend them uniquely to a probability measure on $\mathcal{R}^{\mathbb{N}}$. (Proof: semi-algebra variant of Carathéeodory)

More generally true for $(S, \mathcal{S}) \to (\mathbb{R}, \mathcal{R})$ where there is a 1-1 map such that ϕ, ϕ^{-1} are measurable. If S is a (Borel subset of a) complete separable M, then $(S, \mathcal{S})$ is nice. (Proof: map to $[0,1]^{\mathbb{N}}$, then to $[0,1]$ via binary expansion.)

Fubini: Check definition makes sense: if f measurable, show that restriction of f to slice $\{f(x,y) : x = x_0\}$ is measurable as function of y, and the integral over slice is measurable as function of x_0. Check Fubini for indicators of rectangular sets, use π-λ to extend to measurable indicators. Extend to simple, bounded, L^1 (or non-negative) functions.

Summing 2 independent X, Y. Note $X + Y \leq a$ lives in $X \times Y$. Use Fubini to get

$$P(X + Y \leq a) = \int_{-\infty}^{\infty} F_X(a - y) f_Y(y)\, dy$$
$$f_{X+Y}(a) = \int_{-\infty}^{\infty} f_X(a - y) f_Y(y)\, dy.$$

Summing normal variables: $(\sum \mu, \sum \sigma^2)$.

Weaken "variances add" from independent to uncorrelated (because to find the variance of $\sum X_i$, we will only have products involving at most 2 X_i).

Todo: Index-card BCT to DCT stuff, other basics. Look at proof of Carathéeodory and Kolmogorov extension. Make sure you understand distributions on $\mathbb{R}$ (why can you differentiate?).

Moment generating function:

1. Idea: define pgf $\sum_n x^n P(X = n)$. Get nice things out like mean, variance...
2. Don't just think of it formally, note it's $\mathbb{E}(x^n)$! It's natural to set $x = e^t$, especially since this allows us to define a mgf when X is continuous.
3. $M'(t) = \mathbb{E}(Xe^{tX})$. When are you allowed to take a derivative inside an integral?

> 🔑 $M^{(n)}(0) = \mathbb{E}(X^n)$. *Knowing all the derivatives at a single point tells you the moments.*
> Another way to see: expand it out!
> Adding independent random variables corresponds to multiplying moment generating functions.
> Mgf's help us understand what happens when we sum up a lot of independent copies of the same rv.

Some transformations.

Z	$M_Z(t)$
aX	$M_X(at)$
$X + b$	$e^{tb}M_X(t)$
$X + Y$	$M_X(t)M_Y(t)$

> ! Mgf's are not defined for distributions with fat tails! $f_X(x)$ needs to decay superexponentially.

> 🔑 Inequalities allow us to deduce limited information about a distribution when we know only the mean (Markov) or the mean and variance (Chebyshev).
>
> - Markov: if $\mathbb{E}[X]$ is small, then it is not too likely that X is large.
> - Chebyshev: if $\sigma^2 = \text{Var}[X]$ is small, then it is not too likely that X is far from its mean.

1.2 Laws of large numbers and Central Limit

1.2.1 Laws of large numbers

Theorem 6.1.6 (Weak laws of large numbers)**:** (Classical weak law) Let X_i be iid (uncorrelated is enough) with mean μ, and such that $\mathbb{E}|X|$ is finite (i.e. X is L^1). For all

$\varepsilon > 0$,

$$A_n := \frac{\sum_{k=1}^n X_k}{n} \to \mu$$

in law, i.e.,

$$\lim_{n\to\infty} P(|A_n - \mu| > \varepsilon) = 0.$$

Theorem 6.1.7: (Weak law for triangular arrays) Suppose $X_{k,n}$ are random variables with the variables within each row independent.

$X_{1,1}$
$X_{2,1}$ $X_{2,2}$
$X_{3,1}$ $X_{3,2}$ $X_{3,3}$

Let b_n be such that $b_n \to \infty$ and let $\overline{X}_{n,k} = X_{n,k}1_{|X_{n,k}|\le b_n}$ (large thresholds). (See the explanation on truncation below.) Suppose

1. (RV's don't blow up) $\sum_{k=1}^n P(|X_{n,k}| > b_n) \to 0$.

2. (Thresholds much larger than variance) $\frac{1}{b_n^2}\sum_{k=1}^n \mathbb{E}\overline{X_{n,k}}^2 \to 0$ as $n \to \infty$. Then $\frac{S_n - a_n}{b_n} \to 0$ in probability.

Note: almost uncorrelated X_i sometimes enough. αn balls into n bins. Fraction of bins with no balls concentrates around expectation, $e^{-\alpha}$.

Proof. For finite variance: Use Chebyshev. Key point: σ multiplies only by $\sqrt{n}$ when there are n copies of X.

First approach:

> Use truncation $X = X1_{X>N} + X1_{X\le N}$. Choose N so that $\mathbb{E}A$ is small, use LoLN for B.

Second approach:

> Characteristic function $\phi(t) = \mathbb{E}(e^{itX}) = M(it)$. Well defined at all t.

Use Lévy's continuity theorem: $\lim_{n\to\infty}\phi_{X_n}(t) = \phi_X(t)$ implies $X_n \to \mu$ in law.

Reduce to mean 0 case. Now calculate:

$$\lim_{n\to\infty}\phi\left(\frac{t}{n}\right)^n = \left(\phi(0) + \frac{t}{n}\phi'\frac{t}{n} + o\left(\frac{t}{n}\right)\right)^n = e^{\phi'(0)} = 1.$$

using $\lim_{n\to\infty}\left(1+\frac{t}{n}\right)^n = e^t$, locally uniformly in t. □

Examples

1. Define the Bernstein polynomial $f_n(x) = \sum_{m=0}^n \binom{n}{m} x^m (1-x)^{n-m} f\left(\frac{m}{n}\right)$. Then $\lim_{n\to\infty}\sup_{x\in[0,1]}|f_n(x)-$ $f(x)| = 0$. Proof. Let X be Bernoulli(x). Then we need to show $\mathbb{E}(f(A_n)) \to \mathbb{E}(f(X))$ uniformly in x. Note that the weak law gives $A_n \to X$ in probability. Use continuity and boundedness of f.

2. A high-dimensional cube is almost the boundary of a ball. Note $\frac{X_1^2+\cdots+X_n^2}{n} \to \frac{1}{3}$ in probability.

Theorem 6.1.8 (Strong law of large numbers)**:** Let X_i be iid's with $\mathbb{E}X_i = \mu$ and $\mathbb{E}|X_i| < \infty$. Let $S_n = \sum_{i=1}^n X_i$ and $A_n = \frac{S_n}{n}$. Then $A_n \to \mu$ a.s. as $n \to \infty$.

Proof. Technique: Use Borel-Cantelli. We used Markov/Chebyshev to show weak LoLN since the statement of Markov/Chebyshev (a random variable is usually within epsilon) gives *in probability* convergence. Here we want *a.s.* convergence, and if we can rephrase what we want

$$(A_n \to \mu) \iff \text{NOT } (E_n \text{ infinitely often})$$

then we can reduce to showing $\sum P(E_n) < \infty$. We work out what the events E_n should be by the definition of convergence:

$$(A_n \to \mu) \Leftarrow \forall \varepsilon, \text{NOT } (A_n - \mu > \varepsilon \text{ infinitely often}).$$

Obstacle 1: To get any kind of bound we need control on variance. However, the variance may be infinite. Hence we use the standard

Technique: Truncation. It turns out $\overline{X}_k := X_k 1_{|X_k| \le k}$ works fine, $\overline{A}_k := \frac{1}{n}\sum_{k=1}^n \overline{X}_k$ works fine.

- Claim: If $\overline{A}_k \to \mu$ a.s., then $A_k \to \mu$ a.s.

  Proof: It suffices to show almost surely the truncation will affect only finitely many terms. To do this use Borel-Cantelli. An integral estimate gives

$$\sum_{i=1}^n P(|X_i| > k) \le \int_0^\infty P(|X_1| > t)\, dt = \mathbb{E}|X_i| < \infty \implies P(X_k \ne \overline{X}_k \text{ i.o.}) = 0.$$

Obstacle 2: $\sum_n P(A_n - \mu > \varepsilon)$ will diverge. (For example, in the L^2 case this will be $\sum_n O\left(\frac{1}{\sqrt{n}}\right)$, no good.)

Idea: We only need to control a subsequence of the A_n.

> Using Borel-Cantelli: Control a finite subsequence and use monotonicity to show that the rest of the events will (approximately) hold.

What is the sparsest sequence that it suffices can control? Something geometric, provided that we can choose the ratio arbitrarily close to 1. (Geometric, as it turns out, will be excellent for making our sum converge.)

Reduction: We can assume $X_n \ge 0$; otherwise decompose $X_n = X_n^+ - X_n^-$.

Carrying out the plan: We calculate by Chebyshev and exchanging order of summation

$$\sum_{n=1}^{\infty} P(|\overline{A}_{k(n)} - \mathbb{E}\overline{A}_{k(n)}| \le \varepsilon) \le \varepsilon^{-2} \sum_{m=1}^{\infty} \mathrm{Var}(\overline{X}_m) \sum_{n:k(n) \ge m} k(n)^{-2} < \infty$$

when we take $k(n) = \lfloor \alpha^n \rfloor$, by the lemma:

Lemma 6.1.9: $\sum_{k=1}^{\infty} \frac{\text{var}(Y_k)}{k^2} \leq 4\mathbb{E}(|X_1|)$.

Proof: Use the $P(>)$ way of expressing moments, and exchange order of summation. Now bound A_m for $k(n) < m < k(n+1)$, and take $\alpha \to 1$. □

Proof 2. Get a condition for $\sum X_n$ to converge: if X_i are independent and $\mathbb{E}X_n = 0$ and $\sum \text{var}(X_n) < \infty$ then $\sum X_n$ converges a.s.

Apply to $Z_k = Y_k - \mathbb{E}Y_k$ and use partial summation. □

Rates of convergence. Note that wLoLN gives the expected value at most $O\left(\frac{1}{\sqrt{n}}\right)$, but here we want a.s. The random series proof gives convergence rates because if $\sum X_n = 0$ we can replace X_n by $\frac{X_n}{a_n}$, ans see how slow growing we can make the a_n so that $\sum_{n=1}^{\infty} \text{var}(X_n) < \infty$ still holds.

1. If $\mathbb{E}X_1^2 < \infty$, then we can take $a_n = n^{\frac{1}{2}}(\ln n)^{\frac{1}{2}+\varepsilon}$.
2. If given $1 < p < 2$, $\mathbb{E}|X_1|^p < \infty$, we can take $a_n = n^{\frac{1}{p}}$ (cf. when $p = 1$). (Use $k^{\frac{1}{p}}$ as the truncation threshold. Note in addition we need to estimate the truncated μ_m; we do that by bounding L^1 with L^p.

Kolmogorov 3-series theorem

Theorem 6.1.10: Fix $A > 0$ (a threshold). Then $\sum X_i$ converges iff

1. (X not too large)
2. (Sum of expected value of truncated converges)
3. (Sum of variance of truncated converges)

Proof. Kolmogorov zero-one law implies that $\sum X_i$ converges with probability $p \in \{0, 1\}$. We just have to show that $p = 1$ when all hypotheses are satisfied (sufficiency of conditions) and $p = 0$ if any one of them fails (necessity). To prove sufficiency, apply Borel-Cantelli to see that probability that $X_n = Y_n$ i.o. is zero. Subtract means from Y_n, reduce to case that each Y_n has mean zero. Apply Kolmogorov maximal inequality. □

1.2.2 Large deviations

We've looked at what's the minimum a_n to make $\frac{1}{a_n}S_n \to 0$ a.s. But now we consider large deviations and we want to know how fast $P(S_n \geq d(n)) \to 0$ for some large $d(n)$. "Kind of a quantitative form of the weak law of large numbers. The empirical average A_n is very unlikely to be ε away from its expected value (where "very" means with probability less than some exponentially decaying function of n)."

$\gamma(a) = \lim_{n\to\infty} \frac{1}{n} \ln P(S_n \geq na)$.

(cf. how in generating functions, we ask what is r so that $a_n \sim r^n$?)

Exercises from Durrett.

2.1.6 (Abstract away what we need for re-metrization): $\int_0^a \leq \int_b^c$.

2.2.2 (It's enough for the X_n to be uncorrelated enough; "examine the proof to weaken conditions")

2.2.7 (Calculating the expected value of $H(X)$ given h) Fubini.

2.3.9 ?

2.3.12 We have $P(\bigcup^n A_k) \to 1$. LHS says $\prod P(A_n^c) \to 0$. Now $\prod(1 - x_n) \to 0$ implies $\sum x_n < \infty$. Use Borel-Cantelli.

2.3.19

1.2.3 Central limit theorem

Tools.

1. Use what we know about convergence of rv's to get convergence of distributions.

   Theorem 6.1.11 (Skorohod's Theorem)**:** (Going from convergence of distributions to convergence of random variables) If $F_n \to F_1$, then we can find corresponding random variables Y_n on a common measure space so that $Y_n \to Y_1$ almost surely.

   Proof. We establish a correspondence between distributions on $\mathbb{R}$ and random variables on the common measure space $(0, 1)$. It is given by

   $$Y_n(x) = \sup \{y : F_n(y) < x\} .$$

   □

   See picture.

   Corollary 6.1.12: When proving things given $X_n \implies X_\infty$, we may assume the X_n are on a common measure space and $X_n \to X_\infty$ a.s. Thus for instance $g(X_n) \to g(X_\infty)$ a.s.

2. **Theorem 6.1.13:** (Testing convergence in distribution using functions) $X_n \implies X_\infty$ if and only if for every bounded continuous g we have $\mathbb{E}g(X_n) \to \mathbb{E}g(X_\infty)$.

   Proof. Forward direction is by corollary and BCT.

   Backwards direction is approximating $1_{(\infty,x]}$ by continuous functions. □

   Generalization of idea of corollary: ok as long as $P(X_\infty \in D_g) = 0$. (D_g is discontinuities.) Then $g(X_n) \implies g(X_\infty)$. If g is bounded, $\mathbb{E}g(X_n) \to \mathbb{E}g(X_\infty)$.

   Proof. Use the previous criterion. □

2.4 equivalent criteria for $X_n \implies X_\infty$. (cf. shrinking opens and expanding closeds). (Remember by taking convergent sequence.)

3.

Theorem 6.1.14 (Helly selection)**:** Given a sequence F_n of distribution functions, there is a subsequence $F_{n(k)}$ and righ continuous nondecreasing F so that $F_{n(k)}(y) \to F(y)$ at all continuity points.

WARNING: may not be distribution function becuase mass may escape to ±∞. Need a tightness assumption to make that the case. Say μ_n are **tight** if for every ε we can find an M so that $\mu_n[-M, M] < \varepsilon$ for all n (uniformly). corresponding real random variables or distributions functions.

Every subsequential limit of the F_n above is the distribution function of a probability measure if and only if the F_n are tight.

cf. Arzela-Ascoli: Given a sequence of real-valued continuous functions $(f_n)_{n\in\mathbb{N}}$ defined on $[a, b]$. If this sequence is uniformly bounded and equicontinuous, then there exists a subsequence (f_{n_k}) that converges uniformly.

Proof. cf. Arzela-Ascoli: enumerate (by rationals, say). Diagonlize. Note that if $F_{n(k)}(q) \to G(q)$ for rational q, G may not be right continuous, need to define $F(x) = \inf\{G(q) : q > x\}$.

For tightness, simply consider $F(x) - F(-x)$ for x large. □

Criterion for tightness: if there is $\varphi \geq 0$ so that $\varphi(x) \to \infty$ as $|x| \to \infty$ and $\sup_n \int \varphi(x)\, dF_n(x) < \infty$, then tight.

4. Total variation distance $\|\mu - \nu\| := \sup_B \|\mu(B) - \nu(B)\|$. Intuitively, it two measures are close in the total variation sense, then (most of the time) a sample from one measure looks like a sample from the other. Corresponds to L^1 distance between density functions when these exist.

   Much stronger than weak convergence (ex. consider discrete approximation to continuous).

   What does weak convergence have to do with def'n in functional analysis?

   Consider space of measures. What does it mean for $\mu_n \to \mu$ in $C(K)^*$ in w^* sense? (implicitly use Riesz representation) $\int f\, d\mu_n \to \int f\, d\mu$ for all $f \in C(K)$.

5. Characteristic function. Note

   (a) uniformly continuous.

   (b) periodic if X takes integer values.

   (c) real when X symmetric around 0.

For moments we need to worry about differentiation under the integral sign! When can we do so?

$$\frac{d}{dt}\int_a^b f(x,t)\,dx = \int_a^b f_t(x,t)\,dx.$$

Regardless, we need $\int_a^b |f|\,dx < \infty$ (1-L^1 condition) and f_t to exist and be continuous in t (2-C^1 condition). Two ways to think about this:

1. Dominated convergence. What we need is that

   $$\left|\frac{f(x,t+h)-f(x,t)}{h} - f_t(x,t)\right| < g(x)$$

   uniformly in h (for h small enough) and

   $$\int |g(x)|\,dx < \infty.$$

   (So really everything is fine if it's $[a,b]\times[c,d]$ by uniform continuity.)

2. Fubini. Note that since we're differentiation in t, we need to know something about the function for $t+\varepsilon$ (consider for instance $f = t^2(x^2+1)$). $f_t(x,0) = 0$ but $\frac{f(x+h,t)-f(x,t)}{h} - f_x(x,t) = h(x^2+1)$, whose integral over x is ∞.

   We need (3-continuity condition at $x = y$) $\int_a^b f_t(x,t)\,dx$ and (4-L^1 for product space) $\int_a^b \int_{t-\varepsilon,t+\varepsilon} |f_t(x,s)|\,dy\,ds$.

We actually generalize to x being in a measure space.

We get the moment result: if $\int |x|^n\,\mu(dx) < \infty$ then $\varphi^{(n)}(t) = \int (ix)^n e^{itx}\,\mu(dx)$. For example, for $n = 1$ and (4) we just need to check for each x_0, $\int_{-\infty}^{\infty}\int_a^b |f'|\,\mu(dx)\,dt < \infty$ for some interval $[a,b] \ni x_0$, which is clear from the condition. (The others are easier.)

We can replace (3) and (4) by

$$\int_S \left|\sup_{s\in[t-\delta,t+\delta]} f_t(x,s)\right| \mu(dx) < \infty.$$

You can show (3) and (4) from this, though I think it's more clear from the DCT POV. (write the difference as an integral. We could weaken this by writing sup − inf, but we won't really need it.)

Recall Fourier inversion:

$$f(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \widehat{f}(t)e^{-itx}\,dt.$$

When exactly is this true?

Theorem 6.1.15 (Characteristic function inversion)**:**

$$\lim_{T\to\infty}\frac{1}{2\pi}\int_{-T}^{T}\frac{e^{-ita}-e^{-itb}}{it}\phi(t)\,dt = \mu(a,b) + \frac{1}{2}\mu(\{a,b\}).$$

Proof. look me up □

Given any function ϕ and any points $x_1, \ldots, x_n$, we can consider the matrix with i, j entry given by $\phi(x_i - x_j)$. Call ϕ positive definite if this matrix is always positive semidefinite Hermitian.

Theorem 6.1.16 (Bochner)**:** A continuous function $\mathbb{R} \to \mathbb{R}$ with $\phi(1) = 1$ is a characteristic function of some probability measure on $\mathbb{R}$ iff it is positive definite.

Why called characteristic function?

Theorem 6.1.17 (Central limit theorem)**:** If X_i are iid with $\mathbb{E}X_i = \mu$, $\mathrm{Var}(X_i) = \sigma^2 \in (0, \infty)$, and $S_n = \sum_{k=1}^n X_k$, then

$$\frac{S_n - n\mu}{\sigma n^{\frac{1}{2}}}$$

in distribution.

Proof. WLOG $\mu = 0$.

$$\mathbb{E}e^{\frac{itS_n}{\sigma n^{1/2}}} = \left(1 - \frac{t^2}{2n} + o(n^{-1})\right)^n = e^{-\frac{t^2}{2}}.$$

□

Theorem 6.1.18 (Lindeberg-Feller)**:** Suppose $X_{n,m}$ is a triangular array, $\sum_{m=1}^n \mathbb{E}X_{n,m}^2 \to \sigma^2 > 0$, $\lim_{n\to\infty} \mathbb{E}(|X_{n,m}|^2 : |X_{n,m}| > \varepsilon) = 0$. Then $S_n \implies N(0, 1)$.

Proof. Use characteristic functions $\phi_{n,m} = \phi_{X_{n,m}}$. Try to get some uniform handle on how close they are to their quadratic approximations. □

If a third moment exists, convergence is very fast.

Theorem 6.1.19 (Berry-Esseen)**:**

Proof. You can convolve with something that has a characteristic function with compact support. Play around with Fubini, error estimates. □

3.3.16 Tight $\iff$ equicontinuous

3.3.17 (i) Solution 1: write out the taylor expansion $f_n = \varphi\left(\frac{x}{n}\right)^n = (1 + \varphi'(0)\frac{x}{n} + o(x))^n$. Now $f_n' \to f'$ by noting that the derivative converges uniformly (do some work here). Solution 2: use the trick $x^n \sim e^{(x-1)n}$ when $x \to 1$. (ii) Solution 1: Convergence in probability gives convergence in distribution; by the continuity theorem $\varphi\left(\frac{t}{n}\right)^n \to e^{iat}$, point mass. Solution 2: Similar to solution 2 above, use $\ln z \sim z - 1$ at $z = 1$.

See `http://www.math.uconn.edu/~kconrad/blurbs/analysis/diffunderint.pdf`

1.3 Martingales

1.3.1 Conditional expectation

1. Defining $\mathbb{E}(X|\mathcal{G})$: (distinguish from $\mathbb{E}(X)$) We want to average with respect to $\mathcal{G}$.
   (a) First idea: $\mathbb{E}(X|G)(x) = \mathbb{E}_{x\in A}(X) = \mathbb{E}(X1_A)/\mathbb{P}(A)$ when $x \in A$, A is an atom of Y. Problem: Atoms may not exist.
   (b) Second idea: In terms of the properties we want it to satisfy. Let $Y = \mathbb{E}(X|G)$ be the unique rv such that
      i. Y is G-measurable.
      ii. $\mathbb{E}(Y) = \mathbb{E}(X)$. We want something stronger. $\mathbb{E}(Y1_A) = \mathbb{E}(X1_A)$ for all $A \in G$, or equivalently, for all *bounded* $\mathcal{G}$-measurable Z, $\mathbb{E}(XZ) = \mathbb{E}(YZ)$.
2. (1.9) Uniqueness: easy. Existence:

   > To show a function on functions is well-defined, define it for
   >
   > (a) A subset of positive, bounded functions (rv's), such as L^2.
   >
   > (b) Consider $\min(X, n) = X \vee n$ and use MCT to define for positive rv's.
   >
   > (c) Consider $X = X^+ - X^-$ to define for all rv's.

   Here we show for L^2 by using the fact we have projections in a Hilbert space. Project to the G-measurable functions.
3. Basic properties
   (a) 1.14
   (b) 1.18 Conditional MCT, Fatou, DCT, Jensen (note for Jensen we need $\varphi(X)$ to be integrable or φ nonnegative). In particular, taking $\mathbb{E}(\bullet|G)$ can only decrease L^p norm. *Pf.* Idea: approximate below by linear functions.
   (c) 1.19 Tower property.
   (d) 1.20 Taking out what is known. Strategy is variation of that above:

   > Prove for simple functions, and then extend to $X \geq 0$ by MCT, and then use $X^+ - X^-$.

4. 1.24 !
5. Examples.

Pset 1 `http://www.statslab.cam.ac.uk/~ps422/ex-sheet-1.pdf` `http://www.statslab.cam.ac.uk/~ps422/Solution_1_Vittoria.pdf`

1. General idea: "a measure is determined by its integrals." First, since $\mathbb{E}$'s are well-defined, $\sigma(X) = \sigma(Y)$. We hence have $\mathbb{E}(YZ) = \mathbb{E}(XZ)$ for all measurable Z, so $X = Y$ a.s.

   Concretely, we can take Z as in the hint.

2. 0 on $\{X = 0, Y = 0\}$ and $\frac{2pq+2p^2}{2pq+p^2} = \frac{1}{2-p}$ on the rest, so $\frac{1}{2-p}1_Z$.

3. We see a concrete example of how to compute an expectation with respect to another variable. There's no explicit formula, so to check we see (1) it's measurable, and (2) check $\mathbb{E}(f(X)1_A) = \mathbb{E}(h(X)1_A)$. Indeed

$$\int\int \frac{1}{2}\int_0^Z h(u)\,du\theta e^{-\theta x}\,dx\,\theta e^{-\theta y}\,dy = \int\int_{A'} \theta e^{-\theta(x+y=z)}\,d(x{+}y = z)\,d(\frac{y-x}{2}) = \frac{1}{Z}\int_0^Z h(u)\,du.$$

4. Idea: we have to just leave the parts when $Y = 0$ and use $X \neq 0$ there. Careful: include $Y \le 0$ as well. $\mathbb{E}(Y1_{Y\le 0}) = \mathbb{E}(X1_{Y\le 0}) \ge 0$, so $= 0$, $\mu(Y = 0) = 0$.

   Write down in math terms: $\{x > 0\} \subseteq A \subseteq B := \{\mathbb{E}(X|\mathcal{G})\}$ with A $\mathcal{G}$-measurable. then using (a) for 1st part,

$$\mathbb{E}(\mathbb{E}(X|\mathcal{G})1_B) \ge \mathbb{E}(\mathbb{E}(X|\mathcal{G})1_A) = \mathbb{E}(X1_A) = \mathbb{E}(X1_B)$$

   so equality holds.

Williams, Ch. 0

1. The children problem.

   Suppose the distribution of children is given by the pgf

$$f(\theta) = \sum_k P(Z = k)\theta^k$$

   where Z is the number of children. Note this equals $\mathbb{E}(\theta^Z)$—it's not just a formal series, but actually an expected value!

   (a) Then the number of children at time $n + 1$ is

$$f_{n+1}(\theta) = \sum_\ell \sum_k \theta^k \underbrace{P(Z_n = \ell)}_{[\theta]^\ell f_n} \underbrace{P(Z_{n+1} = k|Z_n = \ell)}_{[\theta^k]f^\ell} = f_n(f).$$

   (b) A theorem (makes sense!) Extinction probability is unique root of $\pi = f(\pi)$ in $(0, 1)$.

   (c) Note we get a martingale with $M_n = \frac{Z_n}{\mu^n}$, but the exponential blowup means we have to be careful with convergence. We can have $0 = \mathbb{E}(M_\infty) \neq \lim \mathbb{E}(M_n) = \mathbb{E}(M_0) = 1$. Fatou's lemma: the expected value might stay constant but the expected value at the limit may be smaller.

(d) One solution: compose with a function that makes it bounded.

$$\mathbb{E}e^{-\lambda M_\infty} = \lim \mathbb{E}e^{-\lambda M_n}.$$

The RHS is $\lim \mathbb{E}[e^{-\lambda/\mu^n \cdot Z_n}] = f_n(e^{-\lambda/\mu^n})$.

(e) Functional equation: $L(\lambda\mu) = f(L(\lambda))$ from

$$f(L(\lambda)) = f(\lim_{n\to\infty} f_n(e^{-\lambda/\mu^n}) = \lim_{n\to\infty} f_{n+1}(e^{-\lambda/\mu^n}) = L(\lambda\mu).$$

(f) In the geometric case we can easily compute. How do we compute the distribution of M from $e^{-\lambda M}$?

2. Generalities

   (a) Why we care about measure theory: Williams p. 4-6; a bad attempt at defining probability space.

   (b) Why we have to be careful about M_∞. The Fatou factor: how the balance is achieved by big values times small probabilities.

   (c) Q: How is the behavior of Z conditional on M_∞?

(11/18)

1.4 Problems

Problems 2

1.

2.

3. This is a nice application of martingales. On the surface the idea of martingales is a very concrete statement about "you can't beat the system if the game is fair." However, looking beyond the literal, martingales are a lot more powerful because you can *create invariants (in terms of expectations)* and conclude things form those "invariants" being martingales.

   Two steps to solving this question.

   (a) What stays constant in expectation? The expectation of total money increases by $1 each time step. Thus $M_n - n$ is a martingale,

   $$\mathbb{E}[M_n - n] = E[M_0 - 0] = 0 \text{ for all } n.$$

   (b) Put in the stopping time. Stop when the monkey produces ABRACADABRA. At this time the total money in the game is $\$26^{11} + 26^4 + 26$, from the gamblers who have just seen ABRACADABRA, ABRA, and A. Thus $E[M_T] = 26^{11} + 26^4 + 26$ (this is true all the time). We get by the Optional stopping theorem

   $$E[M_T - T] = 0 \implies E[T] = 26^{11} + 26^4 + 26.$$

(c) Actually we need to be careful: we have to make sure we can apply the theorem. Things can be funny when we go on infinitely long.

We only get $\mathbb{E}[M_{T\wedge t}] = \mathbb{E}[X_0]$ from Optional Stopping. But note $|\mathbb{E}[M_{T\wedge t}]| \leq 26^{11} + 26^4 + 26$ is finite, and $E[T]$ is bounded by $\sum_{n=1}^{\infty} 11n\left(1 - \left(\frac{1}{26}\right)\right)^{11(n-1)}\left(\frac{1}{26}\right)^{11}$. Hence $\mathbb{E}[(M_T - M_{T\wedge t}) - (T - T\wedge t)] \to 0$ as $t \to \infty$.

4. This is an exercise in knowing how to apply basic properties of martingales and conditional expectation.

1.5 Talks

“Randomness and Continuum”

Speaker: Prof Wendelin Werner (ETH Zurich) When: 7-8pm, Monday 3rd February Where: MR2, CMS One can have a rather intuitive perception of the fact that space and time can be continuous, which is very directly related to the mathematical notion of continuity of functions. On the other hand, when one thinks of random phenomena, the natural examples that first come to mind are of discrete nature, such as coin tossing. The conceptual question on how ”randomness” can be split up into and reassembled from infinitesimal little pieces turns out to be quite tricky. It is related to contemporary research in mathematics that we shall illustrate via some concrete examples.

At the beginning of the 20th century, several problems puzzled mathematicians, physicists and philosophers, for instance, unprovability. Parallel to that, measure theory developed.

One can have a rather intuitive perception of the fact that space and time can be continuous.

Our intuition is ready to accept that space and time can be viewed as continuum. They can be subdivided into small events that then fit together again, and come naturally equipped with the idea of additivity.

However, our intuition about random phenomenon are more related to discrete events: coin tossing, etc.

Problem 6.1.20: Is it possible to spread randomness continuously into infinitesimal pieces into space or time? If so, how, and what do we learn from this?

Answers: Yes.

1. White noise: a sequence of coin tosses. We approximate the continuum by discretization.

   Question: which color has the majority?

   - This is a linear question: one adds the outcomes.
   - We are interested in the limit when the number of coin tosses tends to ∞. Is there a continuous limiting structure?

   For a random walk: after N steps, the typical order of magnitude of the walker is $\sqrt{N}$ (because $\mathbb{E}|X|^2 = N$).

This system is fairly stable: (1) the outcome of one coin toss has virtually no influence on the outcome of who wins. (2) misreading a small proportion of the bits has typically no big influence of the outcome. (3) If we see the outcome of the f

2.

3.

2 Percolation

2.1 Examples 1

1. Suppose $\frac{x_m}{m} = k$. Then for any $1 \le r < m$,

$$\begin{aligned} x_{km+r} &\le kx_m + x_r \\ \implies \frac{x_{km+r}}{km+r} &\le \frac{x_m}{m} + \frac{x_r}{km+r} \\ \implies \frac{x_n}{n} &\le \frac{x_m}{m} + \underbrace{\frac{1}{n}\max_{1\le r<m} x_r}_{\to 0 \text{ as } n\to\infty}. \end{aligned}$$

   Hence $\limsup_{n\to\infty} \frac{x_n}{n} \le k$.

   Given $\liminf_{n\to\infty} \frac{x_n}{n} = l$, we can find $\frac{x_m}{m}$ arbitrarily close to l (or arbitrarily negative, if $l = \infty$). This gives $\limsup_{n\to\infty} \frac{x_n}{n} \le l = \liminf_{n\to\infty} \frac{x_n}{n}$, so $\lim_{n\to\infty} \frac{x_n}{n} = k = l$.

2. ?

3. (3.4, covering graphs) Define the dual graph G' of G to be the graph whose vertices correspond to the edges e of G, and where there is an edge between e, f iff e, f are adjacent to the same vertex in G.

   A cluster of vertices in G' then corresponds to a connected cluster of edges in G.

4. (3.7) By the union bound,

$$\mathbb{P}_p(L_n > u) = \mathbb{P}_p(\bigvee_{k=1}^{n} \{r(k) \ge u\}) \le np^u.$$

   Hence

$$\begin{aligned} \mathbb{P}_p\left(L_n > \frac{(1+\varepsilon)\ln n}{\ln\left(\frac{1}{p}\right)} \right) &\le np^{(1+\varepsilon)\log_p \frac{1}{n}} \\ &= n \cdot \frac{1}{n^{1+\varepsilon}} = n^{\varepsilon} \to 0 \text{ as } n \to \infty. \end{aligned}$$

5. Given $\omega \in \{0,1\}^E$ not having an infinite path starting from the origin (in the standard percolation model), we construct $f(\omega)$ that does not have an infinite oriented path starting at the origin.

   Define $f(\omega)$ as follows. Let S be the set of open edges in ω connected to the origin. Choose a spanning tree for the graph determined by S. Now orient the edges outwards with respect to the origin. For every edge with exactly 1 endpoint in S, orient it towards the endpoint in S, so that it does not allow further percolation. For the rest of the edges, have it point right/up if it was originally open, and left/down if it was originally closed.

   Note f is injective on ω that do not have an infinite path starting from the origin, so

   $\mathbb{P}(\omega$ does not have an infinite oriented path$) \ge \mathbb{P}(\omega$ does not have an infinite oriented path$)$

   thus

   $\eta\left(\frac{1}{2}\right) = \mathbb{P}(\omega$ has an infinite oriented path$) \le \mathbb{P}(\omega$ has an infinite oriented path$) = \theta\left(\frac{1}{2}\right) = 0.$

6. ?

7. (4.2) For a set $A' \subseteq \{0,1\}^{n-1}$ and $i = 0$ or 1, write $A'i = \{(\omega(1), \ldots, \omega(n-1), i) : \omega \in A'\}$. Because A is increasing, we can write

$$A = A_1 0 \cup A_1 1 \cup A_2 1$$

for some disjoint $A_1, A_2 \subseteq \{0,1\}^{n-1}$.

For the base case $n = 1$, note we actually have $A \subseteq B$ or $B \subseteq A$; WLOG $A \subseteq B$ and the inequality reduces to $\mathbb{P}_p(A) \ge \mathbb{P}_p(A)\mathbb{P}_p(B)$.

For the induction step, let $\mathbb{P}_p(A_i) = a_i$ and $\mathbb{P}_p(B_i) = b_i$ (probability with respect to $\{0,1\}^{n-1}$. Then

$$\begin{aligned}
\mathbb{P}_p(A \cap B) &= (1-p)\mathbb{P}_p(A_1 \cap B_1) + p\mathbb{P}_p((A_1 \cup A_2) \cap (B_1 \cap B_2) \\
&\ge (1-p)a_1 b_1 + p(a_1 + a_2)(b_1 + b_2) && \text{induction hypothesis} \\
&= a_1 b_1 + p(a_1 b_2 + a_2 b_1 + a_2 b_2) \\
\mathbb{P}_p(A)\mathbb{P}_p(B) &= ((1-p)a_1 + p(a_1 + a_2))((1-p)b_1 + p(b_1 + b_2)) \\
&= (a_1 + pa_2)(b_1 + pb_2)
\end{aligned}$$

Thus

$$\mathbb{P}_p(A \cap B) \ge \mathbb{P}_p(A)\mathbb{P}_p(B).$$

(4.3)

8. (4.5, Equivalence of FKG condition and monotonicity)

   (a) Write $d(\omega_1, \omega_2)$ for the number of places where ω_1, ω_2 differ. Note the inequality is trivial if $\omega_1 \le \omega_2$ or $\omega_2 \ge \omega_1$. (Equality holds.)

   Suppose the inequality holds for all pairs ω_1, ω_2 that differ on at most 2 elements. We show by induction that if ω_1, ω_2 differ on at most n elements, the inequality holds. If ω_1, ω_2 are comparable, we are done. Else, since $n \ge 3$, without loss of generality there exist e, f such that

   $$\begin{aligned}
   \omega_1(e) &= 0 & \omega_2(e) &= 1 \\
   \omega_1(f) &= 1 & \omega_2(f) &= 0
   \end{aligned}$$

   In other words, $\omega_1 = (\omega_1)_e^f$ and $\omega_2 = (\omega_2)_f^e$. We will apply the inequality to (ω_1^e, ω_2) and $(\omega_1, (\omega_1 \wedge \omega_2)^e)$. This is valid since

   i. $\omega_1^e(e) = 1 = \omega_2(e)$, so $d(\omega_1^e, \omega_2) = d(\omega_1, \omega_2) - 1$

   ii. $\omega_1(f) = (\omega_1 \wedge \omega_2)^e(f) = 1$, so $d(\omega_1^e, \omega_2) < d(\omega_1, \omega_2) - 1$.

   We get

   $$\mu(\omega_1^e \vee \omega_2)\mu(\underbrace{\omega_1^e \wedge \omega_2}_{(\omega_1 \wedge \omega_2)^e}) \ge \mu(\omega_1^e)\mu(\omega_2)$$

   $$\mu(\underbrace{\omega_1 \vee (\omega_1 \wedge \omega_2)^e}_{\omega_1^e})\mu(\underbrace{\omega_1 \wedge (\omega_1)_f^e}_{\omega_1 \wedge \omega_2}) \ge \mu(\omega_1)\mu((\omega_1)_f^e).$$

   Multiplying and cancelling (since μ is positive) gives the result.

(b) We can rewrite the condition as: $\frac{\mu(\omega^e)}{\mu(\omega^e)+\mu(\omega_e)}$ is nondecreasing in ω. Note that for monotonicity to hold, it suffices that this inequality holds for ω_1, ω_2 differing in 1 place, because we can chain the inequalities together.

By (a), it suffices to show that monotonicity is equivalent to the FKG lattice condition for pairs that differ by 2 elements. We may assume the pairs are non-comparable, so $\omega_2 = (\omega_1)^e_f$ for some e, f. μ is monotone iff for all $e \neq f$ we have (applying monotonicity to $\omega_1^f > (\omega_1)_f$) gives

$$\begin{aligned}
\frac{\mu(\omega^{fe})}{\mu(\omega^{fe})+\mu(\omega^f_e)} &\geq \frac{\mu(\omega^e_f)}{\mu(\omega^e_f)+\mu(\omega_{ef})} \\
\iff \mu(\omega_1^{ef})\mu((\omega_1)_{ef}) &\geq \mu((\omega_1)^f_e)\mu((\omega_1)^e_f) \\
\iff \mu(\omega_1 \vee \omega_2)\mu(\omega_1 \wedge \omega_2) &\geq \mu(\omega_1)\mu(\omega_2).
\end{aligned}$$

9. Let $|E| = n$.

$$\begin{aligned}
\frac{d}{dp}\mathbb{E}_p(X) &= \frac{d}{dp}\sum_{\omega\in\{0,1\}^n} p^{|\omega|}(1-p)^{n-|\omega|}X(\omega) \\
&= \sum_{\omega\in\{0,1\}^n}\left(\frac{|\omega|}{p} - \frac{n-|\omega|}{1-p}\right)X(\omega) \\
&= \mathbb{E}_p\left[\sum_{e_i,\omega(e_i)=1}(\mathbb{P}(\omega^{e_i})-\mathbb{P}(\omega_{e_i}))X(\omega) - \sum_{e_i,\omega(e_i)=0}(\mathbb{P}(\omega_{e_i})-\mathbb{P}(\omega^{e_i}))X(\omega)\right] \\
&= \mathbb{E}_p\left[\sum_{e,\omega'(e)=1}\mathbb{P}(\omega)X(\omega) - \sum_{e,\omega'(e)=0}\mathbb{P}(\omega)X(\omega^e) - \sum_{e,\omega'(e)=0}\mathbb{P}(\omega)X(\omega)\sum_{e,\omega'(e)=1}\mathbb{P}(\omega)X(\omega_e)\right] \\
&= \mathbb{E}_p\sum_{e\in E}\mathbb{P}(\omega)[X(\omega^e)-X(\omega_e)] \qquad =
\end{aligned}$$

where in the third to last line we replace each $\omega^{e_i}, \omega_{e_i}$ by ω and change the sum accordingly.

Note $1_A(\omega^e) - 1_A(\omega_e) = (e \text{ is pivotal for } \omega)$.[1] By the above,

$$\mathbb{P}_p(A) = \sum_{e\in E}\mathbb{E}_p(\delta_e 1_A) = \mathbb{E}_p\sum_{e\in E}(e \text{ is pivotal for } \omega).$$

Iterating the formula for $\delta_e X$ gives

$$\frac{d^n}{dp^n}\mathbb{P}_p(X) = \sum_{e_1,\ldots,e_n\in E}\mathbb{E}_p(\delta_{e_1}\cdots\delta_{e_n}X).$$

We can check that for $n=2$, $\delta_{e_1}\delta_{e_2}1_A(\omega)$ is 1 only if exactly 3 of $\kappa_{e_1}\omega, \kappa_{e_2}\omega, \kappa_{e_1}\kappa_{e_2}\omega, \omega$ are the same; think of this as saying ω is sensitive to both the e_1, e_2 bits (jointly).

[1] Here we use the notation $(P) = \begin{cases}1, & P \text{ true}\\ 0, & P \text{ false}\end{cases}$.

Chapter 7

Statistics

1 Statistics of networks

From "detecting community structures."

In practice, most approaches to graph partitioning have been based on iterative bisection: we find the best division we can of the complete graph into two groups, and then further subdivide those two until we have the required number of groups. Among the many algorithms suggested for the problem, two have dominated the literature:

1. the spectral bisection method [15,16], which is based on the eigenvectors of the graph Laplacian, and

2. the KernighanLin algorithm [17], which improves on an initial division of the network by optimization of the number of within- and between-community edges using a greedy algorithm.

The KernighanLin algorithm is a greedy optimization method that assigns a benefit function Q to divisions of the network and then attempts to optimize that benefit over possible divisions.

The principal technique in current use is hierarchical clustering

The most common method, called the single linkage method, is to declare the components formed as the edges are added to be the communities.

complete linkage method. In this method edges are once again added to an initially empty graph in order of decreasing similarity, but now the communities are defined as being the maximal cliques in the network rather than the components

Of the two methods described, the complete linkage method has perhaps the more desirable properties, but it is rarely used,

Sociological studies have tended to concentrate on the property known as structural equivalence. Two vertices are said to be structurally equivalent if they have the same set of neighbours (other than each other, if they are connected). Thus two individuals in a friendship network are structurally equivalent if they have the same friends.

A similarity measure not based on structural equivalence is the count of edge- (or vertex-) independent paths between vertices.

This is typical of the hierarchical clustering method: it tends to be good at finding parts of communitiesthose parts corresponding to individuals with high similarity according to whatever similarity measure is chosenbut usually leaves some others unassigned to any major group.

Newman: The basic requirements for a general community finding algorithm are that it should find natural divisions among the vertices without requiring the investigator to specify how many communities there should be, or placing restrictions on their sizes, and without showing the pathologies evident in the hierarchical clustering method of Section 2.2.

(1) it is a divisive method, in which edges are progressively removed from a network, by contrast with the agglomerative hierarchical clustering method; (2) the edges to be removed are chosen by computing betweenness scores as described in detail below; (3) the betweenness scores are recomputed following the removal of each edge. The motivation behind the method is as follows.

Thus if we consider some model of traffic on the network and look for the edges with highest traffic, we should find the edges between the communities. Removing these should then split the network into its natural communities.

The betweenness of an edge is defined to be the number of geodesic (i.e., shortest) paths between vertex pairs that run along the edge in question, summed over all vertex pairs.

modularity, which is a numerical index of how good a particular division is.

fraction of all edges that lie within communities minus the expected value of the same quantity in a graph in which the vertices have the same degrees but edges are placed at random without regard for the communities.

Tyler et al. suggest instead that only a subset of vertices i be summed over, giving partial betweenness scores for all edges; if a random sample is chosen, this will give a Monte Carlo estimate of betweenness that tends to the true betweenness as the size of the sample becomes large.

stochastic element into the algorithm. By doing so, vertices whose community assignment is ambiguous, like vertex 3 in Figure 2, will sometimes be put in one community and sometimes in another, and by repeating the calculation many times one can make an estimate of the extent to which particular assignments are reliable.

short loops of edges in the networkloops of length three, or triangles, in the simplest case. Edges that run between communities (see Fig. 1) are unlikely to belong to many short loops,

it relies on the presence of triangles in the network.

conjectured that essentially all real-world networks have a statistically high proportion of triangles in them [41], but recent results making use of a more accurate null model argue otherwise

consider the electrical circuit formed by placing a unit resistor on each edge of the network and then applying a unit potential difference between two vertices chosen arbitrarily. If the network divides strongly into two communities and the vertices in question happen to fall in different communities, then the spectrum of voltages on the rest of the vertices should, the authors argue, show a large gap corresponding to the border between the communities.

it can also be used to find the particular community to which a specified vertex belongs, without first finding all communities in the network

Chapter 8

Logic and category theory

1 Logic

1.1 Gödel Incompleteness Theorem

In this article we'll discuss Gödel's Incompleteness Theorem, which essentially says that *not all mathematical truths are provable.* Before Gödel, many people believed implicitly that mathematics was a path to discover all truths in the world (at least, truths that can be put in the language of mathematics), so this was a shocking result to many mathematicians.

It's important to note that the Incompleteness Theorem is a actual mathematical *theorem* ("metamathematical," if you like) not (just) a philosophical statement. Of course, many people have enjoyed thinking about the philosophical implications of it (which we'll skip here).

We'll give some context for GIT, sketch the proof of GIT, and discuss some of its implications.

Difference between truth and provable.

The idea behind GIT is to create a mathematical sentence that says

"I am not provable."

If this statement were false, then it would be provable. But then it must be true! This is a contradiction. Hence the statement is true, so *it is not provable.*

You might have two objections:

- "I" is an illegal self-reference: we can't make a mathematical statement refer to itself.
- But this statement is *obviously* true, and it doesn't tell us much if the statements we can't prove are obviously true anyway.

We first have to discuss self-reference.

We can't just allow it, otherwise we get weird paradoxes...

Problem 8.1.1: Consider the statement "This statement is false." If it's false, then it's true, and if it's true, it's false. Thus all of logic breaks down, and how can reality even exist?
What's wrong with this?

Problem 8.1.2: The hangman's paradox

1.2 Self-reference

Try this:

Problem 8.1.3: Write a computer program that prints out a copy of its own code. (You're not allowed to use any external files, etc.)

This problem seems impossible at first glance: how can a program contain a copy of itself AND the instruction to print itself out? It seems all of this would have to be larger than the program itself.

Could we build a robot that makes a copy of itself? Then the copy, sharing all the properties of the original robot, would have to be able to make another copy, and so forth, so it seems like the robot has infinitely many copies "inside" it, and that takes up infinitely much space.

But this line of reasoning is incorrect. After all, humans succeed in making more humans—not exact copies, but close enough—without an infinite sequence of smaller and smaller homunculi in our sperm/egg. (But for a fascinating story about an alternate reality where the homunculi "run out," see Ted Chiang's story.) We know we have DNA, a code that can make copies of itself.

Can we write a sentence in English so that when you carry it out, you create a copy of the sentence? Sure,

- Print out a copy of this sentence.

We know what we mean by "this sentence," but it's not clear how to make a computer program understand this. So can we write a sentence in English so that when you carry it out, you create a copy of the sentence, *without* using self-referencing words like "this"?

- Print the following sentence two times, the second time in quotes.

  "Print the follow sentence two times, the second time in quotes."

This time we don't have an illegal self-reference: we could imagine converting this into a computer program that knows what is meant by "the following sentence."

Why did this work? The key point is that we *thought of a statement in two ways.*

🔑

1. We thought of a statement as a *command*: Print the following sentence two times, the second time in quotes.

2. We thought of a statement as simply a *string, a sequence of symbols without meaning.* The second line is not carried out as a command; instead it is used as input into the first line: “Print the following sentence two times, the second time in quotes.”

So you can now have a go at writing a **quine** (program that prints out its own code) in your favorite programming language. Solutions are available here `http://rosettacode.org/wiki/Quine`.

For much, much more on self-reference, see Hofstadter’s book Gödel Escher Bach.

1.3 Undefinability of truth

We will also view mathematical statements in two ways: as something that has meaning (semantics) and something that is just “a string of symbols (rather, a number) to be operated on.”

1.4 Example class 1

5. (It’s not a set in any reasonable set theory.)

   Claim: $A = \mathcal{P}(f(A))$.

   Proof: For all x with $\mathcal{P}(f(x)) \subseteq x$, $A \subseteq x$. Now apply f to A to get that $f(A) \subseteq f(x)$, and $\mathcal{P}(f(A)) \subseteq \mathcal{P}(f(x)) \subseteq x$.

   Thus $\mathcal{P}(f(A)) \subseteq A$. Thus $A = \mathcal{P}(f(A))$. $\square$

   Thus $f(A) \in A$. Let $B = A \backslash \{f(A)\} \subseteq A$.

   Claim: $\mathcal{P}(f(B)) \subseteq B$.

   Proof: $\mathcal{P}(f(B)) \subseteq \mathcal{P}(f(A)) \backslash \{f(A)\} \subseteq A \backslash \{f(A)\} \subseteq B$.

   This is a contradiction because $B \subset A$ but A is minimal.

21. $F(0) = 1$, $F(1) = 1$, $F(n+2) = F(n) + F(n+1)$. Define $g(0) = \mathrm{pair}(1,1)$ and $g(n+1) = pair(fst(g(n)) + snd(g(n)), fst(g(n))$, $F(n) = snd(g(n))$.

   🔑 Pipelining: keep track of the multiple previous values, and project.

   (2) $H_f(0,n) = f(n)$ and $H_f(m+1,n) = f(H_f(m,n))$, so $H_f(m,n) = f^{(m+1)}(n)$.

   (3) Pipeline, try to define $F(n) = \langle H(n), n \rangle$. Idea: $H(n+1)$ is H iterated n times *applied to*

22. Being coprime is a "primitive recursive predicate." (bounded quantification) Now sum over $m < n$.

33. easy

?. Build an immune set. Let $W_i = \{n \in \mathbb{N} : \{i\}(n) \downarrow\}$ be an enumeration of languages accepted by Turing machines. Let $Z_0, Z_1, \ldots$ be the infinite semidecidable sets. Let A_0, B_0 be the first/second element of Z_0, and $A_{n+1} = A_n \cup \{$first element of $Z_{n+1} \setminus \bigcup_{i<n+1}(A_n \cup B_n)\}$. make up some subset of the complement. Put things in the complement to ensure none is going to be a subset. $B_{n+1} = B_n \cup \{$the first element of $Z_{n+1} \setminus (\bigcup_{i=n+1}(A_i \cup B_i) \cup A_{n+1})\}$. Let $X = \bigcup_{n \in \mathbb{N}} A_n$.

38. (iv) take union of stuff stopped after a stages. $X_a = \{n : T(n, n, a)$ halts$\} = \{n : \{n\}(n) \downarrow_a\}$. Let $X = \bigcup_a X_a$.

61. Get own number e, and then halt if x is greater than e.

    Let $h(n)$ be the Gödel code of the Turing machine machine that does (take input m and if $m < n$ then HALTS otherwise goes in an infinite loop). By the fixed point theorem there is $e \in \mathbb{N}$ such that $\{e\} = \{h(e)\}$.

    Define $h : \mathbb{N} \to \mathbb{N}$ by the Gödel code of the Turing machine that takes input m and run $\{m\}(n)$. We get $\{e\} = \{h(e)\}$.

2 Topos theory

These are notes from the first lecture of the Topos Theory course. I ended up not taking it.

2.1 Cartesian closed categories

Definition 8.2.1: Let $\mathcal{C}$ be a category with finite products.

1. An object A of $\mathcal{C}$ is exponentiable if $(-) \times A : \mathcal{C} \to \mathcal{C}$ has a right adjoint $(-)^A$.

2. $\mathcal{C}$ is **cartesian closed** if all its objects are exponentiable.

Think of them as hom sets internalized to the category in which we're working. The property is precisely the adjunction.

Example 8.2.2: 1. ((Set)) is cartesian closed, with B^A taken to be the set of all functions $A \to B$. Given $f : C \times A \to B$, we can regard f as a function $\overline{f}(c)(a) = f(c, a)$.

2. ((Cat)) is cartesian closed, with $\mathcal{D}^{\mathcal{C}}$ taken to be the functor category $[\mathcal{C}, \mathcal{D}]$.

3. In ((Sp)), the category of topological spaces and continuous maps, X is exponentiable iff it is locally compact. In this case we define Y^X to be the set of continuous maps $X \to Y$, with the compact-open topology.

4. For any small category $\mathcal{C}$, the functor category $[\mathcal{C}, ((Set))]$ is cartesian closed. The Yoneda lemma tells us how to define G^F for functions F and G: $G^F(U)$ is a bijection with the set of natural transformations $gU \to G^F$, and has hence with the set of natural transformations $gU \times F \to G$. We take this as the definition of $G^F(U)$: give a $U \to V$, we define $G^F(\alpha) : G^F(V) \to G^F(U)$to be composition with $g\alpha \times F \to gV \times F$.

   This makes G^F into a functor $\mathcal{C}^{\mathrm{op}} \to ((\mathrm{Set}))$: the bijection between morphisms $H \to G^F$ and $H \times F \to G$ holds by definition if H is representable.

   An arbitrary H can be expressed as a colimit $\mathrm{colim}_{i \in g}\, gU_i$ of representables, so we have

   $$\begin{aligned}[\mathcal{C}^{\mathrm{op}}, \mathrm{Set}](H, G^F) &\cong \lim_{i \in g} [\mathcal{C}^{\mathrm{op}}, \mathrm{Set}][yU_i, G^F] \\ &\cong \lim_i [\mathcal{C}^{\mathrm{op}}, ((\mathrm{Set}))] \\ &\cong [\mathcal{C}^{\mathrm{op}}, ((\mathrm{Set}))](\mathrm{colim}_i(yU_i \times F), G) \\ &\cong [\mathcal{C}^{\mathrm{op}}, ((\mathrm{Set}))]((\mathrm{colim}_i\, yU_i) \times F, G).\end{aligned}$$

   since $(-) \times F$ preserves colimits, because $(-) \times A$ does so in $((\mathrm{Set}))$ and products and limits in $[\mathcal{C}^{\mathrm{op}}, ((\mathrm{Set}))]$ are constructed pointwise. Alternatively, for existence, use the Adjoint Functor Theorem. (It's useful to have an explicit expression though.)

5. A poset $(P, \leq)$ is cartesian closed iff it's a **Heyting semilattice**, i.e., a $\wedge$-semilattice equipped with an additional operation $(a, b) \mapsto (a \implies b)$ with the property $c \leq (a \implies b)$ iff $c \wedge a \leq b$.

   If P also has finite $\vee$, we call it a **Heyting algebra**.

   If P is complete (i.e., has arbitrary $\vee$'s), then it's a Heyting algebra iff it satisfies $a \wedge \vee S = \bigvee \{a \wedge s : s \in S\}$ for all $a \in P$, $S \subseteq P$. In particular, for any space X, the lattice $\mathcal{O}(X)$ of open subsets of X satisfies this law, and is hence a Heyting algebra.

Most categories are either cartesian closed or have almost no exponentiable objects. For example, in ((Grp)) the only exponentiable obj is the terminal object, which is always exponentiable. (The product map is the dentity functor, which has itself as an adjoint.) Thus we can think of cartesian closed as a property of set-like categories rather than group-like categories.

In general, B^A is characterized by the existence of a map $B^A \times A \xrightarrow{\mathrm{ev}}$ (the counit of the adjunction) such that given any $f : C \times A \to B$, there exists a unique $\overline{f} : C \to B^A$ such that

$$C \times A \xrightarrow{\overline{f} \times 1_A} B^A \times A \xrightarrow{\mathrm{ev}} B$$

equals f.

Now we'll need to assume the existence pullbacks (all finite limits).

Given any object B of C, we write $\mathcal{C}/B$ for the for the category whose objects are morphisms $f : A \to B$ in $\mathcal{C}$, and whose morphisms are commutative triangles

$$\begin{tikzcd} A \arrow[rr] \arrow[dr, "f"'] & & A' \arrow[dl, "f'"] \\ & B & \end{tikzcd}$$

The forgetful functor $\Sigma_B : \mathcal{C}/B \to \mathcal{C}$ sending $f : A \to B$ to A has a right adjoint B^* if $\mathcal{C}$ has finite products, given by $B^*(A) = (A \times B \to B)$.

Lemma 8.2.3: If $\mathcal{C}$ has finite limits, then $B^* : \mathcal{C} \to \mathcal{C}/B$ has a right adjoint π_B iff B is exponentiable.

Proof. $\Longrightarrow$: $(-) \times B$ is the composite $\Sigma_B \circ B^*$, so it has a right adjoint $\pi_B \circ B^*$.

$\Leftarrow$: Given $f : A \to B$ in $\mathcal{C}/B$, form the product

$$\begin{tikzcd}
P \arrow[r] \arrow[d] & A^B \arrow[d, "f^B"] \\
1 \arrow[r, "\overline{\pi_i}"] & B^B
\end{tikzcd}$$

The morphisms $C \to P$ correspond to morphisms $C \to A^B$ making

$$\begin{tikzcd}
C \arrow[r] \arrow[d] & A^B \arrow[d, "f^B"] \\
1 \arrow[r] & B^B
\end{tikzcd}$$

commute, and hence to morphisms $C \times B \to A$ making

$$\begin{tikzcd}
C \times B \arrow[r] \arrow[d] & A \arrow[d, "f"] \\
1 \times B \arrow[r, "\pi_i"] & B
\end{tikzcd}$$

commute, i.e., to morphisms $B^*C \to f$ in $\mathcal{C}/B$. □

Definition 8.2.4: We say $\mathcal{C}$ is **locally cartesian closed (lcc)** if it has finite limits and all its sliced categories $\mathcal{C}/B$ (including $\mathcal{C}/1 \cong \mathcal{C}$) are cartesian closed.

This is stronger than being cartesian closed.

Corollary 8.2.5: For $\mathcal{C}$ with finite limits, $\mathcal{C}$ is lcc iff, for every $f : A \to B$ in $\mathcal{C}$, the functor $f^* : \mathcal{C}/B \to \mathcal{C}/A$ has a right adjoint π_F.

Proof. $(\mathcal{C}/\mathcal{B})/f$ is isomorphic to $\mathcal{C}/A$, by an isomorphism which identifies $f^* : \mathcal{C}/B \to \mathcal{C}/A$ with $f^* : \mathcal{C}/B \to (\mathcal{C}/B)/f$.

Hence ((Cat)) is not lcc, since epimorphism aren't stable under pullback. □

Chapter 9

Number theory

[Readability: 2]

What I've learned in number theory.

- Elementary number theory—Olympiad-style
- Additive number theory
  - 18.784, following Nathanson, Ch. 1-8
  - Arithmetic combinatorics at Cambridge, following Gowers's and Green's notes, Tao-Vu.
- Algebraic number theory (including class field theory), Section **??**
- Analytic number theory—up to proof of Siegel-Walfisz. `http://web.mit.edu/~holden1/www/math/analytic-nt.pdf`
  - Davenport, Elkies's notes
- Elliptic curves and arithmetic geometry (Section 3)
- Modular forms
  - 18.785
  - Dirichlet series and modular forms, Apostol
  - Ken Ono's REU—paper on my website

A collection of problems

1. Somebody incorrectly remembered Fermat's little theorem as saying that the congruence $a^n + 1 \equiv a \pmod{n}$ holds for all a if n is prime. Describe the set of integers n for which this property is in fact true. (1.1, `http://www-groups.dcs.st-and.ac.uk/~john/Zagier/Problems.html`) Idea: no prime powers, $p \mid n$ gives $p-1 \mid n$. (order)

2. Prove or disprove: for every odd number k there is a prime of the form $2^n k + 1$. (1.2, `http://www-groups.dcs.st-and.ac.uk/~john/Zagier/Problems.html`) Covering congruence! (order)

1 Algebraic number theory

Writings:

1. ANT notes. `http://web.mit.edu/~holden1/www/math/ant.pdf`

Learned from...

- 18.786
- Cox, Primes of the form $x^2 + ny^2$ [R]
- Neukirch
- Serre (Local fields)
- Milne, ANT and CFT
- Cassels-Fröhlich

1.1 Analytic algebraic number theory

3/13/14

Ch. The analytic class number formula

$$\boxed{\begin{aligned}
\frac{\pi}{4} &= 1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}+\cdots \text{ eq:acnf-ex1} && (9.1)\\
\frac{\ln(\sqrt{2}+1)}{\sqrt{2}} &= 1-\frac{1}{3}-\frac{1}{5}-\frac{1}{7}+\frac{1}{9}+\cdots \text{ eq:acnf-ex2} && (9.2)\\
\frac{2\ln\left(\frac{1+\sqrt{5}}{2}\right)}{4} &= 1-\frac{1}{2}-\frac{1}{3}+\frac{1}{4}+\frac{1}{6}+\cdots \text{ eq:acnf-ex3} && (9.3)\\
&= \sum_{n=1}^{\infty} \frac{1}{5n+1}-\frac{1}{5n+2}-\frac{1}{5n+3}+\frac{1}{5n+4}
\end{aligned}}$$

See Mazur in PCTM for an introduction to algebraic number theory that highlights these formulas.

In this chapter we explore a formula that relates *analytic* with *algebraic* quantities: values of the zeta function with the class number, regulator, and discriminant of a number field.

In this section we will prove the analytic class number formula.

Theorem 9.1.1 (Analytic class number formula)**:** Let K be a number field. Then

$$\operatorname{Res}_{s=1}\zeta_K(s) = \frac{2_1^r(2\pi)^{r_2} h_K \operatorname{Reg}_K}{\sqrt{|\Delta_K|}w_K}$$

where h_K is the class number, Reg_K is the regulator, w_K is the number of roots of unity in K, and Δ_K is the discriminant.

Our plan is the following. We grok what's going on by looking at the class number formula for quadratic fields—which already gives all the different types of behavior. To prove the theorem for general K it's just a matter of getting reacquainted with the embedding $\mathbb{R}^r \times \mathbb{C}^s$, and getting our hands dirty. We'll massage our formula into nicer forms for quadratic fields and for cyclotomic fields, and see what algebraic information we can milk out from the class number formula.

How does this formula come about?[1] $\zeta_K(s)$ is a sum over ideals of $\mathcal{O}_K$ where the ideals are weighted depending on their norm; we are "counting ideals" with appropriate weight. The growth of ζ_K near $s = 1$ depends estimates for the number of ideals with norm $< r$. An expression for the *analytic* quantitiy $\operatorname{Res}_{s=1}\zeta_K(s)$ comes from combining the following *geometric* and *algebraic* information.

1. Geometric: We count algebraic integers in K. Geometrically, they form a lattice in $\mathbb{R}^r \times \mathbb{C}^s$. We can estimate the number of points in a given region around the origin. This depends on the embedding, on the volume of a fundamental parallelpiped of the lattice. This is how we get the quantity

$$\frac{2^r(2\pi)^s}{\sqrt{|\Delta_K|}}.$$

2. Algebraic: Note $\zeta_K(s)$ is a sum over *ideals*, not over *numbers* in $\mathscr{O}_K$. So we need to multiply by a factor that tells us what we're off by in considering numbers rather than ideals; we can do this because of the multiplicative structure of $\mathscr{O}_K$. This will depend on the units (the fundamental units and the roots of unity) and the class number. This is how we get the factor

$$\frac{h_K \operatorname{Reg}_K}{w_K}.$$

[1] We follow the discussion in `http://math.stackexchange.com/questions/292104/how-to-derive-the-class-number-formula`.

Make sure you remember the following.

1. How to show $\operatorname{Res}_{s=1}\zeta(s) = 1$. (We used a "summation by parts" argument. The same argument analytically continued $\zeta(s)$ from $\Re s > 1$ to $\Re s > 0$.)

2. The embeddings used to prove the finiteness of the class group and find the rank of the unit group. The definition of the regulator.

Problem 9.1.2: Recall that the zeta function for $\mathbb{Q}$ can be defined as

$$\zeta(s) = \prod_{\text{prime } p}\left(1 - \frac{1}{p^s}\right) = \sum_{n=1}^{\infty}\frac{1}{n^s}$$

for $s > 1$. How do we modify this definition to define the zeta function for an arbitrary finite extension $K/\mathbb{Q}$?
If we expand out $\zeta_K(s) = \sum_n \frac{a_s}{n^s}$, what

The identity above relied on unique factorizaiton. In general we only have unique factorization of *ideals*, and we measure the size of an ideal with the *norm*. So we define

$$\zeta_K(s) = \sum_{\mathfrak{a}\in I_K}\frac{1}{\mathfrak{N}\mathfrak{a}^s}$$

and find it equals $\prod_{\mathfrak{p}}\left(1 - \frac{1}{\mathfrak{N}\mathfrak{p}^s}\right)$

1. Quadratic number fields

Problem 9.1.3: 1. Consider the zeta function for $K = \mathbb{Q}(i)$. When we expand out $\zeta_K(s) = \sum_n \frac{a_s}{n^s}$, what do the coefficients a_s represent?

2. Evaluate $\operatorname{Res}_{s=1} \zeta_K(s)$ (recall how we evaluated $\operatorname{Res}_{s=1} \zeta(s)$), using some area calculations.

3. Can you write $\zeta_K(s)$ in terms of L-functions you are familiar with? Derive (9.1).

4. Do the same for $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]]$ and $\mathbb{Z}[\sqrt{-5}]$. What's different about the last case?

5. Do the same for $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. (The argument is more complicated, but make a guess.) Derive (9.2) and (9.3).

6. Conjecture the general class number formula (we already told you, but don't look back).

7. We saw that in (9.1) through (9.3) that we can evaluate in closed form series of the form $\sum \pm n$ (where the $\pm$ are periodic). What happens when you combine this with part 3?

   Can you do this in general? Given a character $\chi : \mathbb{Z}/N \to \{-1, 1\}$, evaluate in closed form
   $$\sum_{n=1}^{\infty} \frac{\chi(n)}{n}.$$

   Try to simplify your formula as much as possible.

   Hint: (a) power series are nice, (b) $\sum_{n=1} \frac{1}{n}$ reminds us of logarithms. However we seem to have nasty sums such as $\sum_{n \equiv m \pmod p} \frac{1}{n^s}$. What's the technique?

For a leisurely account of the class number formula for quadratic fields (assuming few prerequisites) see [PROMYS notes].

If d is a imaginary quadratic field with discriminant D, then

$$\operatorname{Res}_{s=1} \zeta_K(s) = \frac{2\pi h_K}{w_K\sqrt{|D_K|}},$$

and if d is a real quadratic field and ε a fundamental unit, then (note $w_K = 1$)

$$\operatorname{Res}_{s=1} \zeta_K(s) = \frac{\pi h_K \ln \varepsilon}{\sqrt{|D_K|}}$$

The proof.

1. Reduce to a sum over numbers in $\mathscr{O}_K$, not ideals. We separate the sum by ideal classes

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathfrak{N}\mathfrak{a}^s}$$

$$= \sum_{[I]\in \mathrm{Cl}_K} \sum_{\mathfrak{a}\in[I]} \frac{1}{\mathfrak{N}\mathfrak{a}^s}$$

where the sum $[I] \in \mathrm{Cl}_K$ is over ideal classes.

Now for each $[I]$ choose $\mathfrak{b}_I \in [I]^{-1}$

$$= \sum_{[I]\in \mathrm{Cl}_K} \sum_{\mathfrak{a}\in[I]} \frac{1}{\mathfrak{N}(\mathfrak{a}\mathfrak{b})^s}\mathfrak{N}(\mathfrak{b}_I)^s$$

$$= \sum_{[I]\in \mathrm{Cl}_K} \sum_{(\alpha),\alpha\in\mathfrak{b}_I} \frac{1}{\mathfrak{N}(\alpha)^s}\mathfrak{N}(\mathfrak{b}_I)^s$$

since $\mathfrak{a} \mapsto \mathfrak{b}$ is a bijection from the ideals in $[I]$ to principal ideals that are divisible by $\mathfrak{b}$, i.e., principal ideals in the form (α), $\alpha \in \mathfrak{b}$. If we manage to show each of the inner sums is $\frac{2^r(2\pi)^s h_K \mathrm{Reg}_K}{\sqrt{|\Delta_K} w_K}$, the we'll be done.

2. The sum is over principal ideals, but we'd like the sum to be over elements. The obstruction is that many elements will give the same ideal, so we'd like a canonical way of choosing a generator of (α). We'd like a region such that every set of associated elements has exactly one element in that region, a kind of *fundamental domain.*

Any two generators will differ by a product $\zeta\varepsilon_1^{a_1}\cdots\varepsilon_{r+s-1}^{a_{r+s-1}}$ where ζ is a root of unity and $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ are the fundamental units. Now in the case of a vector space, and we say 2 elements are equivalent if they differ by an element of a lattice, we know what a fundamental domain would look like—a parallelopiped. We have here a product rather than a $\mathbb{Z}$-linear combination, so we'll have to embed and then take logs.

Recall the embedding and the log map from Proposition **??**:

$$K \xrightarrow{\sigma=(\sigma_1,\ldots,\sigma_{r+s})} \mathbb{R}^r \times \mathbb{C}^s \xrightarrow{L=(\ln|\cdot|,\ldots,\ln|\cdot|,\ln 2|\cdot|,\ldots \ln 2|\cdot|)} \mathbb{R}^{r+s}.$$

(The kernel of this map is the roots of unity.) Recall that $L(U_K)$ is the subspace with $x_1 + \cdots + x_{r+s} = 0$, i.e. the subspace with $\mathbf{x}\cdot(1,\ldots,1) = 0$. We choose our canonical element α such that its projection onto this subspace is in the fundamental parallelopiped made by the $L(\varepsilon_1), \ldots, L(\varepsilon_{r+s-1})$, i.e. we require

$$L(\alpha) \in \underbrace{([0,1]L(\varepsilon_1) + \cdots + [0,1]L(\varepsilon_{r+s-1}))}_{=:P} + (1,\ldots,1)$$

(For a set S of scalars and a vector v we let $Sv = \{sv : s \in S\}$.) Taking the inverse image under σ and noting the kernel is the roots of unity (Proposition **??**), we have the following.

- For any $\alpha \in \mathscr{O}_K$, there are exactly w_K associates β of α such that

$$\sigma(\beta) \in \mathbb{R}L^{-1}(P).$$

3. Now we show how the sums in 2 reduce to a volume calculation. We claim the following.

Lemma 9.1.4: Let L be a lattice in $\mathbb{R}^n$. Let V be a bounded, measurable set containing the origin that the points at a distance of at most c from the boundary satisfy

$$\mathrm{Vol}[B(\partial V, 1)] \precsim_c t^{n-1}.$$

(There aren't too many points near the surface.)[2] Then

1. The number of points inside tV satisfies

$$|tV \cap L| \sim \frac{\mathrm{Vol}(V)}{\Delta(L)} t^n$$

2. Suppose $[0,1]V = V$. Let $N(x) = (\inf\{c > 0 : x \in cV\})^n$. The function

$$\sum_{x \in L} \frac{1}{N(x)^s}$$

is meromorphic with residue equal to $\frac{\mathrm{Vol}(V)}{\Delta(L)}$ in a neighborhood of $s = 1$.

Proof. 1. This is standard: Take a fundamental parallelopiped and place one at each point in $tV \cap L$; now bound the difference between this area and the area of tV.

2. We use summation by parts to get

$$\sum_{x \in L} \frac{1}{N(x)^s} = \int_t \#\{x \in L : |x| < t\} \frac{1}{t^{s+1}}\, dt = \int_t [\frac{\mathrm{Vol}(V)}{\Delta(L)} t^n + O(t^{n-1})]|x| \frac{1}{t^{s+1}} = \ldots$$

a discrepancy in exponents

□

4. Calculate the volume of $\sigma(\beta) \in [0,1]L^{-1}P$, which will be the V in (3). We want to evaluate

$$\int \cdots \int_{[0,1]L^{-1}P \subseteq \mathbb{R}^r \times \mathbb{C}^s} dx_1 \,\ldots\ldots\, dx_s = \int \cdots \int_{[0,1]e^P 2^r (2\pi)^s} x_{r+1} \cdots x_s \, dx_1 \,\ldots\, dx_s$$

where we note that the integral only depends on $|x_i|$, so for the ones over $\mathbb{C}$ we can switch to polar coordinates (θ, r), and integrating over θ gives the 2π. Now change coordinates via the map L which has Jacobian $e^{x'_1} \cdots e^{x'_r} e^{2x'_{r+1}} \cdots e^{2x'_s}$ to get

$$\int \cdots \int_{P-[0,\infty)(1,\ldots,1)} 2^r (2\pi)^s e^{x'_{r+1}} \cdots e^{x'_s} (e^{x'_1} \cdots e^{2x'_s}\, dx'_1 \,\ldots\, dx'_s) = 2^r (2\pi)^s \mathrm{Vol}(P)$$
$$= 2^r (2\pi)^s \, \mathrm{Reg}_K \,.$$

Now combine everything: Each sum in (1) is w_K times the volume, so $\frac{w_K 2^r (2\pi)^s \,\mathrm{Reg}_K}{\sqrt{|\Delta_K|}}$. qed.

get the $\sqrt{}$ clear.

Theorem 9.1.5 (Formulas for L-functions)**:** We have

$$L(1, \chi) = \begin{cases} -\frac{\tau(\chi)}{m} \sum_{k \in (\mathbb{Z}/m)^\times} \overline{\chi(k)} \ln \sin \frac{\pi k}{m}, & \chi \text{ even} \\ \frac{\pi i \tau(\chi)}{m^2} \sum_{k \in (\mathbb{Z}/m)^\times} \overline{\chi(k)} k, & \chi \text{ odd.} \end{cases}$$

In particular, if K is a real quadratic field with discriminant D, then

$$L(1, \chi) = -\frac{1}{\ln \varepsilon} \sum_{0 < k < \frac{D}{2}, x \perp D} \chi(x) \ln \sin \frac{\pi k}{m}.$$

[2] See also VI.§2 in Lang. His Theorem 2 is phrased in terms of $(n-1)$-Lipschitz parametrizable boundaries.

(In BS, Theorem 3, p. 336; Theorem 1, p. 344)

Proof. We'll write the nasty sum $\sum_{n\equiv m}\frac{1}{n^s}$ (the partial zeta function) in terms of nice sums using characters. We have

$$\begin{aligned}\sum_n \chi(n)\frac{1}{n^s} &= \sum_m \chi(m)\sum_{n\equiv m}\frac{1}{n^s}\\ &= \sum_m \chi(m)\sum_k\sum_n \zeta^{(n-m)k}\frac{1}{n^s}\\ &= \sum_m\sum_k \chi(m)\zeta^{-mk}\sum_n \frac{\zeta^{-nk}}{n^s}\end{aligned}$$

use abel summation. □

We can calculate for cyclotomic

$$h = \frac{p^{p/2}}{2^{m-1}\pi^m R}\prod_{\chi\neq\chi_0} L(1,\chi)$$

for even and odd characters

$$\begin{aligned}|L(1,\chi^{2k}) &= \frac{2}{\sqrt{p}}|\sum_{r=0}^{m-1}\theta^{2kr}\ln|1-\zeta^{g^r}|\\ |L(1,\chi^{2k-1}) &= \frac{\pi}{p^{3/2}}|F(\theta^{2k-1})|\end{aligned}$$

and

$$h = \underbrace{\frac{2^{m-1}}{R}\prod_{k=1}^{m-1}\left|\sum_{r=0}^{m-1}\theta^{2kr}\ln|1-\zeta^{g^r}|\right|}_{=h^+}\underbrace{\frac{1}{(2p)^{m-1}}|F(\theta)\cdots F(\theta)^{p-2}|}_{h^*}.$$

Show directly h^+ is class number of totally real subfield.

problem for CFT: Show that if L/K is an extension with no proper unramified extension, then $h_K \mid h_L$.

Where else does the class number appear? There is no explicit formula for the fundamental unit, but remarkably we can find an explicit formula that works for all real quadratic fields and gives a *power* of the fundamental unit. The class number appears as the exponent.

Theorem 9.1.6: Let K be a real quadratic field with discriminant D and character χ. Then

$$\eta := \prod_{a\perp D, 0<a<\frac{D}{2}}\left(\sin\frac{\pi a}{D}\right)^{-\chi(a)}$$

is a unit and if $\varepsilon > 1$ is the fundamental unity,

$$\varepsilon^h = \eta.$$

In particular, $\prod_{\left(\frac{b}{p}\right)=-1}\sin\frac{\pi b}{p} > \prod_{\left(\frac{a}{p}\right)=1}\sin\frac{\pi a}{p}$.

For $p \equiv 1 \pmod 4$, think of the last statement as saying that quadratic residues mod p cluster at the beginning of $(0, p/2)$ (where $\sin \frac{\pi x}{p}$ is small) and the quadratic residues mod p cluster at the end. What about $p \equiv 3 \pmod 4$?

Proof. Exponentiate both sides of

$$\begin{aligned} h &= -\frac{1}{\ln \varepsilon} \sum_{x \perp D, 0<x<\frac{D}{2}} \chi(x) \ln \sin \frac{\pi x}{D} \\ (\ln \varepsilon) h &= \sum_{x \perp D, 0<x<\frac{D}{2}} \ln \sin \frac{\pi x}{D} (-\chi(x)) \\ \varepsilon^h &= \prod_{a \perp D, 0<a<\frac{D}{2}} \left(\sin \frac{\pi a}{D}\right)^{-\chi(a)}. \end{aligned}$$

□

In the imaginary quadratic case, we have an explicit formula for the class number that depends just on calculating quadratic residues, and not on any anything analytic (ln, sin,...).

Theorem 9.1.7: Let $p \equiv 3 \pmod 4$ and let R, N be the number of quadratic residues and nonresidues in $(0, \frac{p}{2})$. Then the class number of $\mathbb{Q}(\sqrt{-p})$is

$$h = \begin{cases} \frac{1}{3}(R-N), & p \equiv 3 \pmod 8 \\ R-N, & p \equiv 7 \pmod 8. \end{cases}$$

In particular, $R > N$.

(p. 346 in BS)

Proof. We use an averaging argument: to simplify a sum we pair up elements like $\chi(x), \chi(m-x)$ or $\chi(x), \chi(\frac{m}{2}+x)$ for cancellation.

Consider 2 cases.

1. If $|D|$ is even, it is a multiple of 4. Note $2^{r-1}+1$ is not a quadratic residue modulo 2^r for $r \geq 2$ (why), so $\frac{m}{2}+1$ is not a quadratic residue modulo m, and $\chi(m) = -1$. We pair up $\chi(x), \chi(x+\frac{m}{2})$ to get

$$h = \frac{1}{2} \sum_{0<x<\frac{m}{2}} \chi(x).$$

2. If $|D|$ is odd, noting the character of an imaginary quadratic field is odd, $\chi(-1) = -1$, again we pair up $\chi(x)$ and $\chi(m-x)$ to get

$$h = -\frac{2}{|D|} \sum_{0<x<\frac{m}{2}} \chi(x)x + \sum_{0<x<\frac{m}{2}} \chi(x).$$

There is a sum of $\chi(x)x$, but there's a trick to get rid of it. We instead flip some of the x into $m-x$, so that we hit exactly the multiples of 2, and then take out a $\chi(2)$. We get

$$h\chi(2) = -\frac{4}{|D|}\sum_{0<x<\frac{m}{2}}\chi(x)x + \sum_{0<x<\frac{m}{2}}\chi(x).$$

Subtracting we get

$$h = \frac{1}{2-\chi(2)}\sum_{0<x<\frac{m}{2}, x\perp D}\chi(x).$$

Now apply to $p \equiv 3 \pmod 4$, $\mathbb{Z}\left[\frac{-1+\sqrt{-p}}{2}\right]$. □

Note that there does not seem to be an "elementary" proof of $R > N$ for $p \equiv 3 \pmod 8$. See http://mathoverflow.net/questions/25707/intuition-for-a-formula-that-expr for a discussion.

(Euler's remarkable prime-producing polynomial) No nonconstant polynomial in one variable can produce only primes at integer values. But the polynomial x^2+x+1 does awfully well: it produces primes for $0 \le x \le 39$: 41 , 43 , 47 , 53 , 61 , 71 , 83 , 97 , 113 , 131 , 151 , 173 , 197 , 223 , 251 , 281 , 313 , 347 , 383 , 421 , 461 , 503 , 547 , 593 , 641 , 691 , 743 , 797 , 853 , 911 , 971 , 1033 , 1097 , 1163 , 1231 , 1301 , 1373 , 1447 , 1523.

Problem 9.1.8: Why? (What's special about **41**?) Give a conjecture that generalizes this, and prove it. Can you weaken one of the directions?
Do you think that x^2+x+1 has lots of primes compared to other quadratic polynomials? (Can you give a conjecture for the density of primes in x^2+x+n?)

[3] [4]

Theorem 9.1.9: Let $n \in \mathbb{N}$. The following are equivalent.[5]

1. $K := \mathbb{Q}(\sqrt{1-4n})$ is a UFD.
2. x^2+x+n is prime for integer $x \in [0, n-2]$.
3. x^2+x+n is prime for integer $x \in [0, \lfloor\sqrt{\frac{n}{3}}\rfloor]$.

Proof. Recall that every ideal class has a representative with $\mathfrak{Na} \le \frac{\sqrt{1-4n}}{3}$. (Theorem 16.4.1) These $\mathfrak{a}$ satisfy $\mathfrak{a}\bar{\mathfrak{a}} \le \frac{\sqrt{1-4n}}{3}$. Thus K is a UFD iff for every $0 < m \le n-2$ with $m = \mathfrak{a}\bar{\mathfrak{a}}$, $\mathfrak{a}$ is principal. It suffices to check the primes m (why?), so (1) is equivalent to

1.1. For every prime $p \le n-2$, p does not split into nonprincipal ideals.

[3] See http://math.stackexchange.com/questions/2561/eulers-remarkable-prime-producing-polyno

[4] See http://en.wikipedia.org/wiki/Ulam_spiral#Hardy_and_Littlewood.27s_Conjecture_F

[5] (2) $\iff$ (3) was IMO 1987/6.

How could we test if a prime p of $\mathbb{Z}$ splits into nonprincipal ideals?

1. We have a criterion for when p splits: p splits iff $x^2+x+n \equiv 0 \pmod{p}$ has a solution. (This is since p splits $\iff \mathbb{Z}\left[\frac{1+\sqrt{1-4n}}{2}\right]/(p) = \mathbb{F}_p[X]/(X^2+X+N)$ is not a field $\iff x^2+x+n \equiv 0 \pmod{p}$ for some x.)

2. If a prime splits into *principal* ideals, then for some a, b of the same parity,
$$p = \frac{-a+b\sqrt{1-4n}}{2} \cdot \frac{-a-b\sqrt{1-4n}}{2} = \frac{a^2+b^2(4n-1)}{4} \ge n$$

So $p < n$ automatically means either p remains prime or p splits into *non*principal ideals. So 1.1 is equivalent to

1.2. For every prime $p \le n-2$, $x^2+x+n \not\equiv 0 \pmod{p}$ for any x.

For $x \in [0, n-2]$, $x^2+x+p < n^2$ so if x^2+x+p is composite it has a prime factor less than n. But if (1.2) holds, then x^2+x+p cannot have any prime factors less than n, so (1.2) implies (2). (2) implies (1.2) because to see whether $x^2+x+n \equiv 0 \pmod{p}$ has a solution, it suffices to check $0 \le x \le p \le n$.

(2) is stronger than (3), so we need to check (3) $\implies$ (2). To do this, we show that if $\sqrt{\frac{n}{3}} < x \le n-2$ makes x^2+x+n composite, then there is a smaller x making it composite. How could we get a smaller solution?

Suppose x^2+x+n is composite. Let its smallest prime factor be p; note
$$p < \sqrt{x^2+x+n} < n.$$
Note that any $x \bmod p$ and $(p-1-x) \pmod{p}$ are also solutions of $x^2+x+n \equiv 0 \pmod{p}$. Thus if
$$x > \frac{p-1}{2}$$
then we can replace x with $y = x \bmod p$ or $y = p+1-x \bmod p$ to get a smaller solution. Note $y^2+y+n > n \ge p$, so y^2+y+1 is composite.

This is possible whenever
$$x > \frac{\sqrt{x^2+x+1}-1}{2}$$
which is true when $x \ge \sqrt{\frac{n}{3}}$. Thus if (3) is true, then there cannot be $0 \le x \le n-2$ making x^2+x+n prime; else taking the minimal such x gives a contradiction. □

Bernoulli numbers

Definition 9.1.10: Define the **Bernoulli numbers** as the coefficients of the exponential generating function
$$\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$
Alternatively, they are defined to satisfy $B_0 = 1$, $B_1 = 0$, and
$$\sum_{k=0}^{m-1} \binom{m}{k} B_k.$$

To see the equivalence, match up coefficients in

$$\frac{t}{e^t-1}\cdot\left(\sum_{n=0}^{\infty}B_n\frac{t^n}{n!}\right)=1.$$

(Shafarevich: notation: for a polynomial or power series $f(x)=\sum_k a_kx^k$, write $f(B)=\sum_k a_kB_k$. Then $\frac{t}{e^t-1}=e^{Bt}$ and $e^{at}e^{Bt}=e^{(a+B)t}$.

Bernoulli numbers pop up in many places.[6] One of the first applications is to give a formula for summing powers.

Theorem 9.1.11: Let

$$S_m(N):=\sum_{0\le n<N}n^m=1^m+\cdots+(n-1)^m.$$

Then

$$S_m(N)=\frac{1}{m+1}\left(\sum_{k=0}^{m}\binom{m+1}{k}B_kN^{m+1-k}\right).$$

Symbolically we can write

$$S_m(N)=\frac{1}{m+1}((B+N)^{m+1}-B^{m+1})$$

where we replace B^k by B_k.

Proof. We load up the $S_m(n)$ as coefficients of a generating function, and interchange the sums.[7]

$$\begin{aligned}\sum_{m=0}^{\infty}S_m(N)\frac{t^m}{m!}&=\sum_{m=0}^{\infty}\sum_{k=0}^{n-1}\frac{k^mt^m}{m!}\\&=\sum_{k=0}^{n-1}\sum_{m=0}^{\infty}\frac{(kt)^m}{m!}\\&=\sum_{k=0}^{n-1}e^{kt}\\&=\frac{e^{nt}-1}{e^t-1}\\&=\frac{e^{nt}-1}{t}\cdot\frac{t}{e^t-1}\\&=\left(\sum_{k=0}^{\infty}\frac{n^{k+1}t^k}{(k+1)!}\right)\left(\sum_{k=0}^{\infty}B_k\frac{t^k}{k!}\right)\\&=\frac{1}{m+1}\left(\sum_{k=0}^{m}\binom{m+1}{k}B_kN^{m+1-k}\right)\end{aligned}$$

The $\frac{e^{nt}-1}{t}$ produces the "$\frac{1}{m+1}((\bullet+N)^{m+1}-\bullet^{m+1})$." □

[6] http://en.wikipedia.org/wiki/Bernoulli_number

[7] See the generating functions lecture http://onlinemathcircle.com/wp-content/uploads/2011/04/18-genfunc.pdf §3.2 for another example where we load polynomials as coefficients of a generating function.

We will prove some number-theoretic properties of the B_n, and then mention where they pop up in number theory.

Theorem 9.1.12 (von Staudt)**:** Let p be prime and m even.

1. If $p-1 \nmid m$, then B_m is p-integral.

2. If $p-1 \mid m$, then pB_m is p-integral, and $pB_m \equiv 1 \pmod{p}$.

Theorem 9.1.13 (Kummer's congruence)**:** If p is prime, m is even, $p-1 \nmid m$, then $\frac{B_m}{m}$ is an integer, and

$$\frac{B_m}{m} \bmod p$$

depends only on $m \bmod p-1$.

We can evaluate zeta values in terms of Bernoulli numbers.

Theorem 9.1.14: We have

$$\sum_{n=1}^{\infty} \frac{1}{n^m} = \zeta(2m) = \frac{(-1)^{m-1}(2\pi)^{2m}}{2(2m)!} B_{2m}$$

and

$$\zeta(1-2m) = -\frac{\pi B_{2m}}{4m}.$$

Proof. How do we evaluate a sum like $\sum_{n=1}^{\infty} \frac{1}{n^m}$? The key is to view it as a special value of a periodic function. We'll get this function if we just load up the $\zeta(2m)$ as the coefficients of a generating function.

$$\begin{aligned}
\sum_{m=1}^{\infty} \zeta(2m) t^{2m} &= \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{1}{n^{2m}} t^{2m} \\
&= \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \left(\frac{t}{n}\right)^{2m} \\
&= \sum_{n=1}^{\infty} \frac{\left(\frac{t}{n}\right)}{1-\left(\frac{t}{n}\right)^2} \\
&= \sum_{n=1}^{\infty} \frac{t}{n^2-t^2} \\
&= \frac{1}{t} - \sum_{n\in\mathbb{Z}} \frac{1/2}{t-n} && \text{partial frac decomp}
\end{aligned}$$

What's a periodic function that has single poles exactly at $t \in \mathbb{Z}$? $-\frac{1}{2}\frac{e^{2\pi i t}}{e^{2\pi i t}-1}$. We can check indeed that its expansion equals that above. (Or to avoid this, use a change of variable in

$\cot z = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2-(\pi n)^2}$, $z \hookleftarrow \frac{2\pi}{i} z$.) Then

$$\begin{aligned} &= -\frac{1}{2}\frac{e^{2\pi i t}}{e^{2\pi i t}-1} \\ &= -\frac{1}{2}\sum_{t=0}^{\infty} B_{2m}\frac{(2\pi i t)^{2m}}{(2m)!} \end{aligned}$$

Equating coefficients gives

$$\zeta(2m) = \frac{(-1)^{m-1}(2\pi)^{2m}}{2(2m)!} B_{2m}.$$

The functional equation for ζ gives

$$\begin{aligned} \zeta(1-2m) &= \frac{\zeta(2m)}{2(2\pi)^{2m-1}}\sin(\pi m)\Gamma(2m) \\ &= \frac{(-1)^{m-1}B_{2m}(2\pi)^{2m}}{2(2m)!}\frac{(-1)^m(2m-1)!}{2(2\pi)^{2m-1}} \\ &= -\frac{\pi B_{2m}}{4m} \end{aligned}$$

□

Generalize, see washington p. 32.

1.2 Class field theory

Questions to resolve:

1. CFT being 1-D Langlands—this is sketchy in the notes.
2. Quartic reciprocity—handwaviness in the notes. Need a way to compute.

1.2.1 Problems

Answer to `http://math.stackexchange.com/questions/596195/conceptual-reason-why` `rq=1&newreg=e50d498e05254595aefbb31cf28d435f`

I'll refer to my notes for some precise statements and definitions: http://web.mit.edu/ holden1/www/ma

Define I_K^S to be the group of ideals in K generated by prime ideals not in S (or not dividing primes in S). Define $P_K(1,\mathfrak{m})$ to be the group of principal ideals that are "1 modulo $\mathfrak{m}$." (10.3)

By class field theory (10.4.1), if L/K is abelian, $\mathfrak{m}$ is a modulus containing the set of primes of K ramifying in L, and S the set of primes dividing $\mathfrak{m}$, there is an isomorphism $\psi_{L/K} : I_K^S/(P_K(1,\mathfrak{m}) \cdot \mathrm{Nm}_{L/K}(I_L^S)) \xrightarrow{\cong} G(L/K)$, and this is compatible with field extension M/L to form a commutative square, the right side of the square being the natural projection $G(M/K) \to G(L/K)$.

The case of $\mathbb{Q}$:

The above may seem complicated, but it's much easier to understand in the case of $\mathbb{Q}$, because Kronecker-Weber encapsulates much of the statement above.

Every abelian extension $L/\mathbb{Q}$ corresponds to (N,m) where $N \subseteq (\mathbb{Z}/m)^\times$ satisfies $(\mathbb{Z}/m)^\times/N \cong G(L/\mathbb{Q})$. Indeed, $I_{\mathbb{Q}}^S/P_{\mathbb{Q}}(1,m\infty) = (\mathbb{Z}/m)^\times$, and the norm group $\mathrm{Nm}_{L/\mathbb{Q}}(I_L^S)$ can be thought of as a subgroup of $(\mathbb{Z}/m)^\times$. We can all make this very explicit if we want (and avoid CFT): $L = \mathbb{Q}(\sum_{j\in N}\zeta_m^j)$, and the isomorphism is given by $j \mapsto (\zeta_m \mapsto \zeta_m^j)$. From this it is clear, for example, that $-1 \in N$ iff L is real.

Note that if $m \mid m'$ and N' projects to N, then (N,m) and (N',m') correspond to the same extension. For quadratic L, the smallest m we can take is the discriminant. (It is the same as the smallest m such that $L \subseteq \mathbb{Q}(\zeta_m)$.)

The Problem

Let $L/\mathbb{Q}$ be quadratic. The following are equivalent.

(1) $L/\mathbb{Q}$ occurs inside a $\mathbb{Z}/4$ field.

(2) There is (N,m) corresponding to L and $N_1 \subseteq N$ such that $(\mathbb{Z}/m)^\times/N_1 \cong \mathbb{Z}/4$.

(3) L is real and the discriminant of L is divisible only by primes $p \equiv 1,2 \pmod 4$.

(4) $-1 \in \mathrm{Nm}_{L/\mathbb{Q}}(L)$.

(1) $\iff$ (2) follows from the preceding discussion.

(3) $\implies$ (2): The argument is elementary but the group theory is messy. Choose m such that $8 \mid m$ and the discriminant d divides m, and write $m = \prod_i p_i^{e_i}$. Let $h_i : G_i \to \mathbb{Z}/2$ be the unique nontrivial map. Let $h_i : G_i \to \mathbb{Z}/2$ be a nontrivial map (the only place we have to be careful is $p_i = 2$, here use the map $G_i \cong \mathbb{Z}/2 \oplus (\mathbb{Z}/2)^{e_i-2} \to (\mathbb{Z}/2)^{e_i-2} \to \mathbb{Z}/2$). One can check $N = \ker \sum h_i$ corresponds to the unique real quadratic extension with discriminant d. Because all $p_i \equiv 1,2 \pmod 4$, there exist surjective maps $h_i' : G_i \to \mathbb{Z}/4$ and we can let $N_1 = \ker \sum h_i'$. This shows (2).

(3) $\implies$ (2): Suppose by way of contradiction N_1 works. Write $m = \prod_i p_i^{e_i}$ and keep the notation from above.

First suppose L is not real. Then $-1 \notin N$. But then -1 would have order 4 in G/N_1, contradiction.

Suppose k is such that $p_k \neq 4k+1, 2$. Now $G_k/G_k \cap N \cong \mathbb{Z}/2$ (as opposed to $\{1\}$) because otherwise $(N', m/p_k)$ would also represent m, where N' is the projection of N to $\prod_{i\neq k} G_i$. Now consider $g \in \prod G_i$ such that $g_i = 1$ for each $i \neq k$ and g_k is a generator of G_k. Then $g \notin G_k \cap N$ so $g \notin N$. This means g has order 4 in G/N_1. But $\mathbb{Z}/4$ is not a quotient of G_k, contradiction.

For (3) $\iff$ (4), note $x^2 - my^2$ is solvable over every $\mathbb{Q}_p$ iff m is only divisible by 2 and $4k+1$ primes. Then use the Hasse norm theorem: for cyclic L/K, an element is a global norm iff it is a local norm over every place.

The moral reason why you can detect the possibility of a $\mathbb{Z}/4$ extension with norms is the correspondence between norm groups and abelian extensions; however, (4) is not immediate from (2) because of the technicality with norms of elements vs. norms of ideals. We've already remarked $-1 \in N$ iff N is real, so whether $-1 \in N$ only measures part of the failure to be part of a $\mathbb{Z}/4$-extension.

Possibly there's something more elementary you can do with quadratic forms.

@Ben: $\frac{g(\beta)}{\beta}$ reminds me of cohomology, although I don't know if that has anything to do with it.

2 Analytic number theory

Zeta function, 15 Feb.

[Iwaniec and Kowalski p. 197: By the approximation for zeta, the problem reduces to estimating sums $\sum_{1\leq n\leq N} n^{-it}$.]

In the proof of Prop. 8.1, we lost a bit when replacing sums over primes by sums over integers, because primes are a sparse set. But we didn't lose too much, because they aren't too sparse. Since the primes are of density $\frac{1}{\ln n}$, we lose by log factors.

For the sums $U(n)$ from Lemma 7.1, we are summing over vectors $(x, x^2, x^3, \dots, x^r)$, $(y, y^2, \dots, y^r)$, and these are a very sparse subset of the box that contains them. This is a 1-dimensional object in a r-dimensional space. We need another idea besides the bilinear structure.

To overcome this, we will need another idea (in addition to the bilinear structure).

Lemma 9.2.1 (Duplication of variables)**:** lem:zeta8-3 Let

$$U(n) = \sum_{x\leq N^{\frac{2}{5}}} \sum_{y\leq N^{\frac{2}{5}}} e(\alpha_1 xy + \alpha_2 x^2y^2 + \cdots + \alpha_r x^r y^r)$$

be as in Lemma 7.1. Then for any natural number k, we have

$$|U(n)| \leq N^{\frac{4}{5}} \left(\frac{1}{N^{\frac{8k}{5}}} (J_{k,r}(N^{\frac{2}{5}}))^2 \prod_{j=1}^{r} \sum_{-kN^{\frac{2j}{5}} \leq \mu_j \leq kN^{\frac{2j}{5}}} \min(3kN^{\frac{2j}{5}}, \frac{1}{\|\alpha_j \mu_j\|}) \right)^{\frac{1}{4k^2}} .$$

where $J_{k,r}(N^{\frac{2}{5}})$ is the number of solutions $(x_1, \dots, x_{2k})$ of the simultaneous equations

$$\sum_{i=1}^{k} x_i^j = \sum_{i=k+1}^{2k} x_i^j \text{ for all } 1 \leq j \leq r$$

with $1 \leq x_i \leq N^{\frac{2}{5}}$ integers.

The $\|\cdot\|$ is what you get from summing geometric progressions.

Proof of Lemma 9.2.1. The proof is like the proof of the Toy Proposition, but with the application of Cauchy-Schwarz replaced by two applications of Hölder's inequality (with exponent $2k$). This has the effect of producing $2k$ duplicate copies of the summands $(x, \dots, x^r)$, $(y, \dots, y^r)$ whose sums cover the containing box more uniformly.

If we raise things to a big power, we get lots of copies rather than 2 copies. We hope the differences smooth out and cover the box.

To simplify the writing, set $Z = N^{\frac{2}{5}}$. By Hölder,

$$\begin{aligned} |U(n)|^{2k} &\leq Z^{2k-1} \sum_{x\leq Z} \left| \sum_{y\leq Z} e(\alpha_1 xy + \cdots + \alpha_r x^r y^r) \right|^{2k} \\ &= Z^{2k-1} \sum_{x\leq Z} \sum_{y_1,\dots,y_{2k}\leq Z} e\left(\alpha_1 x \left(\sum_{i=1}^{k} y_i - \sum_{i=k+1}^{2k} y_i \right) + \cdots + \alpha_r x^r \left(\sum_{i=1}^{k} y_i^r - \sum_{i=k+1}^{2k} y_i^r \right) \right) . \end{aligned}$$

So if we let $J_{k,r}(\lambda_1, \ldots, \lambda_r, Z)$ denote the number of solutions $(x_1, \ldots, x_{2k})$ of $\sum_{i=1}^{k} x_i^j = \sum_{i=k+1}^{2k} x_i^j + \lambda_j$ for all $1 \leq j \leq r$, then (we rewrote the sum as the sum over possible choices of λ's. The bounds are how big/small λ could possibly be.)

$$\begin{aligned} |U(n)|^{2k} &\leq Z^{2k-1} \sum_{x \leq Z} \sum_{-kZ \leq \lambda_1 \leq kZ} \cdots \sum_{-k2^r \leq \lambda_r \leq kZ^r} J_{k,r}(\lambda_1, \ldots, \lambda_r, Z) e(\alpha_1 x \lambda_1 + \cdots + \alpha_r x^r \lambda_r) \\ &\leq Z^{2k-1} \sum_{-kZ \leq \lambda_1 \leq kZ} \cdots \sum_{-kZ^r \leq \lambda_r \leq kZ^r} J_{k,r}(\lambda_1, \ldots, \lambda_r) \left| \sum_{x \leq Z} e(\alpha_1 x \lambda_1 + \cdots + \alpha_r x^r \lambda_r) \right| . \end{aligned}$$

To simplify the writing further, we will usually just write $\sum_{\lambda_j}$ (without a range) to mean $\sum_{-kZ^j \leq \lambda_j \leq kZ^j}$.

In the proof of the Toy Proposition, we were now basically done because we could evaluate the inner sum. Here we cannot do this, so we apply Hölder's inequality again:

$$\begin{aligned} |U(n)|^{(2k)^2} &\leq Z^{2k(2k-1)} \left(\sum_{\lambda_1} \cdots \sum_{\lambda_r} J_{k,r}(\lambda_1, \ldots, \lambda_r, Z) \sum_{x \leq Z} e(\alpha_1 x \lambda_1 + \cdots + \alpha_r x^r \lambda_r) \right)^{2k} \\ &\overset{H}{\leq} Z^{2k(2k-1)} \left(\sum_{\lambda_1} \cdots \sum_{\lambda_r} J_{k,r}(\lambda_1, \ldots, \lambda_r, Z)^{\frac{2k}{2k-1}} \right)^{2k-1} \cdot \sum_{\lambda_1} \cdots \sum_{\lambda_r} \left| \sum_{x \leq Z} e(\alpha_1 x \lambda_1 + \cdots + \alpha_r x^r \lambda_r) \right|^{2k} . \end{aligned}$$

To bound the first bracketed term, note that

$$\begin{aligned} \sum_{\lambda_1} \cdots \sum_{\lambda_r} J_{k,r}(\lambda_1, \ldots, \lambda_r)^{\frac{2k}{2k-1}} &\leq \max_{(\lambda_1, \ldots, \lambda_r)} J_{k,r}(\lambda_1, \ldots, \lambda_r, Z)^{\frac{1}{2k-1}} \cdot \sum_{\lambda_1} \cdots \sum_{\lambda_r} J_{k_r}(\lambda_1, \ldots, \lambda_r, Z) \\ &\leq Z^{2k} \max_{(\lambda_1, \ldots, \lambda_r)} J_{k,r}(\lambda_1, \ldots, \lambda_r)^{\frac{1}{2k-1}} \end{aligned}$$

since $\sum_{\lambda_1} \cdots \sum_{\lambda_r} J_{k,r}(\lambda_1, \ldots, \lambda_r, Z)$ counts all vectors $(x_1, \ldots, x_{2k})$ with $1 \leq x_i \leq Z$ integers. Also for any $(\lambda_1, \ldots, \lambda_r)$ we have

$$\begin{aligned} J_{k,r}(\lambda_1, \ldots, \lambda_r, Z) &= \sum_{L_1, \ldots, L_r \in \mathbb{Z}} (\# \left\{ (x_1, \ldots, x_k) : 1 \leq x_i \leq Z, \sum_{i=1}^{k} x_i^j = L, \forall 1 \leq j \leq r \right\} \\ &\qquad \cdot \left\{ (x_{k+1}, \ldots, x_{2k}) : 1 \leq x_i \leq Z, \sum_{i=k+1}^{2k} x_i^j = L_j - \lambda_j \forall j \right\} \\ &\overset{\text{CS}}{\leq} \sum_{L_1, \ldots, L_r \in \mathbb{Z}} \# \left\{ (x_1, \ldots, x_k) : 1 \leq x_i \leq Z, \sum_{i=1}^{k} x_i^j = L_j \forall 1 \leq j \leq r \right\}^2 \\ &= J_{k,r}(0, \ldots, 0, Z) =: J_{k,r}(Z). \end{aligned}$$

(Choose the $x_1, \ldots, x_k$ however you like, and the rest of the variables to make the sum correct.) Therefore we have

$$|U(n)|^{(2k)^2} \leq Z^{4k(2k-1)} J_{k,r}(Z) \sum_{\lambda_1} \cdots \sum_{\lambda_r} \left| \sum_{x \leq Z} e(\alpha_1 x \lambda_1 + \cdots + \alpha_r x^r \lambda_r) \right|^2 .$$

□

We can't use the structure very efficiently, have polynomial of low degree. We need to do something to smear out the points, so we can apply Hölder and replace the sums with smooth sums. We can swap the sums over and over again. If k is big enough, we'll get better than the trivial bound. (The bound is at worst trivial.) If k is too small there will be few solutions; if k is large, the tuples will be approximately uniformly distributed, so we've done something.

3 Elliptic curves

sec:ec

My writings:

1. [R:4] Notes on CM http://web.mit.edu/~holden1/www/math/ant.pdf
2. [R:3] Notes from Cambridge course: https://dl.dropboxusercontent.com/u/27883775/math%20notes/part_iii_elliptic.pdf
3. [R:2] Notes I'm in the middle of compiling. https://dl.dropboxusercontent.com/u/27883775/math%20notes/elliptic.pdf

Where I learned about elliptic curves.

- 18.783, (computational emphasis) http://co.mit.edu/18.783
- Elliptic curves at Cambridge, following Silverman.
- CM, following Silverman (see ANT notes).
- Diophantine approximation from Diophantine Geometry, Hindry and Silverman. (Did a talk on this for STAGE.)

3.1 Questions

Unsolved

1. Motivation for Weil pairing

Solved

1. Silverman p. 92: What's example of $M \subseteq \text{Hom}(E_1, E_2)$ not finitely generate? Ans: subgroups of matrices may not be f.g...

11-17-13

3.2 EC

[R:2] Summary of Silverman VII. See index card. [Added to elliptic text]

1.

2.

3.

4. Define unramified for $G(\overline{K}/K)$-sets by saying that the action is entirely captured by $G(K^{\mathrm{ur}}/K)$, i.e, I_v acts trivially. $E[m], T_\ell(E)$ are unramified for $m, \ell \perp \operatorname{char}(k)$ because of injectivity $E[m] \hookrightarrow \widetilde{E}(k')$, which means it suffices to look at the action on l/k, i.e. $G(K^{\mathrm{ur}}/K) \cong G(k^s/k)$.

5. Define good, multiplicative (split/nonsplit), additive reduction. 5.4

   (a) Cannot improve from unramified extension (any change of coordinates over an unramified extension can be done over the base field, up to a unit, since the u' doesn't have fractional valuation).

   (b) Good/multiplicative reduction preserved: we'll still have $v(\Delta), v(c_4) = / \neq 0$ in extension.

   (c) Can improve from additive reduction: intuition—$v(c_4) > 0$—by extending valuation can make CoC so that $v(c_4) = 0$. Use Legendre form.

   (d) Good reduction iff j-invariant integral: if good reduction, then $\Delta \in (R')^\times$, need to show in R. But $j = \frac{c_4'}{\Delta'}$, and by good reduction Δ' is in $R'^\times$. If j-invariant integral—note that j-invariant is most closely linked to the Legendre form, so we look at that—λ must be integral, and not "almost" a repeated root, so Δ (think of it as the discriminant of the polynomial!) is good.

6. With NOS, we have a strong link between good reduction and non-ramification, in the sense that a weak result about non-ramification of torsion points (just $E[m]$ unramified at v for infinitely many integers $\perp \operatorname{char}(k)$) implies good reduction.

   Pf. Choose m super-large and relatively prime. The key is that m is more than $E/E_0(K^{\mathrm{nr}})$—because then E_1 can't capture everything and this forces the existence of $(\mathbb{Z}/\ell\mathbb{Z})^2$ in the reduction part, which cannot happen for mult/add reduction.

   7.2 Isogenous $\implies$ both have good reduction, or bad reduction. Look at m-torsion!

   7.3 Pot good reduction iff I_v acts on $T_\ell(E)$ through finite quotient for some/all primes $\ell \neq \operatorname{char}(k)$. Forward direction easy—just extend field until good reduction. Backwards direction: look at fixed field, can find finite subfield giving good reduction (use giving compositum).

Q's

1. In what ways do CM elliptic curves help? i.e., the endomorphism ring should be a crutch for proofs, in what way?

2. What is true in $\mathbb{Q}_p$ that is not true over general local fields ($k((T))$), that we take for granted?

3. Mumford-Fogarty GIT: definition of stable, etc. in moduli space.

4. For abelian varieties, can it reduce to anything of smaller dimension?

Interesting: `http://en.wikipedia.org/wiki/Galois_connection`

3.3 Descent by cyclic isogeny

(moved to elliptic.tex)

Idea: it "tells us what residue classes of $E(K)$ to look for independent generators."
TODO: add Silverman's stuff. Algorithm for computing.
Thread: what do we learn about congruent numbers?
12-23 Glancing through Washington.

1. How is the notion of descent in terms of cohomology (see CFT notes) related to the notion of descent in the Fermat sense? A nice elementary way to see what we're doing is "descent" is write $y^2 = \prod(x - e_i)$ and let $x - e_i = a_i u_i^2$, we expect the u_i to have smaller height. This is an intuitive way to see what the descent thing is actually doing, in an elementary way. (In general, is the cohomology hiding some change of coordinates?) I don't know if the elementary proof is enlightening though—that the kernel is $2E$ is not obvious (i.e. anything in the kernel can be halved).

   Descent as getting simpler (in terms of smaller height) numbers.

2. The variety you get out is isomorphic to the original elliptic curve over K if it has a K-rational point. What's an easy way to see this?

3.4 Revision notes

3.5 PSet 2

[R:1] 11-9-13 (2:30-3:48)

1. SAGE:

   ```
   E=EllipticCurve(GF(13),[1,5])
   E.abelian_group()
   E.points()
   ```

   gives

   ```
   Additive abelian group isomorphic to Z/9 embedded in Abelian group of
   points on Elliptic Curve defined by y^2 = x^3 + x + 5 over Finite Field
   of size 13
   [(0 : 1 : 0), (3 : 3 : 1), (3 : 10 : 1), (7 : 2 : 1), (7 : 11 : 1), (10 : 1
   ```

   $y^2 = x^3 + 1$ is not cyclic:

```
E2=EllipticCurve(GF(13),[0,1])
E2.abelian_group()
Additive abelian group isomorphic to Z/2 + Z/6 embedded in Abelian group
of points on Elliptic Curve defined by y^2 = x^3 + 1 over Finite Field
of size 13
```

Easier to find is $y^2 = x(x-1)(x+1)$: it has 3 points of order 2 so is not cyclic.

All groups require at most 2 generators, because the p-torsion part has rank at most 2 for each p.

2. $\omega = \frac{dx}{x}$. $[n]^*\omega = \frac{d(x^n)}{x^n} = \frac{n\,dx}{x} = n\omega$.

3. Linearity: induction on n shows $q(n^2x) = n^2q(x)$.

   Bilinearity: Let $b(x,y) = q(x+y) - q(x) - q(y)$. Then $b(x_1+x_2,y) = b(x_1,y)+b(x_2,y)$ is equivalent to

   $$q(x_1+x_2+y) - q(x_1+x_2) - q(x_1+y) - q(x_2+y) + q(x_1) + q(x_2) + q(y) = 0.$$

   We need to show the following is bilinear:

   $$\begin{aligned} b(x+y) &:= 2(q(x+y) - q(x) - q(y)) \\ &= q(x+y) - q(x-y). \end{aligned}$$

   We have

   $$\begin{aligned} b(x+z,y) &= q(x+y+z) - q(x+z-y) \\ &= \frac{1}{2}\left[2q(x+y) + \cancel{2q(z)} - \cancel{q(x+y+z)} + 2q(z+y) + \cancel{2q(x)} - \cancel{q(z+y-x)}\right] \\ &\quad - \frac{1}{2}\left[2q(x-y) + \cancel{2q(z)} - \cancel{q(x-y-z)} + 2q(x-y) + \cancel{2q(x)} - \cancel{q(z-x-y)}\right] \\ &= (q(x+y) - q(x-y)) + (q(z+y) - q(z-y)). \end{aligned}$$

   Looks like an annoying functional equation.

4. Frobenius is a homomorphism on the algebra of rational functions over $\mathbb{F}_q$, so $\psi \circ \phi_1 = \phi_2 \circ \psi$. Now

   $$\deg(\psi)\deg(1-\phi_1) = \deg(\psi - \psi\circ\phi_1) = \deg(\psi - \phi_2\circ\psi) = \deg(\psi)\deg(1-\phi_2),$$

   so

   $$|E_i(\mathbb{F}_q)| = |\ker(1-\phi_i)| = \deg(1-\phi_i)$$

   are equal.

5. Suppose $|E(\mathbb{F}_p)| = 1+p-a$, where $a = \mathrm{tr}(\phi)$, ϕ the Frobenius map. Then we can find $|E(\mathbb{F}_p)|$ in 2 ways.

(a) Use 6(i): We have $|E(\mathbb{F}_{p^2})| = \det(I - A^2) = (1-\lambda_1)(1-\lambda_2)$ where λ_1, λ_2 are the solutions to $\lambda^2 - a\lambda + p$.

(b) Use 6(iii): Use the recurrence $\mathrm{tr}(1-\phi^n) = 2 - a\mathrm{tr}(\phi^{n-1}) + p\mathrm{tr}(\phi^{n-2})$. Here, we get $\mathrm{tr}(1-\phi^2) = 2 - a^2 + 2p$, so $|E(\mathbb{F}_{p^2})| = 1 - (2 - a^2 + 2p) + p^2 = p^2 - 2p - 1 + a^2$.

(These are really doing the same thing.) Putting in $p = 13$ and $a = 5$ gives $|E(\mathbb{F}_{13^2})| = \boxed{171}$. This is cyclic as $\mathbb{Z}/9$ imbeds into it, and $9 \perp 19$.

Alternatively, letting E' be the quadratic twist $y^2 = x^3 - 4x + 1$, $|E'(\mathbb{F}_{13})| = 2 \cdot 13 - 8 + 1 = 19$, so the answer is $9 \cdot 19$. do we need relative primality here?

Alternatively, by the parallelogram law, $\deg(1-\phi) + \deg(1+\phi) = 2\deg(\phi) + 2$, $|E(\mathbb{F}_{13^2})| = \deg(1-\phi)\deg(1+\phi) = 9 \cdot 19$.

In general, $\deg(1+\phi)$ is the number of points on the quadratic twiset. Note ψ commuted with ϕ. The twists are isomorphic over $\mathbb{F}_{13^2}$ so they don't commute with the Frobenius maps, they commute up to sign.

6. Follows from the fact deg is a quadratic form.

   (a) Follows from deg being a quadratic form. (Use bilinearity.)

   (b) Calculate $\deg(\phi^2 - 1)$ in two ways.

$$\deg(\phi+1)\deg(\phi-1) = (1 + \mathrm{tr}(\phi) + \deg(\phi))(1 - \mathrm{tr}(\phi) + \deg(\phi)) = 1 - \mathrm{tr}(\phi)^2 + 2\mathrm{tr}(\phi)\deg(\phi) -$$
$$\deg(\phi^2 - 1) = 1 + \mathrm{tr}(\phi^2) + \underbrace{\deg(\phi^2)}_{\deg(\phi)^2}.$$

   (c) We have

$$\begin{aligned}\deg(\phi^2 - [\mathrm{tr}(\phi)]\phi + [\deg\phi]) &= \deg(\phi^2) + \deg(\phi)\mathrm{tr}(\phi^2 - [\mathrm{tr}(\phi)]\phi) + \deg(\phi^2 - [\mathrm{tr}(\phi)]\phi) \\ &= \deg(\phi)^2 + \deg(\phi)(\mathrm{tr}(\phi)^2 - 2\deg(\phi) - \mathrm{tr}(\phi)^2) + (\deg(\phi))(\mathrm{tr}(\phi)^2 - \\ &= 0.\end{aligned}$$

   (This seems rather unenlightening.) (Does this work over finite fields?) Consider the action on $E[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m$ (take field extension if necessary, so m is large). It's a matrix. Matrix satisfies same equation, hence $\mathrm{tr}(\phi) = \mathrm{tr}(A), \deg(\phi) = \deg(A)$. A satisfies own characteristic polynomial. So ϕ does too. (Using fact that ϕ can't send infinitely many things to 0.)

