

Math 5251

Error-Correcting Codes, Finite Fields,...

Prof. Paul Garrett

3:35-5:00 MW in Fraser 102

Course web page:

<http://www.math.umn.edu/~garrett/coding/>

Announcements will appear there, so please check that page often.

Text: My book *Mathematics of Coding Theory: Information, Compression, Error-Correction*, available in the bookstore.

Note that one good thing about a book is that it has an **index**.

If you are hoping to get into this class, send me email asking for a magic number.

garrett@math.umn.edu

Grading:

- take-home quiz each week (given out Monday, collected Wednesday)
- three 85-minute **midterms** on Wed Feb 25, Wed Mar 31, and Wed May 05
- a term project due May 07.
- NO final.

The content of the project is flexible, and can be done either individually or in groups. A single-person project should be 10 pages with a bibliography. Some possible topics are listed on-line.

Each exam is a review of the earlier quizzes. All exams are open-book, open-notes, open-calculator, etc.

Scores will *not* be curved: if everyone does well, everyone gets a good grade. Of the course grade each midterm is 15%, project is 20%, and the take-home quizzes are 35%. Late take-home quizzes (without prior arrangements) lose 10 points per 24 hours late, out of 100.

Challenge Problems

There will also be occasional **challenge problems** intended to both afford some additional entertainment at a higher mathematical level, potentially rewarded by varying amounts of **extra credit**.

They will be linked-to from

<<http://www.math.umn.edu/garrett/challenge/>>

I will grade these myself. The standards for coherence, succinctness, legibility, and other aspects of presentation will be very high. That is, I won't even **try** to read a proposed solution if it looks garbagey. Usually **no** partial credit will be given. I will **not** accept attempted solutions within the last two weeks of the term. You may **not** work together on these problems.

Gradeline ranges:

A : 93.00-100.0	A- : 90.00-92.99	
B+ : 86.67-89.99	B : 83.34-86.66	B- : 80.00-83.33
C+ : 76.67-79.99	C : 73.34-76.66	C- : 70.00-73.33
D+ : 65.00-69.99	D : 60.00-64.99	

Of course **plagiarism** of text or images or other IP is prohibited.

In particular, verbatim copying from **my solutions** from homeworks or exams from prior years is **prohibited** on homework or exams.

Verbatim copying from **lecture notes** is undesirable:

For full credit, you must put things into your own words.

And cutting-and-pasting of text and/or images from the internet without giving credit or in violation of copyright or other IP laws is prohibited.

Office hours: 2:45-3:30 MW in Vincent 353, and 5:00-5:30 MW (in the classroom), and 3:30-5:00 Tuesday (in Vincent 353).

email is by far the best way to reach me

Office: Vincent 353 (north stairwell), phone (612) 624-5012. **EMAIL IS BEST.**

Please do not drop by my office at non-office hour times and ask whether I'm busy or not... (*Ha, ha, ha...*) **Sending email is ok anytime**, because I can reply when I have a spare moment.

We will follow IT/CLA policies on incompletes, scholastic misconduct, etc.

Incompletes can be given only if you've completed a majority of the course with a passing grade and agree to complete the incomplete within a short time after the end of the semester. You **cannot** complete an incomplete by retaking the course in the future.

Writing: All answers on homeworks and midterms should be in complete sentences, with reasonably good grammar and spelling. What you have on the page should make sense when read out loud.

Getting a **final answer** is probably necessary, but is not the whole point.

Showing computations/work is necessary, but is not the whole point.

Following an algorithm is often the right thing to do, but is not the whole point.

Also explain what is happening well enough so that someone else could redo what you have done without prior knowledge.

That is, give a **narrative** that tells what is happening, what is not happening, and why. What branches in an algorithm were *not* taken? What criteria *were* met leading you to do a particular thing? What would you have done *otherwise*?

Do not use *abbreviations* which reduce readability.

Format writing on the page in logical order.

Do not require the reader to *solve a puzzle* to figure out your intent.

Bad grammar and bad spelling are undesirable because they weaken the sense of your writing. It is especially bad to mess up *key words*, or to accidentally write something that says *A implies B* when you meant to say *B implies A*.

Do not write in a manner so that the reader must already know the answer and method to understand what you've written.

But do not tell everything you know on every question! Yes, *figuring out what to say and what not to say is part of every question.*

What is the proper context? What is relevant? What is irrelevant?

What are the primary issues? Secondary? Subordinate? Deciding this is always the most important item.

My grader has worked with me for more than a year, and follows my instructions.

Of course if the grader has blundered, I am more than happy to repair the mistake and apologize for it.

However, you should look at what the grader has written before presuming that the grader blundered.

In particular, choice of numbers of points to deduct is a judgement call which the grader has usually discussed with me beforehand. The grader is careful to be *uniform* in grading.

- Do *not* use any other student's 5251 homework sheet: the papers are *numbered*, and each paper has different data.

This allows me to return papers quickly, both to associate your names and faces, and also to improve privacy.

- *Instead*, send me email if you need to get a homework paper. I will make one for you and send you the URL of the PDF file.

- