Welcome to Algebraic-Geometric Codes!

Fall 2024/5

Gil Cohen

October 30, 2024

Overview

What is this course about?

This course is about a construction of certain error correcting codes known as Goppa Codes or Algebraic Geometric Codes.

These super beautiful and elegant codes beat the parameters of codes obtained via the probabilistic method (namely, the Gilbert-Varshamov bound) in interesting regime of parameters - an extremely rare phenomena.

But before we start, some technicalities.

About us

I am a theoretical computer scientist working mostly within

1. Complexity theory, especially randomness related questions
2. Pseudorandomness & explicit constructions
3. Coding theory
4. Spectral graph theory

Tomer, your TA, is my PhD student, working mostly within AG codes.

Overview

Course mechanics

Meetings

1. We meet in person on Wednesdays from 10:00 to 13:00 in Shenkar-Physics 204.
2. Tomer's recitations take place on Wednesdays from 14:00 to 15:00 in the Melamed Auditorium, Room 006.
3. I am happy to meet upon request to discuss the material and problem sets.
4. Lectures and recitations will be recorded in English; however, I expect in-person attendance. Please note that a Zoom option will not be available.

Homepage & Contact

1. The course homepage: `www.gilcohen.org/2024-agc`.
2. My email: `coheng@gmail.com`.
3. Tomer's email: `tomermanket@mail.tau.ac.il`.

Course mechanics

Grade

The grade will be determined as follows: Half of the grade will be based on a one-hour presentation by each student at the end of the semester, covering topics not discussed in lectures or recitations. The other half will be based on homework assignments, submitted in pairs throughout the semester. We expect to publish about 5 assignments. Only selected questions will be graded, and the overall grade will be determined by these alone.

Course mechanics

Literature & notes

The course will be taught on the blackboard. I will follow lecture notes, which will be published on the course homepage before each class. As we won't be able to prove everything in detail, due to time constraints, some of the more technical or less insightful proofs will be left for you to review in the notes, if you wish. I may record additional videos for some of the selected proofs that are omitted.

The notes are mostly based on

- Dan Haran's lecture notes for the first $\approx \frac{2}{3}$ of the course.
- Stichtenoth's book: Algebraic Function Fields and Codes.

There are several other books we will not be following directly. Please refer to the course homepage for additional information.

Course mechanics

Prerequisites

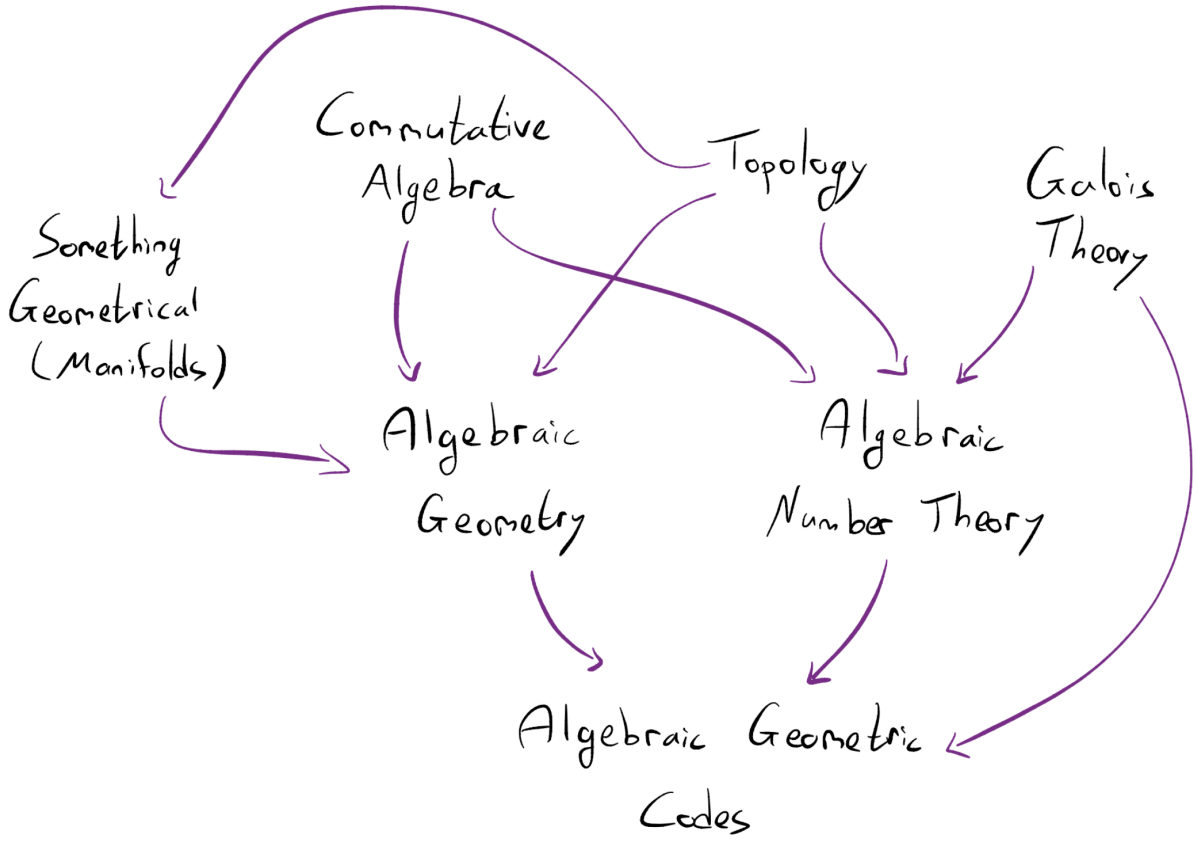
Despite the course's title, you do not need prior knowledge of coding theory or algebraic geometry. However, by the end of the course, you still won't be an expert in coding theory or algebraic geometry! :)