7. (a) Let A be the matrix with eigenvalues satisfying $\lambda^2 - a\lambda + p = 0$. Then by 6(3), $\#E(\mathbb{F}_{p^n}) = \det(I - A^n)$.

   (b) We have by 6(3) $[a]\phi - \phi^2 = [\deg(\phi)] = [p]$. If $p \nmid a$ then $[a]$ is separable (look at its degree), so $[a] - \phi$ is separable. The equation shows $[p]$ is not separable (ϕ is inseparable), so if $p \mid a$ (e.g. $a = 0$), then ψ is inseparable. ω is separable iff $\psi^*\omega \neq 0$. We have $\psi^*\omega = a\omega - \overset{\phi^*\omega}{\cancel{0}} \neq 0$ iff $p \nmid a$.

   If E is supersingular $E(\overline{F}_p)[p] = 0$, then $\deg_i[p] = p^2$, and $[a] - \phi$ must be inseparable, i.e. $p \mid a$. But $|a| \le 2\sqrt{p} < p$ when $p \geq 5$ so $a = 0$.

The reverse direction: $\phi\psi = [p]$ so $\ker(\psi) \subseteq E[p]$. In the supersingular case $E[p] = 0$ so $\ker(\psi) = 0$, so $\deg\psi = p$.

8. This is just like existence of inverse of power series. Write $F(X,Y) = X + Y + \sum_{i,j\ge 1} a_{ij}X^iY^j$, we want
$$-T = (1 + \sum_{j=1}^{\infty} a_{1j}T^j)Y + (\sum_{j=1}^{\infty} a_{2j}T^j)Y^2 + \cdots$$
Find the coefficients inductively. The Y term on the RHS is key, it makes the equation for a_k equal to a_k+(lower order terms)$= 0$.

   Cute: "Hensel's lemma" with power series instead.

9. Differentiate $f(g(T)) = T$ n times and set $T = 0$. For $n = 1$, we get $a_1b_1 = 1$. For $n \ge 2$, we get by induction (using the chain and product rules)
$$f'(g(T))g^{(n)}(T) - P((f^{(i)}(g(T)), g^{(j)}(T) : 1 \le i \le n, 1 \le j \le n-1))$$
for P a polynomial with integer coefficients. This expresses a_1b_n as a polynomial in the $a_1, \dots, a_n, b_1, \dots, b_n$. Thus $b_n \in R$.

10. (i) The polynomial $3X^4 + 12dX$ captures the 3-torsion points, $T \in E[3]$. We have
$$x(P+T) = \left(\frac{y-\sqrt{d}}{x}\right)^2 - x$$
$$x(P-T) = \left(\frac{y+\sqrt{d}}{x}\right)^2 + x.$$
(ii)
$$\eta^2 = \frac{y^2(x^3-8d)^2}{x^6} = \frac{(x^3+d)(x^3-8d)^2}{x^6} = \xi^3 - 27d = D.$$
(iii)
$$\phi^*\left(\frac{dx}{y}\right) = \frac{d\phi^*(x)}{\phi^*(y)} = \frac{d\xi}{\eta} = \frac{dx}{y}.$$
What did we learn? Suppose we're looking for an isogeny with kernel $\{O, T, 2T\}$. We see where the formula came from: add together the x coordinates (we're trying to quotient out by the group generated by T). The formula for η is suggested by the last calculation, it is the derivative of ξ. Follow-up exercise: $y^2 = x^3 + (ax+b)^2$. $T = (0, b)$. Same idea but messier: add up the x-coordinates, etc.

Take 2 elliptic curves isogenous over $\mathbb{Q}$. If one curve has a point of order 5, it looks like the other one has too, so the method of reducing mod all p doesn't always work.

11-10-13 (8–8:30) Wrote up section 4.7 in Silverman. See EC notes.

(meeting 2–3+) Remaining questions. What happens when $v(\Delta) \ge 12$? Can we see a formal group as a functor?

11-16-13

1. How to realize $\mathbb{Q}(\sqrt[n]{a})$ as in a cyclotomic extension?

3.6 PSet 3

[R:1] http://www.sagenb.org/home/holdenlee/10/

1. Note that the primes of bad reduction are contained in the prime factors of Δ, but the containment may be strict since the Weierstrass equation may not be minimal for that prime. The primes dividing Δ with valuation not divisible by 12 certainly are primes of bad reduction. Warning: Just because the discriminant is divisible by 12 doesn't mean you could remove it. Calculating the discriminants,

   (a) $-1 \cdot 3^{12} \cdot 11$ so $\boxed{11}$. Substituting $x \hookleftarrow 3^2 x$, $y \hookleftarrow 3^3 y$ (and dividing through by 3^6) gives $y^2 + y = x^3 - x^2$ which has discriminant -11 and has good reduction at 3.

   (b) $2^8 \cdot 5^2$ so $\boxed{2, 5}$.

   (c) $-16(4a^3 + 27b^2) = -16 \cdot 27 \cdot 16^3 = -2^{12} \cdot 3^3$ so $\boxed{3}$. For 2, make the substitution $y \hookleftarrow y + 4$ to get $(y+4)^2 = x^3 + 16$ or $y^2 + 8y = x^3$, getting $y^2 + y = x^3$.?

2. (a) $y^2 + xy = x^3 - 2x + 1$.

   Solve $(3x^2 - 2 - y, -2y - x) = 0$ gives by substituing $12y^2 - y - 2 = 0$ gives $y = \frac{1 \pm \sqrt{1+96}}{24} = 13$ or 43, $x = 35$ or 36. Which one? Plug back in. $\boxed{(43, 36)}$

   Alternative calculation: rewrite as $(2y+x)^2 = 4x^3 + x^2 - 8x + 4 =: f(x)$. We have $\gcd(f(x), f'(x)) = x - 36$ in $\mathbb{F}_{61}[x]$. This immediately gives the singular point $(x, y) = (36, 43)$.

   (b)
```
for p in [2,3,5,7]:
    E=EllipticCurve(GF(p),[1,0,0,-2,1])
    print E.cardinality()
    print E.abelian_group()
```

```
4
Additive abelian group isomorphic to Z/4 embedded in Abelian group of
points on Elliptic Curve defined by y^2 + x*y = x^3 + 1 over Finite
Field of size 2
6
Additive abelian group isomorphic to Z/6 embedded in Abelian group of
points on Elliptic Curve defined by y^2 + x*y = x^3 + x + 1 over Finite
Field of size 3
9
Additive abelian group isomorphic to Z/9 embedded in Abelian group of
points on Elliptic Curve defined by y^2 + x*y = x^3 + 3*x + 1 over
Finite Field of size 5
7
Additive abelian group isomorphic to Z/7 embedded in Abelian group of
points on Elliptic Curve defined by y^2 + x*y = x^3 + 5*x + 1 over
Finite Field of size 7
```

p	2	3	5	7
$\#\widetilde{E}(\mathbb{F}_p)$	4	6	9	7

(c) We have $\#E(\mathbb{Q})_{\text{tors}} \mid 4\cdot 2^a, 9\cdot 5^b$ for some $a,b\geq 0$, so $E(\mathbb{Q})_{\text{tors}}=\{0\}$.

(d) Consider

$$(\mathbb{Z}_2,+)\cong E_2(\mathbb{Q}_2) \underbrace{\subseteq}_{(\mathbb{F}_2,+)} E_1(\mathbb{Q}_2) \underbrace{\subseteq}_{\#\widetilde{E}(\mathbb{F}_2)=4} = E(\mathbb{Q}_2)$$

We have the last equality because 2 is a prime of good reduction. We have $E(\mathbb{Q}_2)_{\text{tors}} \hookrightarrow \frac{E(\mathbb{Q}_2)}{E_2(\mathbb{Q}_2)}$ which has order 8.

(e) Since $E_1(\mathbb{Q}_7)\subseteq E(\mathbb{Q}_7)$ has index 7, $7P\in E_1(\mathbb{Q}_7)$. So $7P$ does not have integral coordinates.

Also $E_1(\mathbb{Q}_5)\subseteq E(\mathbb{Q}_5)$ has index 9 so $9P\in E_1(\mathbb{Q}_5)$.

3. Check over finite fields of order < 20.

```
def grp(E):
    #E elliptic curve
    #really annoying that E.abelian_group().elementary_divisors() doesn’t wo
    l=[]
    for P in E.gens():
        l.append(P.order())
    return l

def torsion_grp(elist,ub):
    #elist is elliptic curve coefficients
    #ub is upper bound
    #group’s elementary divisors will divide l_1, l_2
    l=[lcm(range(1,13)),2]
    for p in primes(ub): #up to ub
        try:
            F=GF(p)
            E=EllipticCurve(F,elist)
            #http://www.sagemath.org/doc/reference/groups/sage/groups/abelia
            l2=grp(E)#.elementary_divisors()
            if len(l2)==1:
                l2.append(1)
            for (i,m) in enumerate(l):
                print l2[i],m
                l[i]=gcd(l2[i],m)
            print (p,l2)
            if l2==[1,1]:
                return [1,1]
        except ArithmeticError:
            print p,"␣:␣bad␣reduction"
    return l

for elist in [(0,1,1,-2,0),(1,0,1,0,0),(-1,-4,-4,0,0),(0,5,0,4,0)]:
    print elist
    print "Group:␣",torsion_grp(elist,20)
    g= EllipticCurve(elist).torsion_subgroup()#over Q
    print "Actual:␣",g
    print g.gens()
```

p	2	3	5	7	11	Δ
(i)	5	6	9	13		389
(ii)	-	3	9	9	6	-20
(iii)	-	7	7			$-2^7 \cdot 13$
(iv)	-	-	8	8		$2^8 \cdot 3^2$

We get

(a) $\mathbb{Z}/1$

(b) $\mathbb{Z}/3$ with generator $(0, 0)$

(c) $\mathbb{Z}/7$ with generator $(0, 0)$

(d) $\mathbb{Z}/4 \times \mathbb{Z}/2$ with generators $(-1, 0)$ and $(2, 6)$.

I cheated at the end in finding generators. To do this without cheating, keep a list of the generators at each step, CRT them, throw out the large ones?

4. Initial idea: We want $\widetilde{E}(\mathbb{F}_p) = 6k$ for infinitely many p where k is a linear function of p.

Difficulty: In $y^2 = x^3 - D^2x$, we had *cancellation* because the RHS is *odd*, but we don't have that anymore. What to do?

Solution: Choose sufficiently large p, $6 \mid p+1$, so $3 \nmid p-1$, and (key observation) $\mathbb{F}_p \to \mathbb{F}_p : x \mapsto x^3$ is injective. So for every y there is exactly 1 solution for x. We get $|\widetilde{E}(\mathbb{F}_p)| = p+1$. By Dirichlet, $\widetilde{E}(\mathbb{Q})_{\text{tors}} \mid 6$.

Alternate solution: See p. 140, V.4.1 in Silverman, we use $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$. We get the number of points is

$$p + 1 + \sum_x (x^3 + d)^{\frac{p-1}{2}} \bmod p.$$

Now choose $p \equiv 5 \pmod 6$. The sum looks intractable, but it's summed over $x \in \mathbb{F}_p$ and we know powers other than $p-1$th powers disappear. So the coefficient is $\binom{\frac{p-1}{2}}{\frac{p-1}{6}}$ unless of course $6 \nmid p-1$, which is our case. So it's $p+1$. (i.e. the curve is supersingular for $p \equiv 5 \pmod 6$. Now use Dirichlet.

🔑 Count solutions modulo p by taking powers $a^{\frac{p-1}{k}}$.

For (ii),

```
E=EllipticCurve([0,5])
P=E(-1,2)
print 2*P#gives (41/16 : -299/64 : 1)
```

Solution 1: Note $4x, 8y \notin \mathbb{Z}$, so $2P$ ia not torsion, and P is not torsion.

Solution 2: Note there is no rational 2-torsion because 5 is not the cube of a rational number. There is no 3-torsion either because $3 * P \neq O$.

Solution 3: Here's another trick. We have $(x,y) = (0, \sqrt{5}) \in E(\mathbb{R})[3]$. If all torsion points are real, then by the Weil pairing $\mu_3 \subseteq \mathbb{R}$, contradiction. (Or use $E(\mathbb{R}) = \mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.)

5. First, writing $y^2 = x^2(x + a + \frac{b}{x})$ gives that $x + a + \frac{b}{x}$ is a perfect square.

   $y^2 = x^3 + ax^2 + bx = f(x)$. If P is a 2-torsion point, just check it directly. We have $2P = (x_2, y_2) \in E(\mathbb{Q})_{\text{tors}} \cap \mathbb{Z}^2$.

$$x_2 = \left(\frac{f'(x)}{2y}\right)^2 - 2x - a$$

$$x \mid y^2 \mid f'(x)^2 = x ... + b^2.$$

   $a = v_p(x)$, $r = v_p(b)$, $r < a$. $2v_p(y) = v_p(x)v_p(x^2 + ax + b) = a + r$. $y \mid f'(x)$.

   Get $a = v_p(x) \leq r = v_p(b)$.

   Solution 2: Curve has $(0,0)$ which is torsion point, add, also torsion point so has integer coordinates.

   Solution 3: Consider the 2-isogeny (the isogeny with kernel size 2) $\phi : E \to E'$, $(x,y) \mapsto \left(\left(\frac{y}{x}\right)^2, \cdots\right)$. Since $\left(\frac{y}{x}\right)^2 = x + a + \frac{b}{x}$, we get $\frac{b}{x}$ is an integer.

6. I feel like there should be a nice methodical way to do this but I don't know how. I first wrote the equation for adding (messy). I tried the following all of which failed:

   (a) Guessing $x = \frac{t}{g(t)}, y = \frac{t}{(t-1)f(t)}$, and getting an equation in the polynomials f, g

   (b) Trying to use divisors—whoops, the space is infinite since it's affine

   (c) Getting functional equation from the fact that it preserves the group law.

   Looked at Silverman p. 62, which gives no motivation for its coordinate transformations.

   Idea: If we can get the elliptic curve equation to be $f(x,y) = 0$ such that $f(x, mx+b)$ has NO y, y^2 term, and a constant term -1, then by Vieta $x_1x_2x_3 = 1$.

   Step 1: let's try to make it symmetric by making the tangent lines to $(0,0)$ the axes. Let $x' = y + x, y' = y - x$. Then

$$8x'y' = (x' - y')^3$$

   Step 2: Homogenizing helps us look for way forward

$$8X'Y'Z' = (X' - Y')^3$$

Step 3: Now switch to the $Y \neq 0$ patch:

$$8x''z'' = (x''-1)^3.$$

We have

$$x'' = \frac{X'}{Y'} = \frac{y+x}{y-x}.$$

Given $t = \frac{y+x}{y-x}$, how to recover x, y? Solving

$$\begin{aligned} t &= \frac{y+x}{y-x} \\ y^2 &= x^2(x+1) \\ \implies x &= \frac{(1+t)^2}{(1-t)^2} - 1. \end{aligned}$$

Q: lines don't change under projective transformation? Q: is it easier to think $[x:y:z]$?

Solution 2: $x = t^2-1, y = t^3-t$, $1 \mapsto \infty$, $-1 \mapsto 0$, $\infty \mapsto 1$. Find the Möbius map $\frac{z+1}{z-1}$. Plugging in, $\phi(t) = \frac{4t}{z^2-2t+1}$, $\psi(t) = \frac{4t^2+4t}{t^3-3t^2+3t-1}$.

7. First we check the curve has bad reduction. Indeed, the discriminant is $\Delta = -432p^2 - p$, and $12 \nmid v_p(-432p^2-p) = 1$. (Check $p = 2, 3$ separately.)

   If $(0,0)$ lifted to (x,y), then $v_p(y^2+xy) \geq 2$ and $v_p(x^3+p) = 1$, contradiction

   Every point on E reduces to a nonsingular point on $\widetilde{E}$ so the Tamagawa number is 1.

   (This curve has split multiplicative reduction. Reducing modulo p, we get $y^2+xy = x^3$; the LHS factors over $\mathbb{F}_p$, $y(x+y)$, giving the tangent directions. The Tamagawa number is the valuation of the discriminant.)

   Take $y^2+xy = x^3+p^4$. There's a lift (p, p^2).

   (If we have good reduction, the Tamagawa number is 1, and the converse is not true. We can have bad reduction and still have the Tamagawa number 1.)

8. (a) We can choose our Weierstrass equation such that $v_p(\Delta) = 0$. Let $\mathfrak{p} \mid p$ in K. Then $v_{\mathfrak{p}}(\Delta) = 0$ as well. Hence E/K has good reduction at $\mathfrak{p}$.

   (b) Solution 1: $v(c_4) = 0$ is still true.

   Solution 2: Write $y^2 = x^3+ax+b$, $a, b \in \mathbb{Z}$. We have $p \mid \Delta = -16(27b^2+4a^3)$. If $p \mid a, b$ then we have additive reduction. Hence $p \nmid a$ or $p \nmid b$. In fact both are true. We have $p \mid \Delta$. This exactly characterizes: Weierstrass equation is minimal and we have multiplicative reduction.

   (c) We want $v_p(c_4)$ to go from not having 4 as a factor to having 4 as a factor, and $12 \mid v_p(\Delta)$. So consider $y^2 = x^3 - 25x$ where $v_5(c_4) = 2$ and consider over $\mathbb{Q}(\sqrt{5})$; $v_{\sqrt{5}}(c_4) = 4$. It is isomorphic here to the twist

   $$(y5\sqrt{5})^2 = (5x)^3 - (5x) \iff y^2 = x^3 - x$$

   which has good reduction.

   Any change of coordinates would still be possible in an unramified subfield.

3.7 PSet 4

[R:1]

1. The only not-clear part is $\alpha(T')$. We compute it by linearity. Let $(0,0)+(x_2,y_2)=P$. We have
$$x(P)=\left(\frac{y_2}{x_2}\right)^2-a-x_2=x_2+a+bx_2^{-1}-a-x_2$$
, so
$$\alpha((0,0))=\alpha(P)\alpha((x_2,y_2))^{-1}=\frac{bx_2^{-1}}{x_2}=b\in\mathbb{Q}^\times/\mathbb{Q}^{\times 2}.$$
What if there is no other point in $E(\mathbb{Q})$? Note the pairings are compatible under field extension:
$$\begin{aligned} E(K)/\phi E(K)\times G(\overline{K}/K)&\to E[\phi]\\ E(L)/\phi E(L)\times G(\overline{K}/L)&\to E[\phi]\end{aligned}$$
since we have the map behaves under restriction
$$\begin{tikzcd} H^1(K,E[\phi]) \arrow[r, equal] \arrow[d, "\text{Res}"] & E/\phi E(K) \arrow[d, equal, "\text{Res}"] \\ H^1(L,E[\phi]) \arrow[r, equal] & E/\phi E(L). \end{tikzcd}$$
and $G(\overline{K}/L)\hookrightarrow G(\overline{K}/K)$.

2. The following computes the rank by 2-descent. (See `http://sagenb.org/home/pub/5049`.)

```
def findsq(f,s):
    for sum in range(s+1):
        for v in range(sum+1):
            u=sum-v
            if (u,v)==(0,0):
                continue
            for i in [-1,1]:
                for j in [-1,1]:
                    ws=f(i*u,j*v)
                    w=sqrt(ws)
                    if ws>=0 and w==int(w):
                        print (i*u,j*v,w)
                        return True
    return False

def list_of_factors(n):
    l=prime_factors(n)
    return factorlist(l)
```

```
def prime_factors(n):
    l=list(factor(n))
    l=[a[0] for a in l]
    return l

def factorlist(l):
    if l==[]:
        return [-1,1]
    p=l[-1]
    #e=l[-1][1]
    ans=[]
    l2=factorlist(l[:-1])
    for e1 in range(2):#e+1
        ans.extend([p^e1*x for x in l2])
    return ans

def solve_over(a,b,b1,p):
    #tries to solve b1u^4+au^2v^2+(b/b1)v^4=w^2 with nonzero
    #only need to check p|2*b*(a^2-4*b)
    a1=b1
    a2=a
    a3=b/b1
    a0=1
    if a1%p==0 and a2%p==0 and a3%p==0:
        a1=a1/p
        a2=a2/p
        a3=a3/p
        a0=p
    if p==2:
        p=8
    for i in range(p):
        for j in range(p):
            if i!=0 and j!=0:
                if p!=8 and ((a0==1 and kronecker(a1*i^4+a2*i^2*j^2+a3*j^4,p
                    return True
                if p==8 and not (i%2==0 and j%2==0):
                    if a0==1 and (a1*i^4+a2*i^2*j^2+a3*j^4)%8 in [0,1]:
                        return True
                    if a0==2 and (a1*i^4+a2*i^2*j^2+a3*j^4)%8 in [0,2]:
                        return True
    return False #no nontrivial solution over Fp

def solve_p(a,b,b1):
    #only need to check p|2*b*(a^2-4*b)
    l=prime_factors(2*b*(a^2-4*b))
    for p in l:
        if not solve_over(a,b,b1,p):
            print "failed␣to␣solve␣over␣",p
            return False
    return True

def compute_rank(a,b,ub=10):
    #compute E'
    a1=-2*a
    b1=a^2-4*b
    print "(a,b)=",(a,b)
    n1=image_a(a,b,ub)
    print "␣"
    print "(a1,b1)=",(a1,b1)
    n2=image_a(a1,b1,ub)
    print n1, n2
    print "Guess:",log(n1*n2/4.0,2.0)
    print "␣"

def image_a(a,b,ub=10):
    im=0
    l=list_of_factors(b)
    for b1 in l:
        print "b_1=",b1, ":␣", "w^2=", b1, "u^4+", a, "u^2v^2+", b/b1, "v^4"
        if (a^2-4*b<0 or a<0) and b1<0:
            print "␣(No␣real␣solution)"
        else:
            t=findsq(lambda u,v:b1*u^4+a*u^2*v^2+(b/b1)*v^4,ub)
            if t:
                print t
                im+=1
            else:
                #try to prove no solution
                can_solve=solve_p(a,b,b1)
                if can_solve:
                    print "?␣-␣check␣by␣hand"
                #else it will print what failed.
    return im
```

2 is a congruent number iff $y^2 = x^3 - 4x$ has rank at least 1.

```
compute_rank(0,-4)
```

gives

```
 (a,b)= (0, -4)
b_1= -1 :  w^2= -1 u^4+ 0 u^2v^2+ 4 v^4
 (0, -1, 2)
True
b_1= 1 :  w^2= 1 u^4+ 0 u^2v^2+ -4 v^4
 (-1, 0, 1)
```

```
True
b_1= -2 :  w^2= -2 u^4+ 0 u^2v^2+ 2 v^4
(-1, -1, 0)
True
b_1= 2 :  w^2= 2 u^4+ 0 u^2v^2+ -2 v^4
(-1, -1, 0)
True

(a1,b1)= (0, 16)
b_1= -1 :  w^2= -1 u^4+ 0 u^2v^2+ -16 v^4
 (No real solution)
b_1= 1 :  w^2= 1 u^4+ 0 u^2v^2+ 16 v^4
(-1, 0, 1)
True
b_1= -2 :  w^2= -2 u^4+ 0 u^2v^2+ -8 v^4
 (No real solution)
b_1= 2 :  w^2= 2 u^4+ 0 u^2v^2+ 8 v^4
failed to solve over  2
4 1
Guess: 0.000000000000000
```

3.

```
compute_rank(5,4)
```

gives

```
(a,b)= (5, 4)
b_1= -1 :  w^2= -1 u^4+ 5 u^2v^2+ -4 v^4
(-1, -1, 0)
True
b_1= 1 :  w^2= 1 u^4+ 5 u^2v^2+ 4 v^4
(-1, 0, 1)
True
b_1= -2 :  w^2= -2 u^4+ 5 u^2v^2+ -2 v^4
(-1, -1, 1)
True
b_1= 2 :  w^2= 2 u^4+ 5 u^2v^2+ 2 v^4
(-1, -1, 3)
True

(a1,b1)= (-10, 9)
b_1= -1 :  w^2= -1 u^4+ -10 u^2v^2+ -9 v^4
 (No real solution)
b_1= 1 :  w^2= 1 u^4+ -10 u^2v^2+ 9 v^4
(-1, 0, 1)
True
b_1= -3 :  w^2= -3 u^4+ -10 u^2v^2+ -3 v^4
 (No real solution)
```

```
b_1= 3 :  w^2= 3 u^4+ -10 u^2v^2+ 3 v^4
failed to solve over  2
4 1
Guess: 0.000000000000000
```

4. The answers are 0, 1, 2, 3.

```
compute_rank(6,-2)
compute_rank(8,-7)
compute_rank(-3,10)
compute_rank(0,-377)
```

gives

```
(a,b)= (6, -2)
b_1= -1 :  w^2= -1 u^4+ 6 u^2v^2+ 2 v^4
failed to solve over  2
b_1= 1 :  w^2= 1 u^4+ 6 u^2v^2+ -2 v^4
(-1, 0, 1)
True
b_1= -2 :  w^2= -2 u^4+ 6 u^2v^2+ 1 v^4
(0, -1, 1)
True
b_1= 2 :  w^2= 2 u^4+ 6 u^2v^2+ -1 v^4
failed to solve over  2

(a1,b1)= (-12, 44)
b_1= -1 :  w^2= -1 u^4+ -12 u^2v^2+ -44 v^4
 (No real solution)
b_1= 1 :  w^2= 1 u^4+ -12 u^2v^2+ 44 v^4
(-1, 0, 1)
True
b_1= -2 :  w^2= -2 u^4+ -12 u^2v^2+ -22 v^4
 (No real solution)
b_1= 2 :  w^2= 2 u^4+ -12 u^2v^2+ 22 v^4
failed to solve over  2
b_1= -11 :  w^2= -11 u^4+ -12 u^2v^2+ -4 v^4
 (No real solution)
b_1= 11 :  w^2= 11 u^4+ -12 u^2v^2+ 4 v^4
(0, -1, 2)
True
b_1= -22 :  w^2= -22 u^4+ -12 u^2v^2+ -2 v^4
 (No real solution)
b_1= 22 :  w^2= 22 u^4+ -12 u^2v^2+ 2 v^4
failed to solve over  2
2 2
Guess: 0.000000000000000

(a,b)= (8, -7)
```

```
b_1= -1 :  w^2= -1 u^4+ 8 u^2v^2+ 7 v^4
failed to solve over  2
b_1= 1 :  w^2= 1 u^4+ 8 u^2v^2+ -7 v^4
(-1, 0, 1)
True
b_1= -7 :  w^2= -7 u^4+ 8 u^2v^2+ 1 v^4
(0, -1, 1)
True
b_1= 7 :  w^2= 7 u^4+ 8 u^2v^2+ -1 v^4
failed to solve over  2

(a1,b1)= (-16, 92)
b_1= -1 :  w^2= -1 u^4+ -16 u^2v^2+ -92 v^4
 (No real solution)
b_1= 1 :  w^2= 1 u^4+ -16 u^2v^2+ 92 v^4
(-1, 0, 1)
True
b_1= -2 :  w^2= -2 u^4+ -16 u^2v^2+ -46 v^4
 (No real solution)
b_1= 2 :  w^2= 2 u^4+ -16 u^2v^2+ 46 v^4
(-3, -1, 8)
True
b_1= -23 :  w^2= -23 u^4+ -16 u^2v^2+ -4 v^4
 (No real solution)
b_1= 23 :  w^2= 23 u^4+ -16 u^2v^2+ 4 v^4
(0, -1, 2)
True
b_1= -46 :  w^2= -46 u^4+ -16 u^2v^2+ -2 v^4
 (No real solution)
b_1= 46 :  w^2= 46 u^4+ -16 u^2v^2+ 2 v^4
(-1, -3, 8)
True
2 4
Guess: 1.00000000000000

(a,b)= (-3, 10)
b_1= -1 :  w^2= -1 u^4+ -3 u^2v^2+ -10 v^4
 (No real solution)
b_1= 1 :  w^2= 1 u^4+ -3 u^2v^2+ 10 v^4
(-1, 0, 1)
True
b_1= -2 :  w^2= -2 u^4+ -3 u^2v^2+ -5 v^4
 (No real solution)
b_1= 2 :  w^2= 2 u^4+ -3 u^2v^2+ 5 v^4
(-1, -1, 2)
True
b_1= -5 :  w^2= -5 u^4+ -3 u^2v^2+ -2 v^4
```

```
 (No real solution)
b_1= 5 :  w^2= 5 u^4+ -3 u^2v^2+ 2 v^4
(-1, -1, 2)
True
b_1= -10 :  w^2= -10 u^4+ -3 u^2v^2+ -1 v^4
 (No real solution)
b_1= 10 :  w^2= 10 u^4+ -3 u^2v^2+ 1 v^4
(0, -1, 1)
True

(a1,b1)= (6, -31)
b_1= -1 :  w^2= -1 u^4+ 6 u^2v^2+ 31 v^4
(-1, -1, 6)
True
b_1= 1 :  w^2= 1 u^4+ 6 u^2v^2+ -31 v^4
(-1, 0, 1)
True
b_1= -31 :  w^2= -31 u^4+ 6 u^2v^2+ 1 v^4
(0, -1, 1)
True
b_1= 31 :  w^2= 31 u^4+ 6 u^2v^2+ -1 v^4
(-1, -1, 6)
True
4 4
Guess: 2.00000000000000

(a,b)= (0, -377)
b_1= -1 :  w^2= -1 u^4+ 0 u^2v^2+ 377 v^4
(-2, -1, 19)
True
b_1= 1 :  w^2= 1 u^4+ 0 u^2v^2+ -377 v^4
(-1, 0, 1)
True
b_1= -13 :  w^2= -13 u^4+ 0 u^2v^2+ 29 v^4
(-1, -1, 4)
True
b_1= 13 :  w^2= 13 u^4+ 0 u^2v^2+ -29 v^4
(-3, -1, 32)
True
b_1= -29 :  w^2= -29 u^4+ 0 u^2v^2+ 13 v^4
(-1, -3, 32)
True
b_1= 29 :  w^2= 29 u^4+ 0 u^2v^2+ -13 v^4
(-1, -1, 4)
True
b_1= -377 :  w^2= -377 u^4+ 0 u^2v^2+ 1 v^4
(0, -1, 1)
```

```
True
b_1= 377 :  w^2= 377 u^4+ 0 u^2v^2+ -1 v^4
(-1, -2, 19)
True

(a1,b1)= (0, 1508)
b_1= -1 :  w^2= -1 u^4+ 0 u^2v^2+ -1508 v^4
 (No real solution)
b_1= 1 :  w^2= 1 u^4+ 0 u^2v^2+ 1508 v^4
(-1, 0, 1)
True
b_1= -2 :  w^2= -2 u^4+ 0 u^2v^2+ -754 v^4
 (No real solution)
b_1= 2 :  w^2= 2 u^4+ 0 u^2v^2+ 754 v^4
failed to solve over  13
b_1= -13 :  w^2= -13 u^4+ 0 u^2v^2+ -116 v^4
 (No real solution)
b_1= 13 :  w^2= 13 u^4+ 0 u^2v^2+ 116 v^4
(-2, -1, 18)
True
b_1= -26 :  w^2= -26 u^4+ 0 u^2v^2+ -58 v^4
 (No real solution)
b_1= 26 :  w^2= 26 u^4+ 0 u^2v^2+ 58 v^4
failed to solve over  13
b_1= -29 :  w^2= -29 u^4+ 0 u^2v^2+ -52 v^4
 (No real solution)
b_1= 29 :  w^2= 29 u^4+ 0 u^2v^2+ 52 v^4
(-1, -1, 9)
True
b_1= -58 :  w^2= -58 u^4+ 0 u^2v^2+ -26 v^4
 (No real solution)
b_1= 58 :  w^2= 58 u^4+ 0 u^2v^2+ 26 v^4
failed to solve over  13
b_1= -377 :  w^2= -377 u^4+ 0 u^2v^2+ -4 v^4
 (No real solution)
b_1= 377 :  w^2= 377 u^4+ 0 u^2v^2+ 4 v^4
(0, -1, 2)
True
b_1= -754 :  w^2= -754 u^4+ 0 u^2v^2+ -2 v^4
 (No real solution)
b_1= 754 :  w^2= 754 u^4+ 0 u^2v^2+ 2 v^4
failed to solve over  13
8 4
Guess: 3.00000000000000
```

5. We have

$$E : y^2 = x(x^2 - p^2)$$

$$E' : y^2 = x(x^2 + 4p^2)$$

We try to solve the following. We give the solution or another equation obtained by noting forced divisibility, and why it can't be solved.