This is primarily a course in pure mathematics with an algebraic focus. A basic understanding of groups, rings, and fields is assumed. Starting from mid-semester, we will also be using Galois Theory.

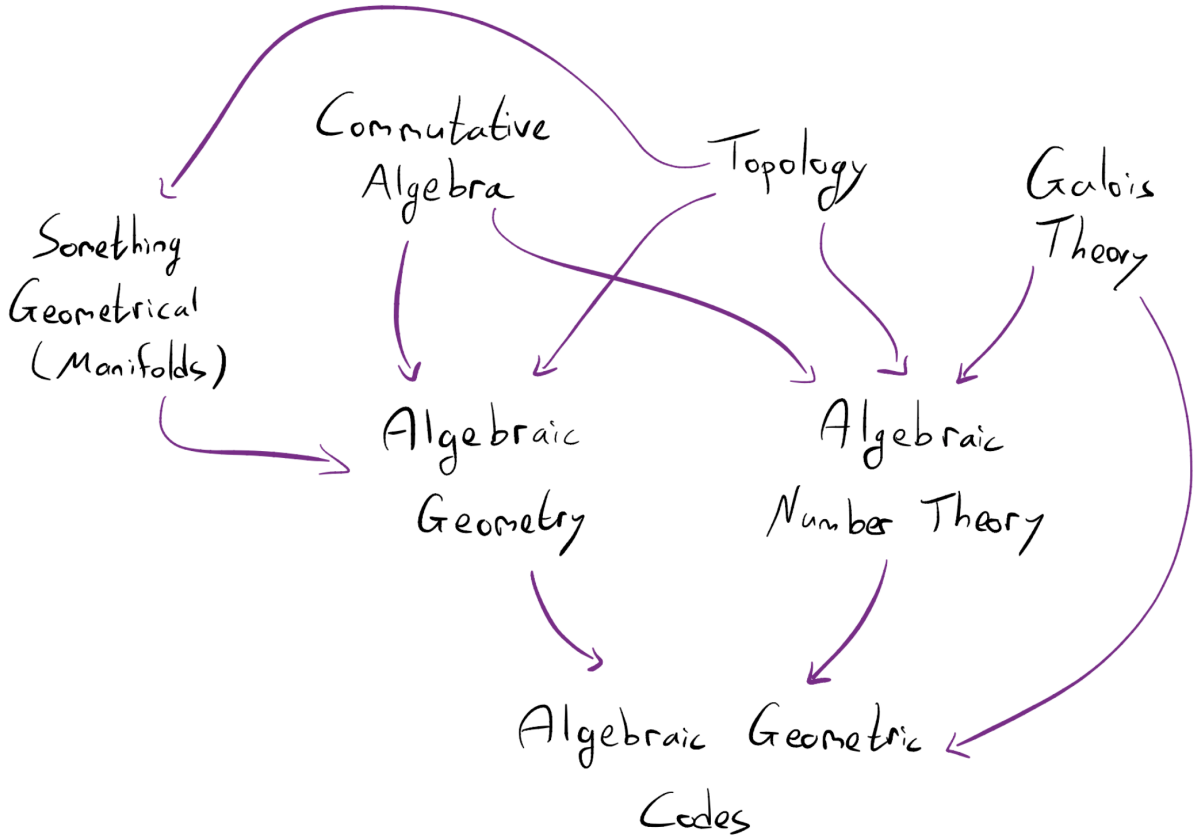
Overview

More on prerequisites

Polynomials and similar structures are extremely useful in theoretical computer science (TCS), and the underlying mathematics of AG codes is much deeper and more powerful than what is typically used in TCS. By this logic, the theory should have further applications. The challenge, however, lies in the steep learning curve for those with a typical TCS background.



More on prerequisites



Our approach will be algebraic—faster and more powerful, but also more abstract and less intuitive. I will informally introduce the geometric (and number-theoretic) concepts and provide insights into the broader context within commutative algebra.

Overview

How do we proceed?

A quick and dirty introduction to coding theory

The basics of the theory

- Abstracting the notion of a point on a curve
- Function fields

  ⋮

- Riemann's Theorem (1857) and the genus

Goppa codes

How do we proceed?

Going deeper for explicit code constructions

- The Riemann-Roch Theorem (1865).
- Function field extensions (here is were Galois theory will come in).
- Proof of The Riemann Hypothesis for curves over finite fields (raised by Artin (1924); proved by Hasse for genus 1 and Weil (1949) for the general case).

  ⋮

- Construction of AG codes

[8] As to this, cf. H. Hasse, J. Reine Angew. Math. vol. 172 (1935) pp. 37–54. I regret that I did not quote either of these papers, where the connection between various kinds of exponential sums and the Riemann hypothesis is quite clearly expressed, in my recent note on the same subject, Proc. Nat. Acad. Sci. U.S.A. vol. 34 (1948) pp. 204–207.

Figure: A footnote from Weil's paper.

Overview

Goppa's paper

Доклады Академии наук СССР
1981. Том 259, № 6

УДК 519.46 МАТЕМАТИКА

В.Д. ГОППА

КОДЫ НА АЛГЕБРАИЧЕСКИХ КРИВЫХ

(Представлено академиком А.А. Дородницыным 23 II 1981)

1. Конструкция кода. Пусть E^n – векторное пространство размерности n над конечным полем F_q, C – проективная кривая рода g над F_q, $P_1, P_2, \ldots, P_n$ – различные точки кривой C, рациональные над F_q, $D = \Sigma P_i$, $G = \Sigma m_Q Q$ – два эффективных дивизора, причем G рационален над F_q, так что вместе с $m_Q Q$ содержит сопряженную точку $m_Q(\sigma Q)$, если Q принадлежит некоторому расширению поля F_q. Предполагается, что носители обоих дивизоров не пересекаются. Через $\Omega(G - D)$ обозначим как обычно пространство дифференциалов таких, что $(\omega) \geqslant G - D$. Введем линейный корректирующий код [1] посредством отображения

$$\Omega(G - D) \xrightarrow{\varphi} E^n,$$

$$\varphi: \ \omega \to (\mathrm{Res}_{P_1}(\omega), \mathrm{Res}_{P_2}(\omega), \ldots, \mathrm{Res}_{P_n}(\omega)).$$

Образ $U = \mathrm{Im}(\varphi)$ назовем (D, G)-кодом рода g степени $\deg G$.

Goppa's paper

2. Оценка параметров. Кодовое расстояние d и число проверочных символов r оцениваются с помощью теоремы Римана–Роха:

$$d \geqslant \deg G - 2g + 2,$$

$$r \leqslant d + g - 1.$$

Для длины кода известна оценка Хассе–Вейля:

$$|n - (q+1)| \leqslant 2g\sqrt{q}.$$

Лучшие параметры кода получаются для кривых, на которых достигается верхняя граница:

$$n = q + 1 + 2g\sqrt{q}.$$

3. Пример кода. Рассмотрим эллиптическую кривую $x^3 + y^3 + z^3$ над полем $F_4 = \{0, 1, \alpha, \beta\}$. Эта кривая — известная ангармоническая кубика с 9 точками, каждая из которых является флексом (имеет тройную касательную):