E			
-1	$w^2 = -u^4 + p^2v^4$	$(u, v, w) = (0, 1, 1)$	
p	$w^2 = pu^4 - pv^4$	$(u, v, w) = (1, 1, 0)$	
$-p$	$w^2 = -pu^4 + pv^4$	$(u, v, w) = (1, 1, 0)$	
E'			
2	$w^2 = 2u^4 + 2p^2v^4$	$2w^2 = u^4 + p^2v^4$	$\left(\frac{2}{p}\right) = -1$
p	$w^2 = pu^4 + 4pv^4$	$pw^2 = u^4 + 4v^4$	$\left(\frac{-4}{p}\right) = -1$
$2p$	$w^2 = 2pu^4 + 2pv^4$	$2pw^2 = u^4 + v^4$	$\left(\frac{-1}{p}\right) = -1.$

We don't look at $-1, -2, -p, -2p$ because they will not be solvable over p. We get $\operatorname{rank} E(\mathbb{Q}) = \log_2\left(\frac{|\mathrm{im}\alpha_E||\mathrm{im}\alpha_{E'}|}{4}\right) = \log_2\left(\frac{4 \cdot 1}{4}\right) = 0$.

6. The image of α_E is in $K(S, 2)$ where S is the factors of b and the image of $\alpha_{E'}$ is in $K(S', 2)$ where S is the factors of $b' = a^2 - 4b$. Thus

$$\operatorname{rank} E(\mathbb{Q}) = \log_2|\mathrm{im}(\alpha_E)| + \log_2|\mathrm{im}(\alpha_{E'})| - 2 \le (\nu(b)+1) + (\nu(a^2-4b)+1) - 2 = \nu(b) + \nu(a^2-4b).$$

For E, if $\frac{b}{b_1} < 0$ and either $a < 0$ or $a^2 - 4b < 0$, then b_1 cannot be in the image. For E', if $\frac{a^2-4b}{b_1'} < 0$ and either $-2a < 0 \iff a > 0$ or $(-2a)^2 - 4(a^2 - 4b) = -16b < 0 \iff b > 0$, then b_1' cannot be in the image.

Either $a < 0$ or $a > 0$, so we can find b_1 or b_1' not in the image, and we have strict inequality.

7. The long exact sequence associated to

$$0 \to E[\phi] \to E[\psi\phi] \xrightarrow{\phi} E[\psi] \to 0$$

gives

$$\frac{E'(K)[\psi]}{\phi E(K)[\psi\phi]} \to H^1(K, E[\phi]) \to H^1(K, E[\psi\phi]) \to H^1(K, E[\psi]) \to \cdots$$

Now apply the nine lemma to

$$\begin{tikzcd}
& 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & S^{(\phi)}(E/K)/E'(K)[\psi] \arrow[r] \arrow[d] & S^{(\psi\phi)}(E/K) \arrow[r] \arrow[d] & \mathrm{im} \subseteq S^{(\psi)}(E'/K) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H^1(K, E[\phi])/\left(\frac{E'(K)[\psi]}{\phi E(K)[\psi\phi]}\right) \arrow[r] \arrow[d] & H^1(K, E[\psi\phi]) \arrow[r] \arrow[d] & \mathrm{im} \subseteq H^1(K, E[\psi]) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_v H^1(K_v, E)[\phi_*]/\ker \arrow[r] \arrow[d] & \prod_v H^1(K_v, E)[\psi\phi_*] \arrow[r] \arrow[d] & \mathrm{im} \subseteq \prod_v H^1(K_v, E)[\psi_*] \arrow[r] \arrow[d] & 0 \\
& 0 & 0 & 0 &
\end{tikzcd}$$

8. If $nP = 0$, then $n^2\widehat{h}(P) = \widehat{h}(nP) = 0$. We know $\widehat{h}(\phi(P)) - dh(P) = O(1)$ not depending on ϕ. Suppose $|\widehat{h}(2(P)) - dh(P)| < K$. Since the number of points on E in K with bounded height is finite, there is 2^nP with $|\widehat{h}(2P)| > K$. Now use the fact that if $x_n > k$ and $2x_n + k \geq x_{n+1} \geq 2x_n - k$, then $\lim_{n\to\infty} \frac{x_n}{2^n} \neq 0$.

9.

10.

11.

12. We get a pairing
$$E(K)/nE(K) \times E[n] \to K(S,n)/K^{\times 2}.$$
Now take generators P, Q of $E[n]$ ($(e_1, 0)$ and $(e_2, 0)$ for $n = 2$) to get
$$\alpha : E(K) \to K(S,n)/K^{\times 2} \times K(S,n)/K^{\times 2}.$$
Now some yucky calculations, see Silverman.

4 Arithmetic combinatorics

11/11

4.1 Weyl equidistribution

Let P by a polynomial. Our goal is the following:

1. Show that the sequence $P(n)$ is equidistributed modulo 1 whenever P has an irrational, nonconstant coefficient.

2. Obtain quantitative estimates for the equidistribution. For instance, find $C(\varepsilon)$ depending on the degree and coefficients of P such that there exists $q \in [C(\varepsilon)]$ with $\|P(q)\| \le \varepsilon$.

This idea is as follows.

1. By Weyl equidistribution 9.4.2, to show that a sequence is equidistributed, it suffices to show $\sum_{n=1}^{N} e(\alpha_n)$ grows slower than linearly. (We will prove a qualitative version first, and then a more quantitative version.)

   Weyl equidistribution holds because on $\mathbb{R}/\mathbb{Z}$, a characteristic function $1_{[a,b]}$ can be approximated by Fourier terms $e(nx)$, and vice versa.

   We now have to evaluate $\sum_{n=1}^{N} e(P(n))$.

2. We use the following trick.

   > (van der Corput trick, Lemma 9.4.13) We can express $\left|\sum_{n=1}^{N} e(\alpha_n)\right|^2$ in terms of sums over h of $\sum e(\Delta_h \alpha_n)$ where $\Delta_h \alpha_n = \alpha_{n+h} - \alpha_n$.
   > In light of Weyl equidistribution, this means that we can conclude equidistribution of a sequence from the equidistribution of its difference sequences $\Delta_h \alpha_n$.

   Thus, we can express the sum $\sum_{n=1}^{N} e(P(n))$ (or rather, its square) in terms of sums over polynomials of degree $d-1$. We iterate this until the polynomial is linear.

This will suffice to prove equidistribution for polynomials. Then we'll try a second time, this time being much more careful, i.e., actually estimating the exponential sums to get a quantitative bound.

3. Our plan to bound $S(P) = \sum e^{P(n)}$ is to keep squaring $S(P)$ until we get to terms with e^{linear}. If we kept on going until e^{constant}, then we could only estimate each term to be at most 1, and we would have no savings. The savings comes from stopping when we get to e^{linear}: when summing these we can avoid getting something on the order of n, because we'll find (Lemma **??**)

   $$\sum e^{\lambda x + b}$$

   will be something on the order of

   $$\min\left(\text{number of terms}, O\left(\frac{1}{\lambda}\right)\right)$$

   (the smaller the λ, the more the terms can accumulate), and if we know how to sum these (Lemma **??**) we'll get savings.[8]

   We'll need a number-theoretic estimate on how close to an integer the λ can get (Lemma **??**), and then we obtain Weyl's inequality 9.4.15. This gives the result after we plug it into a qualitative bound for equidistribution inspired from step 1.

[8] We can think of the differencing operation as that equidistribution for degree $d-1$ implies equidistribution for degree d, or a more qualitative statement that an estimate for an exponential sum of degree $d-1$ implies an estimate for degree d. We don't want to go to $d = 0$, because constants are not equidistributed.

4.1.1 Weyl equidistribution

We say a sequence is equidistributed if in the long run, the proportion of elements falling in an interval is the same as expected if the sequence were random.

Definition 9.4.1: df:equidistribution We say that the sequence $(\alpha_n)_{n\in\mathbb{N}}$ is **equidistributed** (modulo 1) if for any $0 \le a < b \le 1$,

$$\lim_{N\to\infty} \frac{\{n : \alpha_n \in [a,b]\}}{N} = b - a.$$

Generalities on why equidistribution is useful, and examples.

Theorem 9.4.2 (Weyl equidistribution)**:** thm:weyl-equid The following are equivalent.

1. The sequence $(\alpha_n)_{n\in\mathbb{N}}$ is equidistributed. In other words, for all intervals $[a,b] \subseteq [0,1]$
$$\lim_{N\to\infty} \frac{\sum_{n=1}^{N} 1_{[a,b]}(\alpha_n)}{N} = b - a.$$
2. For any nonzero $m \in \mathbb{Z}$,
$$\lim_{N\to\infty} \frac{\sum_{n=1}^{N} e(m\alpha_n)}{N} = 0.$$
(For $m = 0$ this clearly equals 1.)
3. For any continuous function $f : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$,
$$\text{eq:weyl-equid-f} \quad \lim_{N\to\infty} \frac{\sum_{n=1}^{N} f(\alpha_n)}{N} = \int_0^1 f(x)\,dx. \tag{9.4}$$

Note item 3 can be construed as saying that a time average (thinking of the α_n as coming at time n) is the same as a space average (over all x). Ergodic theory gives these kinds of results; the typical setup there is where $\alpha_n = T(\alpha_{n-1})$; i.e., the α_n are from a dynamical system.

Note item (2) gives an analytic criterion for equidistribution, which is often easier to check than (1).

Basic idea: Note (2) is a special case of (3). (2) gives (3) because we can approximate f by exponentials. (1) gives (3) because we can approximate f by simple functions. That (3) gives (1) is of a different flavor: we can't approximate $1_{[a,b]}$ in L^∞ by continuous functions. Instead we approximate using functions whose support is close to $[a,b]$ (think Urysohn-type arguments).

Proof. $\underline{(3) \implies (2)}$: Clear.

$\underline{(2) \implies (3)}$: Given f, because $\{e(mx) : m \in \mathbb{Z}\}$ is dense in the space of continuous functions (this is basically Stone-Weierstrass), given $\varepsilon > 0$, we can find M and a_m so that letting

$$g(x) = \sum_{|m|\le M} a_m e(mx),$$

we have

$$\|f-g\|_\infty \le \varepsilon.$$

Then

$$\begin{aligned}\frac{1}{N}\sum_{n=1}^{N} f(\alpha_n) &= \frac{1}{N}\sum_{n=1}^{N}\left[\left(\sum_{m=1}^{M} a_m e(m\alpha_n)\right)+(f-g)(\alpha_n)\right]\\ &= \underbrace{\sum_{m=1}^{M}\left(a_m\frac{1}{N}\sum_{n=1}^{N} e(m\alpha_n)\right)}_{\to a_0 \text{by (2)}} + \underbrace{\frac{1}{N}\sum_{n=1}^{N}(f-g)(\alpha_n)}_{|\bullet|\le\varepsilon}\end{aligned}$$

Thus since ε is arbitrary, as $N\to\infty$, this goes to $a_0=\int_0^1 f(x)\,dx$. [9]

(1) $\Longrightarrow$ (3): Since (9.4) holds for all $1_{[a,b]}$ by assumption and both sides are linear, we have

$$\lim_{N\to\infty}\frac{\sum_{n=1}^N g(\alpha_n)}{N}=\int_0^1 g(x)\,dx$$

for all functions g that are linear combinations of $1_{[a,b]}$. Now f can be approximated by within ε by such a function: because f is uniformly continuous, we can split f into a finite number of intervals $[x_n,x_{n+1})$ where f does not change by more than ε; then approximate f on each such interval by a function $y_n 1_{[x_n,x_{n+1})}$. Since both sides of (9.4) are continuous in f with respect to the norm L^∞, we get that (9.4) holds for f.

(3) $\Longrightarrow$ (1): Given $[a,b]$, we will find f,g with

$$f\le 1_{[a,b]}\le g$$

with supports very close to $[a,b]$.

1. Let g be a nonnegative continuous function with support contained in $[a,b]$ and with $g=1$ on $[a+\varepsilon,b-\varepsilon]$.

2. Let f be a nonnegative continuous function with support $[a-\varepsilon,b+\varepsilon]$ and with $f=1$ on $[a,b]$.

Now (9.4) holds for a,b, so

$$b-a-2\varepsilon\le\int_0^1 f(x)\,dx\le\lim_{N\to\infty}\frac{f(\alpha_n)}{N}\le\lim_{N\to\infty}\frac{1_{[a,b]}(\alpha_n)}{N}\le\lim_{N\to\infty}\frac{g(\alpha_n)}{N}=\int_0^1 g(x)\,dx\le b-a+2\varepsilon.$$

□

Problem 9.4.3: True or false: (9.4) holds for all *measurable* f.

False. In the proof about we can't approximate f by simple functions; we have to approximate it with linear combinations of $1_{[a,b]}$. ($1_{\{a_n:n\in\mathbb{N}\}}$ is a clear counterexample.) This

[9] We can't have tried to prove this by writing the Fourier series $f=\sum_{m\in\mathbb{Z}}a_m e(mx)$ because the Fourier series may not converge. The approximations for different M may not combine well into one Fourier series. Compare with why Stone-Weierstrass does not imply convergence of Fourier series.

negative result can be cited as: the measure corresponding to $\{\{\alpha n\} : n \le N\}$ converge in the weak sense to the uniform measure, but not in the total variation sense. (See Billingsley, Probability and Measure, p. 338)

We already get the following.

Theorem 9.4.4: thm:aln-equid Let $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ be irrational. Then αn is equidistributed modulo 1.

Proof. By Theorem 9.4.2 it suffices to check (2). We have

$$\left|\sum_{n=1}^{N} e(m\alpha n)\right| = \left|e(m\alpha n)\frac{1-e(m\alpha N)}{1-e(m\alpha)}\right| \le \frac{2}{|1-e(m\alpha)|} = O_N(1)$$

independent of N, as needed. □

4.1.2 Polynomials are equidistributed, take 1

Our goal is to use induction to show that polynomials are equidistributed. The induction will be achieved by the following.

Theorem 9.4.5: thm:fn+r-fn Suppose $f(n)$ is a sequence such that for every r, $(f(n+r)-f(n))$ is equidistributed. Then $f(n)$ is equidistributed.

We will use Weyl's criterion to prove this. Weyl's criterion relates the equidistribution of $f(n)$ to $\sum e(f(n))$. We bound this by bounding its square, $|\sum e(f(n))|^2$. Now if we expand this out, we get $\sum_{1\le n,n+r\le N} e(f(n+r))\overline{e(f(n))}$ which suggests that the equidistribution of f should be related to the equidistribution of $\Delta_r f(n) = f(n+r) - f(n)$ for various r.

Now simply expanding doesn't work, because $|r|$ ranges from 0 to $n-1$ here, and we can't bound all those sums simultaneously. On the other extreme, we have the trivial bound $|\sum e(f(n))|^2 \le \sum e(f(n))\overline{e(f(n))} = N$ where r is only 0 here. The idea is to seek a compromise: bound $|\sum e(f(n))|^2$ by $e(\Delta_r(f(n)))$ for $0 \le r \le h$, and then choose h appropriately.

Lemma 9.4.6 (van der Corput)**:** lem:vdc-equid Let $z_j \in \mathbb{C}$ for $1 \le j \le n$. For $j \notin [1,n]$, write $z_j = 0$ for convenience. Then

$$h^2\left|\sum_{j=1}^{n} z_j\right|^2 \le (n+h-1)\left[\sum_{r=1}^{h-1}(h-r)\Re\sum_{j=1}^{n-r}\overline{z_i}z_{i+r} + h\sum_{k}|z_k|^2\right]$$

Proof. We write

$$\begin{aligned} h^2\left|\sum_{j=1}^{n} z_j\right|^2 &= \left|\sum_{j=-h+2}^{n}\left(\sum_{k=0}^{h-1} z_{j+k}\right)\right|^2 \\ &\le \left|\sum_{j=-h+2}^{n}\left|\sum_{k=j}^{j+h-1} z_j\right|^2\right| && \text{QM-AM inequality} \end{aligned}$$

$$
\begin{aligned}
&\leq \left| \sum_{j=-h+2}^{n} \left| \sum_{j \leq k, k' \leq j+h-1} \overline{z_k} z_{k'} \right|^2 \right| \\
&\leq \left| \sum_{j=-h+2}^{n} \left| \sum_{j \leq k, k' \leq j+h-1} \overline{z_k} z_{k+r} \right|^2 \right| \\
&\leq \left| \sum_{j=-h+2}^{n} \sum_{1 \leq r \leq h-1} \Re(\overline{z_k} z_{k+r}) + h \sum_{k} |z_k|^2 \right| \\
&\leq (n+h-1) \left[\sum_{r=1}^{h-1} (h-r) \Re \sum_{j=1}^{n-r} \overline{z_i} z_{i+r} \right]
\end{aligned}
$$

□

Proof of Theorem **??**. As mentioned, the idea is to choose h not too large (a constant depending on ε), so that all $e(\Delta_h(f))$ will be in a long sum, and choose h not too small, so $h \sum |z_j|^2$ contributes little to the sum.

Fix h. By van der Corput,

$$
\begin{aligned}
\left| \sum_{j=1}^{n} e(f(j)) \right|^2 &\leq \frac{n+h-1}{h^2} \left[2 \sum_{r=1}^{h-1} (h-r) \sum_{j=1}^{n-r} e(\Delta_r(f(j))) + h \sum_{j=1}^{n} |f(j)|^2 \right] \\
&= \frac{2(n+h-1)}{h^2} \sum_{r=1}^{h-r} o_r(n) + \frac{n+h-1}{hn} n^2.
\end{aligned}
$$

Fix $h > \frac{1}{\varepsilon_1}$ large, and then choose n large enough so that $\frac{n+h-1}{nh} < \varepsilon_1 n$, and the $o_r(n)$'s are $< \varepsilon_2 n$. We get this is at most $(2\varepsilon_1\varepsilon_2 + \varepsilon_1)n^2$. Thus the sum is $o(n^2)$. Taking square roots and using Weyl equidistribution gives the result. □

Theorem 9.4.7: Let f be a polynomial with a irrational nonconstant coefficient. Then $f(n)$ is equidistributed.

Proof. Induct using Theorem 9.4.5. □

4.1.3 Weyl's exponential sums and quantitative bounds

Theorem 9.4.4 tells us that for any ε there exists $n \in \mathbb{N}$ such that $\alpha n \in \mathbb{Z} + (-\varepsilon, \varepsilon)$. We know by Dirichlet's Theorem that we can choose $n = O(\varepsilon^{-2})$. Can a quantitative version of Weyl equidistribution tell us something similar?

We would now like a machine to give an estimate for

eq:estimate-weyl-error
$$
\sum_{n=1}^{N} \frac{1_{[a,b]}(\alpha_n)}{N} - (b-a). \tag{9.5}
$$

In particular, if the sum is > 0 then $\alpha_n \in [a,b]$ for some $n \in [N]$. For simplicity, consider the interval $I = (-\varepsilon, \varepsilon)$. For ease of notation, write $I = 1_{(-\varepsilon,\varepsilon)}$. Now if we try to quantify the proof of Theorem 9.4.2 directly, things will be very messy because we can't just expand $1_{(-\varepsilon,\varepsilon)}$ in Fourier series—it has bad convergence. So instead of considering (9.5), let's consider[10]

$$\sum_{n=1}^{N} \frac{I * I(\alpha_n)}{N} - 4(b-a)^2.$$

The function $I * I$ is more well-behaved—it is continuous (it looks like a triangle supported on $[-2\varepsilon, 2\varepsilon]$) and its Fourier series converges absolutely:

$$\text{eq:fourier-i*i}\,\widehat{I * I}(m) = \left(\int_{-2\varepsilon}^{2\varepsilon} e^{-2\pi i m x}\,dx\right)^2 = \begin{cases} \left(\frac{-e^{-2\pi i \varepsilon m}+e^{2\pi i \varepsilon m}}{2\pi i m}\right)^2 = \left(\frac{\sin 2\pi\varepsilon n}{\pi m}\right)^2, & m \neq 0 \\ 4\varepsilon^2, & m = 0 \end{cases} \tag{9.6}$$

(cf. in Fourier analysis, how the Fejér kernel is nicer than the Dirichlet kernel. This is the reason why Fourier series for L^1 functions don't necessarily converge, but the Abel sums do.)

Theorem 9.4.8: Let

$$S(m, N) := \frac{1}{N}\sum_{i=1}^{N} e(-m\alpha_i).$$

Then

$$\left|\sum_{n=1}^{N} \frac{I * I(\alpha_n)}{N} - 4\varepsilon^2\right| = O\left(\frac{1}{C}\varepsilon^2 + C \max_{0<|m|<\frac{C}{\varepsilon^2}} S(m, N))\right).$$

Given $\varepsilon, \varepsilon'$, we can make the RHS at most $\varepsilon'\varepsilon^2$ by choosing C so that $\frac{1}{C} < \frac{\varepsilon'}{2}$, and choosing N so that $\max_{|m|<\frac{C}{\varepsilon^2}} S(m, N) < \varepsilon^2$.

In particular, if we make the RHS less than $4\varepsilon^2$, we get a concrete N such that $\alpha_n \in (-2\varepsilon, 2\varepsilon)$ for some $n \in [N]$.

More generally, we can view this as a special case of the following fact: If f has a certain norm and the Fourier coefficients $\widehat{f}(m)$ for $m \leq M$ are all small, then f cannot be 0 on a large interval. (We'll leave it to the reader to state this precisely.) This makes sense intuitively because f has significant large Fourier modes, which means f should oscillate a lot. To see why our theorem is in a way, a special case, let $f = \delta_{\alpha_1} + \cdots + \delta_{\alpha_N}$; then $\widehat{f}(m) = \sum_{i=1}^{N} e(-m\alpha_i)$. (Actually we're working with distributions so I don't know how to make this rigorous, but I'm sure there's a way.)

Proof. We have by (9.6) that

$$\begin{aligned} \frac{1}{N}\sum_{i=1}^{N} I * I(\alpha_i) &= \frac{1}{N}\sum_{i=1}^{N}\sum_{m\in\mathbb{Z}} \widehat{I * I}(\alpha_i) \\ &= 4\varepsilon^2 + \frac{1}{N}\sum_{i=1}^{N}\sum_{m\in\mathbb{Z}\backslash\{0\}} \left(\frac{\sin 2\pi\varepsilon n}{\pi m}\right)^2 e(-m\alpha_i) \\ &= 4\varepsilon^2 + \sum_{m\in\mathbb{Z}\backslash\{0\}} \left(\frac{\sin 2\pi\varepsilon n}{\pi m}\right)^2 S(m, N) \end{aligned}$$

[10] Note: it would be better to approximate $1_{[a,b]}$ by a trapezoidal function, but the calculations are messier, so we'll give up a precise bound for (9.5) for something simpler.

The main contribution comes from the $m = 0$ term. We look at the contribution from the rest. First note

$$\left(\frac{\sin 2\pi\varepsilon n}{\pi m}\right)^2 \le \min\left(\left(\frac{1}{\pi m}\right)^2, (2\varepsilon)^2\right).$$

We now estimate the sum into two regimes, when $|m| < \frac{C}{\varepsilon^2}$, and $|m| > \frac{C}{\varepsilon^2}$ (it turns out we don't need to further divide into $< \frac{1}{\varepsilon}$ and $> \frac{1}{\varepsilon}$). We get

$$\begin{aligned}
\left|\frac{1}{N}\sum_{i=1}^{N}\frac{I * I(\alpha_i)}{N} - 4\varepsilon^2 N\right| &\le \sum_{m\ne 0, |m|<\frac{C}{\varepsilon^2}} S(m,N)(2\varepsilon)^2 + \sum_{m\ne 0, |m|\ge\frac{C}{\varepsilon^2}} S(m,N)\left(\frac{1}{\pi m}\right)^2 \\
&\le \left(2\left(\frac{C}{\varepsilon^2}\right)(2\varepsilon)^2 \max_{0<|m|<\frac{C}{\varepsilon^2}} S(m,N) + \frac{2N}{\pi^2}\int_{\frac{C}{\varepsilon^2}}^{\infty}\frac{1}{m^2}\,dm\right)(1+o(1)) \\
&\le O\left(C \max_{0<|m|<\frac{C}{\varepsilon^2}} S(m,N) + \frac{1}{C}\varepsilon^2\right).
\end{aligned}$$

□

Corollary 9.4.9: cor:weyl-exist There exist constants $C > 0$ and $\varepsilon' > 0$ such that if N satisfies

$$\max_{0<|m|<\frac{C}{\varepsilon^2}} S(m,N) < \varepsilon',$$

then there exists $n \in [N]$ with $\alpha_n \in (-\varepsilon, \varepsilon)$.

4.1.4 Estimates for summing $e(\alpha x + \beta)$

Lemma 9.4.10: Let $\alpha, \beta \in \mathbb{R}$. Then for $n \in \mathbb{N}$,

$$\text{eq:e(ax+b)} \quad \left|\sum_{x=1}^{n} e(\alpha x + \beta)\right| \le \min\{n, (2\,\|\alpha\|)^{-1}\} \tag{9.7}$$

where $\|\alpha\|$ is the distance from α to the nearest integer, and $e(x) = \exp(2\pi i x)$.

Proof. The constant β doesn't affect the inequality (since a factor of $e(\beta)$ can be pulled out of the sum). If $\alpha = 0$ then the sum is n. If $\alpha \ne 0$ then the sum is a geometric series,

$$\sum_{x=1}^{n} e(\alpha x + \beta) = e(\alpha)\frac{1 - e(\alpha n)}{1 - e(\alpha)} = e\left(\frac{\alpha}{2}\right)\frac{1 - e(\alpha n)}{e\left(-\frac{\alpha}{2}\right) - e\left(\frac{\alpha}{2}\right)}.$$

Since $\sin z = \frac{1}{2i}(e^{iz} - e^{-iz})$, bounding the numerator by 2 trivially, the sum has modulus at most $|\sin \pi\alpha|^{-1}$. Since $|\sin \pi\alpha| \ge 2\,\|\alpha\|$ the inequality follows. □

Lemma 9.4.11: lem:weyl1 Let $\theta_1, \ldots, \theta_m$ be reals with $\|\theta_i - \theta_j\| \ge \frac{1}{r}$ when $i \ne j$. Then

$$\sum_{i=1}^{m} \min\left(\frac{1}{\|\theta_i\|}, Q\right) \le 6(Q + r)\ln Q.$$

Lemma 9.4.12: Let $q, Q, R \in \mathbb{N}$ $Q \geq 2$, and let $\frac{a}{q}$, $a \perp q$ be an approximation to α satisfying $\left|\alpha - \frac{a}{q}\right| \leq q^{-2}$. Then

$$\sum_{r=0}^{R} \min\left(\frac{1}{\|\alpha x+\beta\|}, Q\right) \leq 48(\ln Q)(Q+q)\left(1+\frac{R}{q}\right).$$

Where do these terms come from?

1. $(\ln Q)Q$. Ignoring any terms where $\alpha x + \beta$ is very close to 0, and ignoring the effect of having gone around the circle many times and ending up close to where you started (so only looking at the first q or so terms), we have that at worst the $\frac{1}{\|\alpha x+b\|}$ could look like $\frac{1}{1/Q}, \frac{1}{1+1/Q} + \cdots + \frac{1}{q}$; this tail gives, using an integral estimate, the $q(\ln Q)$ part. Plus Q.

2. If R is much larger than q, then splitting into lengths of size q we multiply by $\frac{R}{q}$.

The point of the Lemma 9.4.11 is just to abstract away what we need for Lemma **??**.

Proof of Lemma 9.4.11. We make two simplifying assumptions.

1. Each θ_i lies in $[-1/2, 1/2]$: Note $\|x+N\| = \|x\|$ for $x \in \mathbb{R}$ and $N \in \mathbb{N}$, so we can take a representative of each θ_i in $[-1/2, 1/2]$.

2. The contribution to the sum from the non-negative θ_i, which we call S^+ is at least one half the total: else we replace each θ_i by $-\theta_i$.

Next suppose the nonnegative θ_i are

$$0 < \theta_1 < \theta_2 < \ldots < \theta_k.$$

Because $\|\theta_i - \theta_j\| \geq r^{-1}$ for $i \neq j$, we have $\theta_i \geq \frac{i-1}{r}$. Then

$$\begin{aligned}
\sum_{i=1}^{k} \min\left(\frac{1}{\|\theta_i\|}, Q\right) &= \sum_{i=1}^{k} \min\left(\theta_i^{-1}, Q\right) \\
&\leq \sum_{i=1}^{k} \min\left(\frac{r}{i-1}, Q\right) && \text{since } \theta_i \geq \frac{i-1}{r} \\
&= \underbrace{\sum_{i=0}^{\lfloor r/Q \rfloor} Q}_{=:A \leq \left(1+\frac{r}{Q}\right)Q} + \underbrace{\sum_{r/Q<i<k} \frac{r}{i}}_{=:B}. && \left(Q \leq \frac{r}{i-1} \Leftrightarrow i-1 \leq \frac{r}{Q}\right)
\end{aligned}$$

We now use an integral estimate for the right-hand sum. Because $i^{-1} \leq 2t^{-1}$ for $i \leq t \leq i+1$ and $i \geq 1$,

$$B \leq r\int_{\lceil r/Q \rceil}^{k} 2t^{-1} \leq r\int_{r/Q}^{k} 2t^{-1} = 2r\left(\ln k - \ln\left(\frac{r}{Q}\right)\right).$$

So

$$\begin{aligned}S^+ &\le A+B \le Q+r+2r(\ln k+\ln Q-\ln r)\\ &\le Q+r+2r\ln Q\\ &\le 3(Q+r)\ln Q,\end{aligned}$$

since $Q\ge e$ implies $\ln Q\ge 1$.

Hence the whole sum is at most

$$2S^+ \le 6(Q+r)\ln Q.$$

□

4.1.5 Putting it all together: Weyl's inequality implies equidistribution of $P(n)$.

Lemma 9.4.13 (Squaring an exponential sum gives a sum of exponential of differences)**:** lem:square-expsum Let $S(f)=\sum e^{f(n)}$. We have

$$|S(f)|^2=\sum_{|d|<N}\sum_{n\in I(d)} e^{(\Delta_d(f)(n))}.$$

Lemma 9.4.14 (Lemma 9.4.13 iterated)**:**

$$|S(f)|^{2^\ell}\le (2N)^{2^\ell-\ell-1}\sum_{|d_1|,\dots,|d_\ell<N}\sum_{n\in I(d)} e(\Delta_{d_\ell,\dots,d_1}(f)(n)).$$

Proof of Lemma 9.4.13. $|S(f)|^2=$ □

Proof. Induct and Cauchy-Schwarz. □

Now we apply this lemma until the finite differences get us down to linear terms, use the fact that summing linear terms gives us stuff of the form $\min\cdots$, and then apply our lemmas on sums of those terms.

Theorem 9.4.15 (Weyl's inequality)**:** thm:weyl-ineq Given the approximation $\left|\alpha-\frac{a}{q}\right|\le\frac{1}{q^2}$, we have

$$S(f)\prec N^{1+\varepsilon}(N^{-1}+q^{-1}+N^{-k}q)^{\frac{1}{K}}$$

where $K=2^{k-1}$.

What can we do with this? We can immediately apply Weyl equidistribution.

Theorem 9.4.16: Suppose $P=\sum a_m x^m$ is a polynomial with

$$d=\max\{m : a_m\in\mathbb{R}\backslash\mathbb{Q}\}\ge 1.$$

Then for any $\varepsilon>0$, there exists $C:=C(P)$ such that for any $\varepsilon'>0$, there exists a positive integer

$$n\le C(\varepsilon')^{-2^{d-1}-\varepsilon}$$

such that

$$\|P(n)\|<\varepsilon'.$$

Proof. We first prove this for P with leading term irrational.

Let q_m be such that $\left\|\alpha m - \frac{a}{q_m}\right\| \le \frac{1}{q_m^2}$. Then by Weyl's inequality, for any $\varepsilon_1 > 0$,

$$S(f) \ll N^{1+\varepsilon_1}(N^{-1} + q_m^{-1} + N^{-d}q_m)^{\frac{1}{2^{d-1}}}.$$

What are the q_m??? Where did we use irrationality?

By Corollary 9.4.9, it suffices to make $C \max_{0<|m|<C/\varepsilon^2} S(m, N) < \varepsilon'$, i.e., make

$$N^{\varepsilon - \frac{1}{2^{d-1}}} < C_1\varepsilon',$$

or

$$N > C_2(\varepsilon')^{\left(\frac{1}{2^{d-1}}+\varepsilon\right)^{-1}}.$$

(Constants can depend on P, ε but not on ε'.) Since $\varepsilon \in (0, \frac{1}{2^{d-1}})$ was arbitrary, we get the result. □

Threads to tie up:

1. Arithmetic questions. 11.1.12. Weyl using Gowers uniformity norms?
2.

4.2 Frieman's Theorem

12-20

1. We look for a generalized arithmetical progression inside $nA - nA$ for some A. (Why do we do this when we want it the other way around, for A to be in a GAP? See next part.) Our plan is to show we have

   $$\text{GAP} \subseteq B(R, \varepsilon) \subseteq 2A - 2A$$

   with relevant constants independent of $|A|$. Basically, $B(R, \varepsilon)$ is the set of all x satisfying some easy-to-characterize condition, that ensures the existence of a GAP inside. We define Bohr sets; Bogolyubov's Lemma gives the second inclusion. Geometry of numbers (Minkowski's Theorem) gives the first inclusion. To get $B(R, \varepsilon)$ inside $2A - 2A$, we would like to work inside $\mathbb{Z}/p$ for some p not too large (treat A like it's inside $\mathbb{Z}/p$); to do this we need a Freiman isomorphism from A to a subset of $\mathbb{Z}/p$; this is Ruzsa's Model Lemma.

2. Now we turn things around, take a GAP in $2A - 2A$ to get A inside a GAP. We will use

   (a) Ruzsa's covering lemma, which says if $|A + B| \le K|A|$ (if B does not expand A too much) then B is in $C(K)$ translates of $A - A$.

   (b) Ruzsa-Plünnecke which gives $\frac{|mA-nA|}{|A|} \le \left(\frac{|A+A|}{|A|}\right)^{m+n}$.

In particular, R-P says $2A-2A$ does not expand A too much, so neither does $P \subseteq 2A-2A$; by Ruzsa covering, A is in $P-P+X$ for X small, i.e. A is in a GAP.

Goal:

Theorem 9.4.17 (Freiman's Theorem)**:** Let $A \subseteq \mathbb{Z}$ be a set such that $|A+A| \leq c|A|$. Then A is contained in a δ-dimensional arithmetic progression P of cardinality at most $\kappa|A|$, where δ and κ depend on c only.

Definition 9.4.18: Let $R = \{r_1, \dots, r_d\} \subseteq \mathbb{Z}/N$. Define a **Bohr set**

$$B(R, \varepsilon) = \left\{ x \in \mathbb{Z}/N\mathbb{Z} : \left\| \frac{r_j x}{N} \right\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon \text{ for } j = 1, \dots, d \right\}.$$

d is the dimension.

How to think about this.

1. A finitary, quantitative analogue of a neighborhood is in a weak topology. Think of it as the set of x which are small with respect to multiplying by the set of r_j.
2. The pullback of the box $[-\varepsilon, \varepsilon]^d$ under the map $\mathbb{Z}/N\mathbb{Z} \to (\mathbb{R}/\mathbb{Z})^d$ given by $\left(\frac{r_1 x}{N}, \dots, \frac{r_d x}{N}\right)$.

Lemma 9.4.19 (Bogolyubov)**:** Suppose $A \subseteq \mathbb{Z}/N\mathbb{Z}$ with cardinality αN. Then $2A-2A$ contains a Bohr set of dimension at most $\frac{4}{\alpha^2}$ and width $\frac{1}{4}$. In particular,

$$B(\text{Spec}_{\alpha^{\frac{1}{2}}/2}(A), \frac{1}{10}) \subseteq 2A - 2A.$$

(Bohr nets of smaller dimension are LARGER. We have a significant Bohr set in A.)

What is the connection to Bohr sets? Why are they useful? Note that another characterization of the definition is that $e\left(\frac{r_j x}{N}\right) \approx 1$ (here we just care to have $e\left(\frac{r_j x}{N}\right) > 0$). (You can already see it might be useful when we have to deal with exponential sums...)

Careful: this is non-normalized Fourier

Q: Why do we look at $2A-2A$? Why does it fail for $A-A$, or A? The key is that we had this nice representation

$$f(x) = 1_A * 1_A * 1_{-A} * 1_{-A}(x) \implies \hat{f}(r) = \left|\widehat{1_A}(r)\right|^4.$$

(cf. Vitali's lemma: if $\mu(A) > 0$ then $A-A$ has a neighborhood of the origin!) $2A-2A$ is more "regular/uniform" than A by Parseval-type bounds.

Proof. To be contained in $2A-2A$ means that $f(x) > 0$. Being in a Bohr neighborhood is exactly a statement that $e\left(\frac{r_j x}{N}\right) > 0$ for all j. By forcing a bunch of these to be 0, by Fourier inversion we can hope to make $f > 0$. Of course we choose take the set of R for which the rth Fourier mode is large!

$$|\widehat{1_A}(r)| \geq \frac{\alpha^{3/2}}{2}.$$

By Parseval, there aren't too many of these, $|R| \le \frac{4}{\alpha^2}$. Now the others can't contribute too much, so $f(x) > 0$ for those $x \in B(R, \frac{1}{4})$.

$$f(x) = \alpha^4 + \underbrace{\sum_{r\in R} |\widehat{1}_A(r)|^4}_{\ge 0} + \underbrace{\sum_{r \notin R \cup \{0\}}}_{\ge -\frac{\alpha^3}{4}\|1_A\|^2} = 0.$$

the second inequality because the other r's have small Fourier coefficients. □

Lemma 9.4.20 (Ruzsa's model lemma, 6.1 in Tao-Vu)**:** Suppose that $A \subseteq Z$ is a finite set where Z is either torsion free or prime cyclic. Let m be an integer such that

$$2n|nA - nA| < N < |Z|.$$

Then there exists a subset $A' \subseteq A$ of cardinality $|A'| \ge \frac{|A|}{n}$ and a Frieman isomorphism $\pi : A' \to B$ from A' to a subset $B \subseteq \mathbb{Z}/N$ or order n.

The idea is a first moment method. Recall this problem: Let A be an additive set of non-zero integers. Then A contains a sum-free subset B of size $|B| > \frac{|A|}{3}$.

Proof idea: Suppose $A \subseteq [0, N)$.

1. How could we get a sum-free subset? Note $\left[\frac{N}{3}, \frac{2N}{3}\right)$ is sum-free, so $\left|A \cap \left[\frac{N}{3}, \frac{2N}{3}\right)\right|$ is sum-free. If this is $> \frac{|A|}{3}$, we're done. But it might not be.

2. What do we do in general? It seems like we could have the inequality hold if we're allowed to vary A, because "on average" $\frac{1}{3}$ values should be in the range. We're in luck because *we have a degree of freedom we haven't used yet.*

   Idea: let N be prime and consider λA for $\lambda \in (\mathbb{Z}/N)^\times$; addition is preserved by multiplication by λ. By a probabilistic/expected value argument, for some λ, $\left|\lambda A \cap \left[\frac{N}{3}, \frac{2N}{3}\right)\right| > \frac{|A|}{3}$.

🔑 First moment method.

This is similar to what we'll do here.

1. How could we get a Freiman isomorphism? We can get a Frieman n-homomorphism by considering $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$, and restricting to A in some interval $[\frac{jN}{n}, \frac{(j+1)N}{n})$. However, it might not be an isomorphism. We have a "collision" problem: maybe we have different $(x_1, \ldots, x_n)$ and $(x_1', \ldots, x_n')$ with same different sum that gets sent to the same thing, i.e. It seems like this has low probability when N is large.

2. Again, we need to use our freedom to vary our set. Technically, we need to work modulo a prime, so that's where we'll consider modifying our set by multiplication by λ; on average, the number of collisions will be small; we choose N large enough to get the average below 1.

Proof. We may as well consider the case where $Z = \mathbb{Z}/p$ is prime cyclic. Consider

$$\mathbb{Z}/p \xrightarrow{\cdot\lambda} \mathbb{Z}/p \xrightarrow{u} \mathbb{Z} \xrightarrow{\pi_N} \mathbb{Z}/N$$

where u is the unfolding map. (Let $\pi = \pi_N \circ u$.) We need to find the average number of collisions when $\lambda \in (\mathbb{Z}/p)^\times$ varies. Straightforward computation shows it is at most (it comes down to rearranging the condition for collision to become $\lambda \in (kN)^{-1}(nA - nA) \bmod p$)

$$\frac{2np}{N}|nA - nA|\frac{1}{p-1} < 1$$

when the conditions are satisfied. □

Geometry of numbers

4.3 Szemerédi's Theorem for $n = 4$

(See Tao-Vu Ch. 11, and Green-Tao paper.)

1. Why are Fourier coefficients insufficient for a dichotomy between randomness and structure that would detect 4-AP's? We can find a counterexample with some set like $\left\{n : \|\alpha n^2\|_{\mathbb{R}/\mathbb{Z}} \le \varepsilon\right\}$: it doesn't correlate with any $e(n\theta)$, but it's not "random" with respect to 4-AP's, basically because $x^2, (x+h)^2, \ldots, (x+3h)^2$ are not independent.

2. How do we state Szemerédi's Theorem for functions instead of sets?

Step 1: Define uniformity norms and establish basic inequalities.

Definition 9.4.21: The **Gowers uniformity norms** are defined on an additive group Z by

$$\|f\|_{U^d(Z)} = \left(\mathbb{E}_{x\in G}\mathbb{E}_{h\in Z^d} \prod_{\omega\in\{0,1\}^d} C^{|\omega|} f(x + \omega\cdot h)\right)^{\frac{1}{2^d}}.$$

where C represents conjugation and $|\omega| = \sum_i \omega_i$.

Alternatively, they are defined inductively by

$$\|f\|_{U^1(Z)} = \mathbb{E}|f|^2, \qquad \|f\|_{U^d(Z)} = \left(\mathbb{E}_h \left\|\overline{T^h f} f\right\|_{U^{d-1}}^{2^{d-1}}\right)^{\frac{1}{2^d}}.$$

(To see this definition, note a d-dimensional piped is a union of 2 $d-1$-dimensional ones.)

Define the **Gowers inner product** by

$$\left\langle (f_\omega)_{\omega\in\{0,1\}^d}\right\rangle_{U^d(Z)} = \left(\mathbb{E}_{x\in G}\mathbb{E}_{h\in Z^d} \prod_{\omega\in\{0,1\}^d} C^{|\omega|} f_\omega(x + \omega\cdot h)\right)^{\frac{1}{2^d}}.$$

We have the basic properties:

1. Well-defined: Clear from the recursive definition.

2. Cauchy-Schwarz inequality:

$$|\langle (f_\omega)\rangle_{U^d(Z)}| \le \langle (f_{\omega',0})\rangle_{U^d(Z)}^{\frac{1}{2}} \langle (f_{\omega',1})\rangle_{U^d(Z)}^{\frac{1}{2}} \le \cdots \le \prod_{\omega\in\{0,1\}^d} \|f_\omega\|_{U^d(Z)}.$$

3. Monotonicity formula (from C-S):

$$\|f\|_{U^{d-1}(Z)} \le \|f\|_{U^d(Z)}.$$

4. Triangle inequality (cf. how Minkowski is proved from Hölder): Use Cauchy-Schwarz and binomial expansion.

What does it measure?

1. $\|1_A\|$ is the proportion of d-dimensional cubes in the set. (Note that unlike $d+1$-AP's, we can immediately get a lower bound with the monotonicity formula. Note that a $d+1$-AP is a d-cube with all h_i equal.)

2. "Maximum correlation with polynomials of degree $d-1$." This is true for $d=2$, as $\|f\|_{u^2(Z)} \le \|f\|_{U^2(Z)} \le \|f\|_{u^2(Z)}^{\frac{1}{2}}$. Think of $\|f\|_{u^2(Z)}$ as maximum correlation with a linear phase:

$$\|f\|_{u^2(Z)} = \max_{\chi} \sum_x f(x)\overline{e(xh)}$$
$$\|f\|_{u^d(Z)} = \sup_{\deg\phi\le d} |\langle f, e(\phi)\rangle_{L^2(Z)}|$$

This is **polynomial bias**. We have $\|f\|_{u^d} \le \|f\|_{U^d}$. Note that applying a U^d norm to $e(P(x))$ in effect "differences" P d times; we get an expected value over $e(\Delta_{h_1}\cdots\Delta_{h_d}P)$. (The $\overline{T^h f}f$ is like differencing except multiplied; it becomes an actual difference in the exponent if $f=e(g)$.)

- Baby example (Green, Lemma 7.9): If $f:\mathbb{Z}\to\mathbb{C}$ is a function with $|f(x)|\le 1$ for all x and $\|f\|_{U^d}$, then $f(x)=e(\phi(x))$ for some polynomial ϕ of degree at most $d-1$.
- Unfortunately, polynomial bias implies lack of uniformity, but not the other way around. Obstructions could be more local.

3. Intuition for $d=2$: we have $\|f\|_{U^2} = \left\|\widehat{f}\right\|_{l^4}$ (which gives the above).

So measuring AP's of length $d+1$ is related to U^d is related to correlation with polys of degree $d-1$.

Step 2: Estimate for Λ_k. Van der Corput lemma replaces the task of bounding a sum of coefficients by that of bounding an a sum of "differenced" coefficients. Use it and induction to get a generalized von Neumann theorem for Λ_k (TV 11.4) or to get a generalized von

Neumann for $\|\bullet\|$ directly (more technical, GT). "One U^{k-1}-uniform function makes Λ_k small, i.e., few 'AP's' in f."

This gives the dichotomy (Green 7.8): A looks random or it has structure: $k-1$ norm at lesat η.

Basic steps:

1. A dichotomy between structure and randomness: either A is random in the sense of having close to the expected number of 4-AP's, or it is quadratically not uniform, $\|f\|_{U^3} \ge \alpha$.

   This uses the von Neumann inequality.

2. So what can we conclude from $\|f\|_{U_3} \ge \alpha$? In the case of 3-AP's, U_2, we immediately have a large Fourier coefficient, i.e. linear bias. Here we don't get correlation with a quadratic function globally, but rather locally.

   (a) First, using $\|f\|_{U^3} = \left(\mathbb{E}_h \left\|\overline{T^h f} f\right\|_{U^2}^4\right)^{\frac{1}{8}}$, we get that the $\|\cdots\|_{U^2}$ is large for many values of h. For U^2 we can rewrite the norm as the ℓ^4 norm of the Fourier transform, so this tells gives us a function ϕ such that $\sum_{k\in B} |\widehat{\Delta(f;k)}(\phi(k))|^2$ is large. (Lemma 7.7)

   (b) But then ϕ must have lots of additive quadruples (L7.8 or Pr.9), and Balog-Szemerédi shows ϕ is linear on a (power-)large progression (L7.9).

   (c) So we have that *the linear bias of* $\Delta(f;k)$ *is large* changes *linearly* with respect to k on this progression, so it makes sense for there to be quadratic bias for f. This gives quadratic bias after partitioning into progressions (L. 7.10).

3. Using the inverse result. We need quadratic bias on progressions to give 1_A being large on a subprogression. Recall how we did it for 3-AP's: given $\sum s_i$, if we want to find a sub-sum where the sum is large in absolute value, we show we can divide the sum into sums on progressions where $\arg(s_i)$ doesn't change too much, so we can lower-bound $\sum_k \left|\sum_{P_k}\right|$. Thus we want progressions on which a quadratic function doesn't change too much: use Weyl equidistribution to control the quadratic term. It's a $\varepsilon = \frac{\varepsilon}{2} + \frac{\varepsilon}{2}$ argument.

4. Now finish using density increment.

Step 3: Inverse theorem

Theorem 9.4.22 (Local inverse theorem)**:** Suppose $\|A\|_{U^3} \ge \delta$. Can divide into progressions

$$\sum_{k=1}^{n} \left| \sum_{x\in P_k} f(x) e(-\phi_k(x)) \right| \ge C_3(\delta N)$$

where $\deg \phi_k \le 2$. We require:

1. The progressions are long $\ge C_2(N,\delta) \to \infty$ as $N \to \infty$. Can take $N^{\delta^{C_d}}$.

2. This holds for N sufficiently large, $N > C_1(\delta)$. Here we can take $e^{1/\delta^{C_d}}$.

To look at: `http://link.springer.com/book/10.1007/978-3-642-14444-8` On Szemeredi.

Reading Gowers's original paper.

1. Estabilishing equivalences. 1. ℓ^4, L^∞, U^2 norm, inner product. 2. U^3 norm in 2 ways, $\forall_{-c_3^2 N}(k, r)$, $\forall_{-c_4 N} k, \Delta(f; k)$ c_4-uniform.

4.4 Example sheet 2

1. Suppose we want a set of size k. (We define fourier coefficients as sums.) We expect with high probability,

   $$|\hat{A}(r)| = \left|\sum_{x\in A} \omega^{-rx}\right| \le C \ln k\sqrt{k}$$

   for all $|r| \le k$.

   Take each point and expand it into an interval. Consider $A + I = \bigcup_{x\in A} x + I$, where $|A| = k$ and $I = \left[-\frac{cn}{k^2}, \frac{cn}{k^2}\right]$. We know the coefficients of $A * I$ are $\hat{A}(r)\hat{I}(r)$. Either way this expression is small.

   We know $\max_{r\ne 0} |\hat{A}(r)| \le c\delta^2 N$ implies $A*A$ is approximately constant, and $\max_{r\ne 0} |\hat{A}(r)| \le c \ln \frac{1}{\delta}\delta^2 N$. Convolution $A * A * I * I$, $I * I$ is like an interval of double the length, $A * A$ is like a random k^2 points. It can't fill up. It's 0 most of the time! Try a small random set with an interval, and mess with the parameters.

2. Define a formal Dirichlet series as

   $$\sum_{n=1}^{\infty} f(n) n^{-s}$$

   using the relations $(mn)^{-s} = m^{-s}n^{-s}$ for multiplication. They form a ring.

   (a) Let $f(n)$ correspond to the Dirichlet generating function $F = \sum_n f(n)n^{-s}$. Then $f * g$ corresponds to FG. Commutativity, associativity, and distributivity follow immediately.

   (b) Note $\frac{1}{\zeta} = \prod_p (1 - p^{-s}) = \sum_n \mu(n)n^{-s}$ formally. We have

   $$\begin{aligned} g(x) &= \sum_{d|x} f(d) & \iff && G &= F\zeta \\ f(x) &= \sum_{d|x} f(x) g\left(\frac{x}{d}\right) & \iff && F &= G\frac{1}{\zeta} \end{aligned}$$

   (c) Uniqueness of inverse follows formally: if a_1, a_2 are inverses to a in a semigroup, then $a_1 = a_1 a a_2 = a_2$.

   To find the inverse we need to solve $\sum_d g(n) f\left(\frac{n}{d}\right) = (n = 1)$ which can be solved for $g(n)$ whenever $f(1) \ne 0$.

(d) We have $\mu * L$ corresponds to

$$\frac{1}{\zeta}\frac{d}{ds}\zeta = \frac{d}{ds}(\ln\zeta) = \sum_n -\Lambda(n)n^{-s}$$

so $\mu * L = -\Lambda$.

(e) We have $\sum_{d|x}\frac{\mu(d)}{d}$ corresponds to

$$\begin{aligned}\frac{\zeta(s+1)}{\zeta(s)} &= \prod_p \frac{1-p^{-s}}{1-p^{-(s+1)}}\\ &= \prod_n \left(1+\frac{(p-1)p^{-(s+1)}}{1-p^{-s}}\right)\\ &= \prod_n \left(1+\frac{p-1}{p}(p^{-s}+p^{-2s}+\cdots)\right)\end{aligned}$$

which corresponds back to $\frac{\varphi(n)}{n}$.

3. WLOG $rd < N$. Let $a_1 = \left\lceil \frac{N}{rd} \right\rceil$. Consider the 2-GAP with differences rd and a_1rd mod d.

4. Note $\Delta_{n-1}x^n = n!x + c$ for some c, so $2^{n-1}+c$ works.

5. Average the square over h.

6. The idea is as follows. (a) Show that the number of $(1-\varepsilon_1)$-popular differences is large. (b) Show that if we consider the graph G with edges (a,b) where $a-b$ is a popular difference, then this graph is $(1-\varepsilon_2)$-dense. (c) Show G^2 (G after "completing triangles") contains a complete $K_{(1-\varepsilon_3)n}$. (d) Show that we can take this as our subset.

For ease of notation, let $\varepsilon = \frac{1}{1000}$.

(a) Define a α-popular difference to be d such that there are at least αn^2 pairs $a, b \in X$ with $a - b = d$.

Let the numbers in $X - X$ be d_i.

The d_i satisfy

$$\text{ac6-1}\sum d_i^2 \ge (1-\varepsilon)n^3 \tag{9.8}$$

$$\text{ac6-2}\sum d_i = n^2 \tag{9.9}$$

$$d_i \le n. \tag{9.10}$$

Choose $\varepsilon_1 > \varepsilon$ and let p be the number of $(1-\varepsilon_1)$-popular differences. Then

$$\begin{aligned}
(1-\varepsilon_1)n^3 &\le \sum_{d_i \text{ popular}} d_i^2 + \sum_{d_i \text{ unpopular}} d_i^2 \\
&\le pn^2 + \max_{d_i \text{ unpopular}} d_i \sum_{d_i \text{ unpopular}} d_i \\
&= pn^2 + \max_{d_i \text{ unpopular}} d_i \left(n^2 - \sum_{d_i \text{ popular}} d_i \right) \\
&\le pn^2 + (1-\varepsilon_1)(n^2 - pn(1-\varepsilon)) \\
\implies (\varepsilon_1 - \varepsilon)n^3 &\le pn^2(1-(1-\varepsilon)(1-\varepsilon_1)) \\
\implies (1-\varepsilon_2)n &\le p, \qquad\qquad \varepsilon_2 := \frac{2\varepsilon - \varepsilon_1\varepsilon}{\varepsilon_1 + \varepsilon - \varepsilon_1\varepsilon} \to 0 \text{ as } \frac{\varepsilon}{\varepsilon_1}, \varepsilon_1 \to 0.
\end{aligned}$$

(b) Let $\mathcal{G}$ be a directed graph with vertex set X and (a,b) a directed edge if $b-a$ is a popular difference. (We include edges (a,a) for simplicity of counting, so there are at most n^2 edges.) Then $\mathcal{G}$ has at least $(1-\varepsilon_2)n(1-\varepsilon_1)n$ edges.