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9
x	1	0	α	1	0	β	0	α	1
y	0	1	0	1	α	0	β	1	α
z	1	1	1	0	1	1	1	0	0

Все 9 точек образуют абелеву группу типа $Z/(3) \times Z/(3)$. В качестве дивизора G выберем цикл пересечения кривой с коникой $xy + yz + zx = 0$. По теореме Безу

Goppa's paper

deg $G = 6$, поэтому $d = 6$, $r = 6$. Порождающая матрица кода имеет вид

$$\begin{pmatrix} 1 & 0 & 0 & \alpha & \alpha & \beta & 0 & \beta & 1 \\ 0 & 1 & 0 & \alpha & \beta & 0 & 1 & \beta & \alpha \\ 0 & 0 & 1 & 0 & 1 & \alpha & 1 & 1 & \alpha \end{pmatrix}.$$

Тот же самый (D, G)-код над полем F_{64} имеет параметры $n = 81$, $r = 6$, $d = 6$.

Поскольку сумма вычетов дифференциала равна 0, для всех кодовых слов сумма координат равна 0.

4. Двоичные коды. Наибольший практический интерес представляют двоичные коды. Такие коды получаются, если в описанной конструкции положить $q = 2^m$, а затем перейти к подкоду над подполем F_2:

$$n = 2^m + 1 + 2g\sqrt{2^m},$$

$$d \geqslant 2t + 2,$$

$$r \leqslant m(t + g - i) + 1.$$

Здесь m четно, $G = 2G'$, $\deg G' = t + g$, i — индекс специальности дивизора G'.

При малых длинах n лучшими оказываются коды на рациональных кривых, а при больших n — коды на кривых большого рода. Например, кривые Эрмита [2] имеют $n = 1 + 2^{3m/2}$ точек, рациональных над F_{2^m}. Род этих кривых равен $g = 2^{m-1} - 2^{m/2-1}$. Соответствующие коды веса $d \geqslant 2t + 2$ имеют $r < t \log n$ проверочных символов при всех $t > 2g = 2^m - 2^{m/2}$, причем разность $\Delta = t \log n - r \geqslant m(t/2 - g)$.

Пример. $m = 8$, $n = 4097$, $t = 250$, $d \geqslant 502$, $r \leqslant 2961$. Если $g \sim q = 2^m$, $t \sim g$, то получается асимптотика

$$\frac{r}{n} \sim 2\frac{d}{n}\log\frac{n}{d}.$$

Goppa's paper

5. Декодирование. Декодирование (D, G)-кодов сводится к следующей задаче диофантовых приближений в поле алгебраических функций. Введем норму Хемминга $\| \omega \|_H$ дифференциала ω – число полюсов ω. Пусть $\| \omega \|_Q$ обозначает норму, порожденную локализацией в точке Q. Для заданного дифференциала S (синдрома) требуется найти дифференциал ω такой, что

$$\| \omega - S \|_{Q_i} \leqslant a_i, \qquad i = 1, 2, \ldots, l,$$

$$\| \omega \|_H \Rightarrow \min.$$

Здесь Q_i и a_i определяются по дивизору $G = \Sigma m_i Q_i$.

При $g = 0$ эта задача эквивалентна задаче наилучшего рационального приближения p-адических чисел и известен простой алгоритм ее решения (алгоритм Малера).

6. Группа симметрии. Симметрии (D, G)-кода определяются автоморфизмами кривой C. Группа автоморфизмов, рациональных над F_q и оставляющих инвариантным дивизор G, является подгруппой группы симметрии кода. Известна оценка Гурвица для числа автоморфизмов кривой при $g > 1$: $|\operatorname{Aut}(C)| \leqslant 84(g-1)$, но она справедлива лишь в характеристике 0. Для кривых над конечным полем эта группа может быть значительно богаче. Известно много примеров кривых с вычисленной группой $\operatorname{Aut}(C)$. Конструкция кодов на алгебраических кривых позволяет строить коды с заданными симметриями.

Вычислительный центр
Академии наук СССР, Москва

Поступило
10 III 1981

ЛИТЕРАТУРА

1. *Hamming R.W.* – Bell. Syst. Tech. J., 1950, vol. 29, p. 147–160. 2. *Segre B.* – Atti Accad. naz. Lincei Mem. Cl. sci fis, mat e natur., 1967, vol. 8, 5, p. 136–236.