(c) Let $d_G(a,b)$ denote the distance between a and b on the graph $\mathcal{G}$.

Claim 1: If d_1, d_2 are $(1-\delta)$-popular, then $d_2 - d_1$ is $(1-2\delta)$ popular. Thus, if (a,b) and (a,c) are edges, then $b-c$ is $(1-2\delta)$-popular.

Proof: The idea is that since we're in a group, we have a kind of homogeneity. Note that there are at least $(1-\delta)n$ values of a' such that $b'-a' = d_1$ for some $b' \in X$, and ditto for d_2. Thus by inclusion-exclusion, there are at least $(1-2\delta)n$ values of a' so that $b'-a' = d_1, c'-a' = d_2$ for some $b', c' \in X$.

Claim 2: If a,b are in the same connected component, then $b-a$ is $(1-2\varepsilon_1)$-popular.

Suppose otherwise. Then by the above, $d_G(a,b) \ge 3$. Take the counterexample such that $d_G(a,b) = k$ is smallest; suppose the shortest path between them is $a_0 \ldots a_k$. Then by the minimality assumption, $a_{k-1} - a_0$ is $(1-2\varepsilon_1)$-popular, so $d := a_k - a_0$ is $(1-4\varepsilon_1)$-popular. Now given any a,b with $b-a=d$, $d_G(a,b) > 2$ because otherwise it is $(1-2\varepsilon_1)$-popular. Let's consider an undirected graph $\mathcal{H}$ with vertex set X and with edges (a,b) with $b-a=d$. Note that a can only be adjacent to $a \pm d$, so that each vertex has degree at most 2, it is a disjoint union of paths and cycles, and $\mathcal{H}$ has at least $\frac{1}{3}(1-4\varepsilon_1)n$ disjoint edges, say (b_i, c_i). Now $d_G(b_i, c_i) > 2$ since d is not $(1-2\varepsilon_1)$-popular. However, this means that $N(b_i), N(c_i)$ are disjoint, and there are many non-neighbors $|N(b_i)^c \cup N(c_i)^c| \ge n$. Now

$$\bigcup_i |N(b_i)^c \cup N(c_i)^c| < \frac{1}{3}(1-4\varepsilon_1)n \cdot n,$$

so there are at least $\frac{1}{6}(1-4\varepsilon_1)n^2$ edges not in G. This is a contradiction if

$$\left[(1-\varepsilon_1)(1-\varepsilon_2) + \frac{1}{6}(1-4\varepsilon_1)\right] n^2 > 1.$$

This finishes the proof of the claim.

Now this shows that for all a, b, $d_G(a,b) \leq 2$ or $d_G(a,b) = \infty$. Thus the graph G^2 obtained by "completing all triangles with 2 edges in G" is a union of disjoint complete graphs. If the largest component has size $(1-\delta)n$, then the number of edges is at most $[(1-\delta)^2 + \delta^2]n^2$, so letting ε_3 be such that

$$(1-\varepsilon_3)^2 + \varepsilon_3^2 = (1-\varepsilon_1)(1-\varepsilon_2),$$

we see $\delta \leq \varepsilon_3$.

(d) Take the largest component, say X', and consider the coset generated by it, i.e., $C = X' + \langle a - b \mid a, b \in X' \rangle$. Note that if d_1, d_2 are popular, then there exist $(a,b), (a,c)$ with $b - a = d_1, a - c = d_2$ again by the PIE argument, so $d_1 + d_2$ is popular. By this "closure" property, we get that for any $a, b \in C$, $b - a$ is a popular difference in X. But there are at most $\frac{n}{1-\varepsilon_1}$ popular differences, so $|C| < \frac{n}{1-\varepsilon_1}$.

Now we just need to choose the ε_j's so that $\frac{1}{1-\varepsilon_1} < \frac{11}{10}$ and $1 - \varepsilon_3 > \frac{1}{9}10$. Omitted.

Can we identify the subgroup? Look at differences between elements of X. Defining

$$D_\eta = \{d : \eta = \text{almost every } x \in X, x + d \in X\},$$

for η-almost x, $x + d_1 \in D$, for η-almost y, $y + d_2 \in D$. We've shown $D_{2\eta} \subseteq D_\eta$. We claim that whenever difference represented a lot of the time, then represented all of the time. Suppose α is a lot bigger than η, $x + d \in X$ for at least αn values of x. Pick y, ε-almost y, $y - x$ is represented $(1-\varepsilon)n$ times, and $y - (x+d)$ is represented $\geq (1-\varepsilon)n$ times.

Now for ε-many x, ε-almost every y, $y - x$ is represented $\geq (1-\varepsilon)n$ times, $y - (x+d)$ is represented $\geq (1-\varepsilon)n$ times.

For 2ε-almost every $w \in X$, $w + y - x \in X$, $w + y - (x+d) \in X$. We boosted it! We showed $D_{1-\alpha} \supseteq D_{2\eta}$. Slightly popular implies very popular.

7. Why is this an extension of Roth's theorem? Because if $A \subseteq [n]$ and $|A| \geq \delta N$, then $A + A \subseteq [2n]$ and hence $|A + A| \leq \frac{2}{\delta}|A|$.

   If $|A| \geq n$ and $|A + A| \leq C|A|$, then by Plünnecke's inequality $|2A - 2A| \leq C^4|A|$ so by Ruzsa's lemma there is $|A'| \geq \frac{|A|}{2}$ that is 2-isomorphic to a subset $B \subseteq \mathbb{Z}/N$, with $N \leq C|A|$. 2-isomorphism means 3-AP's in A' correspond to 3-AP's in B. Now apply normal Roth's Theorem to $|B| \geq \frac{C^4|A|}{2}$ inside $\mathbb{Z}/N$ with $N \leq C|A|$.

8. Cauchy-Schwarz. $\mu_i(A \wedge (A + r)) = \alpha_r$. $\mathbb{E}\alpha_r = \delta^2$. Cubes inside by induction is at least $\alpha_r^{2^{k-1}} N^k$.

   (b) $\langle f_1, \ldots, f_8 \rangle_{U^3} \leq \min_i \|f_i\|_{U^3}, \|f_i\|_\infty \leq 1$. (actually product) Key result: $\mathbb{E}_x f(x)f(x+d)f(x+2d)f(x+3d)$ bounded by U_3.

   We can write $A = \delta + f$, $\|f\|_{U^3}$ is small.

   We get $\mathbb{E}_{x,a,b,c}(\delta + f(x))(\delta + \cdots)$. Product of 16 terms. δ^8, others occurence of f.

9. By Dirichlet's argument, $(r_1x, \dots, r_nx)$, Pigeonhole, $|r_ix - r_iy| < \delta N$

$$|B(r_1, \dots, r_k; \delta)| \geq \frac{N}{\left\lfloor \frac{1}{\delta} \right\rfloor^k} \approx \delta^k N.$$

(some care can probably remove the floor) Note in particular there is a nonzero element when $\delta \gtrsim N^{\frac{1}{k}}$

10. Idea: if we can find a Bohr set inside $A + A + A$ of large radius, then we have a long AP, by the inequality in problem 9, since if $B(R, \varepsilon) \subseteq A + A + A$ and $x \in B(R, \frac{\varepsilon}{n})$, then $x, 2x, \dots, nx \in A + A + A$. Actually we'll have to look at $A + A + A - k$ (which makes sense because the AP may not start at 0!).

We'll copy the proof of Bogolyubov's lemma, noting that we'll fail if we look at $A+A+A$ by the above remark, so we'll apply it for $A+A+A-k$. 3 A's are necessary in order for a bound on the Fourier coefficient to be combinable with the equality $\mathbb{E}_r|\widehat{1_A}(r)|^2 = \delta N$.

Let $R = \left\{r \neq 0 : |\widehat{1}_A(r)| \geq c\right\} = \mathrm{Spec}_{\frac{c}{\delta}}(A)$ (we'll see that any $c = \frac{\delta^2}{2}$ is fine). Then $|R| \leq \frac{2\delta}{c^2}$.

Now

$$\widehat{1}_{A+A+A-k}(x) = \sum_r |\widehat{A}(r)|^2 A(r) e(kr) e\left(\frac{rx}{N}\right)$$

This is

$$\delta^3 + \underbrace{\sum_{r \in R - 0} |\widehat{A}(r)|^2 A(r) e(kr) e\left(\frac{rx}{N}\right)}_{(*)} + \underbrace{\sum_{r \notin R \cup 0} |\widehat{A}(r)|^2 A(r) e(kr) e\left(\frac{rx}{N}\right)}_{|\bullet| \leq c\delta} \overset{?}{>} 0.$$

Try: Get $\Re(*)$ point in a positive direction.

Idea: Sum the sum over k to find one k that works.

But: We want something independent of x though, so we can't include $e\left(\frac{rx}{N}\right)$. Summing over k,

$$\sum_{r \in R - 0} \sum_k |\widehat{A}(r)|^2 A(r) e(kr) = 0$$

Hence we can find k such that $\sum_{r \in R - 0} |\widehat{A}(r)|^2 A(r) e(kr) \geq 0$.

Abstract: If $\Re \sum_{r \in R \setminus 0} a_r \geq 0$ and $x \in B(R, \varepsilon)$ then $\Re \sum_{r \in R \setminus 0} a_r e\left(\frac{rx}{N}\right) \geq -\left(\sum_r |a_r|\right) \cos(2\pi\varepsilon)$. Set $\varepsilon = N^{-\varepsilon_1}$ and we get

$$(*) \geq -\delta \cos(2\pi N^{-\varepsilon_1}).$$

δ, ε_1 is fixed so just pick N large enough for this to be $\geq -\frac{\delta^3}{2}$.

Now by (9) there is a nonzero element in $B(R, N^{-\frac{\delta^3}{8}}) \subseteq A + A + A - k$. So choose $\varepsilon_1 < \frac{\delta^3}{8}$, and we get an AP of length $N^{\frac{\delta^3}{8} - \varepsilon_1}$.

11. Green and Konyagrin

12. Partial summation. $S_m = \sum_{n=1}^{m} b_m$

$$\begin{aligned}
\sum_{n=1}^{N} a_n b_n &= \sum_{n=1}^{N} a_n (S_n - S_{n+1}) \\
&= \sum_{n=1}^{N} a_n S_n - \sum_{n=1}^{N} a_n S_{n-1} \\
&= \sum_{n=1}^{N} a_n S_n - \sum_{n=1}^{N-1} a_{n+1} S_n \\
&= a_N S_N + \sum_{n=1}^{N-1} (a_n - a_{n+1}) S_n \\
&\le |a_N| S + \underbrace{S \sum_{n=1}^{N-1} |a_n - a_{n+1}|}_{S|a_1 - a_N|} .
\end{aligned}$$

$\left|\frac{2}{1-e(\alpha)}\right|$, as long as α not too close to integer. ($S = \max |S_n|$.)

13. This gives an example of a set with small Fourier coefficients that doesn't contain the expected number of progressions of length 4.

Let $I = \left[-\frac{N}{10^4}, \frac{N}{10^4}\right]$, $A(x) = I(x^2)$. We know a lot about the Fourier transform of I: it is a sum of GP's. Then

$$\begin{aligned}
\sum_x I(x^2)\omega^{-rx} &= N^{-1} \sum_s \hat{I}(s) \sum_x \omega^{sx^2 - rx} \\
|\bullet| &\le N^{-1/2} \underbrace{\sum_s |\hat{I}(s)|}_{\le N \ln N} \le N^{\frac{1}{2}} \ln N
\end{aligned}$$

Up to log factor, it's as small as it can possibly be.

Uniform so small number of 3 AP's, extend to 4 AP's.

14.

15. Use compactness.

Given $q \in A$, the set $B_q(\varepsilon) := \{\alpha \in \mathbb{R} : \|q\alpha\| < \varepsilon\}$ is open. These cover $[0,1]$. Thus there is a finite subcover.

16.

$$\begin{aligned}
\eta N^3 &\leq \sum_k |\widehat{\Delta(f;k)}(2\lambda k)|^2 \\
&= \sum_k \left|\sum_x f(x)\overline{f(x-k)}\omega^{-2\lambda k x}\right|^2 \\
&= \sum_k \left|\sum_{x,y} f(x)\overline{f(x-k)f(y)}f(y-k)\omega^{2\lambda k(x-y)}\right| \\
&= \sum_k \sum_{x,u} f(x)\overline{f(x-k)f(x-u)}f(x-k-u)\omega^{-2\lambda k u} \\
&= \sum_{k,x,u} g(x)\overline{g(x-k)g(x-u)}g(x-k-u) \\
&= N^{-1}\sum_r |\hat{g}(r)|^4 \\
&\leq N^{-1}\max_r |\hat{g}(r)|^2 \sum_r |\hat{g}(r)|^2.
\end{aligned}$$

$2ku = x^2-(x-k)^2-(x-u)^2+(x-k-u)^2$. $g(x) = f(x)\omega^{-\lambda x^2}$. We get $\eta^{\frac{1}{2}}N$.

Key idea in Szemeredi: a large Fourier coefficient depends linearly on k. Original things is quadratic... Note $f(x)=\omega^{x^2}$. $\Delta(f;k)(x)=\omega^{2kx+k^2}$.

12-23

	$\widehat{f}$ over $\mathbb{Z}$	f	$\widehat{f}$ over $\mathbb{Z}/N$
Formula	$\widehat{f}(r)=\sum_{n\in\mathbb{Z}} f(n)e(-n\theta)$	$f(n)$	$\widehat{f}(r)=\mathbb{E}_{n\in\mathbb{Z}/N}f(n)e\left(\frac{-nR}{N}\right)$
Convolution	$\widehat{f}\cdot\widehat{\overline{g}}$	$f*g$	$\mathbb{E}_{a+b=r}f(a)\overline{g}(b)$
Norm	$\int_0^1 \widehat{f}(\theta)\overline{\widehat{g}(\theta)}\,d\theta$	$\sum f\overline{g}$	
		$\mathbb{E}fg$	$\sum_{r\in\mathbb{Z}/N}\widehat{f}(r)\overline{\widehat{g}(\theta)}$
Density	$\int_0^1 \lvert\widehat{f}(\theta)\rvert^2\,d\theta=\alpha$	$\sum \lvert f\rvert^2=\alpha N$	$\mathbb{E}\lvert f\rvert^2=\sum\lvert\widehat{f}\rvert^2=\alpha$
3-APs	$\int_0^1 \widehat{f}^2\widehat{f}(-2\theta)\,d\theta=\beta N^2$	$1_A*1_{-2A}*1_A(0)=\beta N^2$	$N^2\sum_{r\in\mathbb{Z}/N}\widehat{f}^2\widehat{f}(-2r)$
4-tuples	$\int_0^1 \lvert\widehat{f}(\theta)\rvert^4\,d\theta=\gamma N^3$	$1_A*1_A*1_{-A}*1_{-A}(0)=\gamma N^3$	$N^3\sum\lvert\widehat{f}(r)\rvert^4$

5 Arithmetic geometry

5.1 Rational points on varieties: Introduction

Major themes of the course are

- rational points on varieties (Diophantine geometry; existence, density, distribution,...)
- Modular forms

Abelian varieties are involved in both themes.
We will keep theorems as simple as possible, and focus on the important ideas.

Diophantine geometry is about studying solutions of polynomials $F_1, \ldots, F_m \in K[x, y, z, \ldots]$ (but 1 polynomial is already a lot of trouble!) when $K = \mathbb{Q}$ or a number field, finite field, functional field...

Algebraic geometry is about studying solutions of polynomials... when K is any field or even commutative algebra. So it is more general than Diophantine geometry.

The focus in the two subjects is different. Still, there are a lot of connections.

Let's consider some examples.

Example 9.5.1: Let $F = x^2 + y^2 \in \mathbb{Q}[x, y]$. The only solution over $\mathbb{Q}$ is $(x, y) = (0, 0)$ because this is the only solution over $\mathbb{R}$. This teaches us an important strategy: we can extend $\mathbb{Q}$ to $\mathbb{R}$ (or another local field) and study solutions there.

Example 9.5.2: Consider $F = x^2 + y^2 - 7z^2 \in \mathbb{Q}[x, y, z]$. The only solution is $(0, 0, 0)$. To see this, suppose (a, b, c) is a solution over $\mathbb{Q}$. We assume $a, b, c \in \mathbb{Z}$. Let's do reduction mod 7. We have

$$\overline{a}^2 + \overline{b}^2 = 0$$

over $\mathbb{F}_7$. Because $\left(\frac{-1}{7}\right) = -1$, this is possible only if $\overline{a} = \overline{b} = 0$, so $a = 7a', b = 7b'$. Then $7 \mid c$ so $c = 7c'$ as well, $c = 7c', a'^2 + b'^2 - 7c'^2 = 0$. Inductively (infinite descent) one can see $a = b = c = 0$. Geometry over $\mathbb{F}_p$ is a lot simpler than over $\mathbb{Q}$.

Example 9.5.3: Let $F = x^5 + y^5 - 7z^5 \in \mathbb{Q}[x, y, z]$. It is unknown whether $(0, 0, 0)$ is the only nonnegative solution.

"Changing the equation a little bit, you can go from paradise to hell."

Example 9.5.4: $F = x^n + y^n - z^n \in \mathbb{Q}[x, y, z]$, $n \geq 3$. This is Fermat's equation.

Example 9.5.5: $F = x^2 + y^2 - z^2 \in \mathbb{Q}[x, y, z]$. F has lots of solutions. In fact for every $m \in \mathbb{Z}$, $(m^2 - 1, 2m, m^2 + 1)$ is a solution.

We generate many solutions using some simple expression. We will see later why equations like this are simple: it is because $X := V(F) \cong \mathbb{P}^1_{\mathbb{Q}}$.

The general set up is the following: K is a field, $X \subseteq \mathbb{P}^n_K$ is a projective variety over K. Let $X = V(f_1, \ldots, f_m)$, $f_1, \ldots, f_m \in K[t_0, \ldots, t_n]$.

Note this could be empty, when X is not trivial. The best way to look at this in terms of schemes, because we look at a ring, not the solution set.

For any field extension $K \subseteq K'$,

$$\begin{aligned} X(K') &= \{\text{rational points over } K'\} \\ &= \{(a_0 : \cdots : a_n) \in \mathbb{R}^n_{K'} : f_i(a_0 : \cdots : a_n) \forall i\}. \end{aligned}$$

The following are natural questions.

1. Is $X(K')$ empty?

2. Is $X(K')$ dense in its Zariski topology? There is also the notion of potential density: if you change the field, is it still dense? (For example, consider closed points $S \subseteq X = \mathbb{P}^1$.

If S is finite, S is not dense; if S is infinite, then S is dense (every closed subset is either finite or the whole space).

3. If $X(K')$ is dense, how are its points distributed?

Consider dimension 1: X is a smooth, projective variety of dimension 1 over a number field K. The most important invariant of X is the genus

$$g = h^0(\omega_X) = h^1(\mathcal{O}_X) = \#\text{holes in } X(\mathbb{C}).$$

Note $X(\mathbb{C})$ is a compact Riemann surface.

In the case $g = 0$, either $X(K) = \phi$ or $X(K)$ is infinite. If $X(K) = \phi$, then $X_{\overline{K}} \cong \mathbb{P}^1_{\overline{K}}$, but maybe $X_K \ncong \mathbb{P}^1_K$.

If $X(K) \neq \phi$, then $X_K \cong \mathbb{P}^1_K$.

When $g = 1$, X is an elliptic curve. This is already hard; for example, the BSD conjecture is about rational points on the curve. Either $X(K)$ has "few" points (universally bounded, bound depending on the field, not the curve), or $X(K)$ has infinitely many points. $X(K)$ is a group.

When $g \geq 2$, $X(K)$ is finite (Faltings). Letting ω_X be the canonical bundle,

1. $g = 0 \implies \omega_X$ is antiample (negative).

2. $g = 1 \implies \omega_X$ is trivial (zero).

3. $g \geq 2 \implies \omega_X$ is ample (positive).

"Geometry determines arithmetic."

In higher dimension there are 2 classes of varieties where this question is well-understood.

1. varieties close to projective spaces.

2. abelian varieties (this is the best understood case, for example we have the Mordell-Weil Theorem).

We can also build up from these well-understood varieties (for example, a variety whose fibers over a projective space are abelian varieties).

Conjecture 9.5.6 (Lang, Campana)**:** Let X is smooth projective over a number field K.

(Lang) If ω_X is ample, then $X(K)$ is not dense.

(Campana) If $\omega_X \cong \mathcal{O}_X$ or ω_C is anti-ample, then $X(K')$ is dense for some finite extension $K \subseteq K'$.

Example 9.5.7: Suppose $X = V(f) \subseteq \mathbb{P}^n_K$, $d = \deg f$.

Then

- ω_X is ample iff $d > n + 1$
- $\omega_X \cong \mathcal{O}_X$ iff $d = n + 1$.
- ω_X is anti-ample iff $d < n + 1$.

Even in this case the conjecture is open.

General strategies: Let X be a smooth projective variety over $\mathbb{Q}$.

1. We can look at $X(\mathbb{Q}) \subseteq X(\mathbb{R})$. This is real manifold, so we have a set of tools coming from differential geometry.

2. $X(\mathbb{Q}) \dashrightarrow X(\mathbb{F}_p)$. (Use the Weil conjectures to relate to $X(\mathbb{F}_{p^r})$.

3. $X(\mathbb{Q}) \subseteq X(\overline{\mathbb{Q}})$. In terms of algebraic closure this is simpler. This involves Galois groups $G(\overline{\mathbb{Q}}/\mathbb{Q})$. The points $X(\mathbb{Q})$ can be characterized as points $X(\overline{\mathbb{Q}})$ invariant under Galois action.

There are nice cohomology relations $H^i(X(\mathbb{C}), \mathbb{C})$ between $X(\mathbb{C})$ and $X(\mathbb{F}_{p^r})$. (Weil conjectures)

There is no guarantee!

6 Algebraic methods in incidence theory

6.1 Example sheet 1

1.

2.

3. The density of sum-of-squares is $O\left(\frac{n}{\sqrt{\ln n}}\right)$. Consider the points $[0, n]^2$ and circles centered at these points with at least 1 lattice point. We get N points and $\frac{N^2}{\sqrt{\ln N}}$ circles ($N \sim n^2$).

   Where did we use the fact the radii are equal? Given 2 points, at most 2 circles can intersect at the 2 points. In a cell we had $N^{\frac{1}{3}}$ points and $N^{\frac{2}{3}}$ circles after optimizing $D = N^{\frac{1}{3}}$.

4. See 18.318 ex. 1.8.

   Strongest argument in favor of 1 (but false): Like circles because we have a degree 2 curve. 2: Like lines because we have the example. Look for an example that says parabolas are like lines.

   This works for $y = x^n$. What if you have other curves, translates of $f(x, y) = 0$? This is not well-understood.

5.

6.

7.

8. Idea: Put all the points close together. 2 close-together circles intersect in 2 points, but two nearby annuli can intersect in lots of points.

   Consider points that are at least a distance δ apart.

   This kind of fattening makes the Kakeya problem harder in $\mathbb{R}^n$ than over finite fields.

Chapter 10

Index cards

1 Directory of current index cards

1.1 Algebra

1. SU_2, SO_3 (11-5-13)

1.2 Analysis

1. Fourier analysis (basics) (10-21-13)
2. Hilbert spaces and fourier series (10-21-13)
3. Functional analysis (Stein and Shakarchi Ch. 1)
4. Functional analysis (course, Ch. 1) [FA]
5. Functional analysis (course, Ch. 2) [FA] (10-31-13)
6. Weak topologies 1 [FA4.1] (11-17-13)
7. Weak topologies 2 [FA4.2] (11-17-13)
8. Krein-Milman Theorem [FA5] (11-20-13)

1.3 Applied

1. Linear programming
2. Mathematical biology
3. Wavelets

1.4 Combinatorics

1. Hales-Jewett and van der Waerden [Ramsey Theory, Arithmetic Combinatorics]
2. Roth's Theorem [AC]
3. Rado's Theorem [RT] (11-15-13)

1.5 Computation

1. Entropy [QIT]
2. Quantum entropy [QIT]

1.6 Numerical analysis

1. The flying trapezium rule (Nick Trefethen's talk) (11-1-13)

1.7 Number theory

1. Kummer Theory (11-17-13)
2. Elliptic curves over local fields (11-17-13)

1.8 Probability

1. Shuffling cards (talk, 11-22-13)

2 To make

2.1 Algebra

1. Homological algebra
2. Yoneda's lemma

2.2 Analysis

1. Other chapters of Stein, Shakarchi
2. PROBABILITY

2.3 Applied

1. Classical information theory (2)
2. QIT: math tools, axioms
3. QIT: distances
4. QIT: measurements
5. BIOPHYSICS

2.4 Combinatorics

1. Ramsey's Theorem

2.5 Geometry

1. Differential geometry of curves
2. 18.965 material

2.6 Number theory

1. Weyl equidistribution
2. Freiman's Theorem
3. Class field theory (several index cards!)

Chapter 11

Questions

1 Interesting questions

Combinatorics

1. 18.821 Project II: sequences avoiding solutions to certain equations. Hypothesize: it has a nice structure iff it's partition regular? @imre

2. What happens when we avoid higher-degree equations? @imre

2 Research questions

3 Things I'm interested in

Too vague to make interesting questions yet at this point.

Big things: ((FF) means far-fetched.)

1. What Strogatz has done with small-world networks. How can we characterize in an abstract and simple way the way that the following are organized (and the way they evolve)?

   (a) neurons in the brain

   (b) the web of knowledge, specifically, mathematical theorems (cf. Jacob's math friend)

   Related stuff

   (a) Graph theoretic ideas of order and disorder, ex. optimal bounds for Szemeredi's Theorem. Are there more flexible versions of these kinds of theorems for certain families of graphs, for example graphs of knowledge above?

   (b) defining metrics

2. Mathematical formulations of complexity, intelligence and information (Kolmogorov complexity, AIXI, "consciousness," machine learning, etc.). In particular, defining complexity (see scholarpedia article).

   (a) Theoretical computer science: computational complexity, P vs. NP, etc. How far does "philosophy" go into this?

   (b) Can we define complexity for something like cellular automata?

   (c) Mathematical theorem proving. Representing mathematical knowledge in useful form. (ex. analogies, parallels between different arguments.

   (d) Information compression. The Hutter prize.

   (e) Defining layers. Programs on several levels. Are genes the same way?

   (f) (FF) Is there a way to characterize what makes a good story mathematically? How to fit some part into another, as in Genesis? Better math than PCA for ConceptNet? (Tensor products??)

3. Open problems that are cool and simply stated (and that probably don't require the kind of machinery that hard number theory problems typically require), Erdős-like problems.

   (a) `http://www.openproblemgarden.org/op/limiting_subsequence_sums_in_z_n_x_z_n`, `http://www.openproblemgarden.org/op/quartic_rationally_derived_polynomials` `http://www.openproblemgarden.org/op/a_discrete_iteration_related_to_pierce_expansions` `http://www.openproblemgarden.org/op/snevilys_conjecture` `http://en.wikipedia.org/wiki/Erd%C5%91s_conjecture` `http://en.wikipedia.org/wiki/Erd%C5%91s%E2%80%93Straus_conjecture#CITEREFElsholtzTao2011` `http://www.openproblemgarden.org/op/erdos_faber_lovasz_conjecture` `http://www.math.ucsd.edu/~erdosproblems/All.html`

4. Randomness in arithmetic.

   (a) Arithmetic dynamics.

   (b) Questions of equidistribution in number theory.

   (c) Additive combinatorics. Randomness and structure.

5. The kind of stuff Diaconis does: a way of doing applied math by asking lots of questions, talking to people, browsing. Ex. dynamics of card-shuffling.

Fuzzy

`http://statweb.stanford.edu/~cgates/PERSI/papers/scho1.pdf` Convolution ↔ group expansion? `http://statweb.stanford.edu/~cgates/PERSI/Courses/Phil166-266/index.html`

Chapter 12

To read

1. Stuff on complexity

   (a) http://www.scholarpedia.org/article/Algorithmic_information_theory

   (b) http://www.scholarpedia.org/article/Neuroanatomy

2. P vs. NP, Borel determinacy

3. Randomness in number theory

   (a) equidistribution, thin groups, Ramanujan graphs in number theory, quantum arithmetic chaos. Peter Sarnak's stuff.

4. Elementary number theory:

   (a) http://en.wikipedia.org/wiki/Pythagorean_triple#Parent.2Fchild_relationships

   (b) Continued fractions

5. Number theory

   (a) Tate's Thesis

   (b) http://mathoverflow.net/questions/52576/zeta-function-zero-density-theorems

   (c) Transcendental number theory

6. Cool!

   (a) Persi Diaconis's paper

7. Connections

   (a) Stats: on the computability properties of finding the right sparse vector

   (b) Functional analysis and quantum mechanics http://www.physicsforums.com/showthread.php?t=

8. Books

   (a) An epsilon of room.

   (b) Kolmogorov complexity

   (c) Nonlinear dynamics and chaos, Strogatz.

General:

- http://terrytao.wordpress.com/
- http://blog.scholarpedia.org/2013/11/04/wikifying-scholarly-canons/
- http://jhnpappas.wordpress.com/

Index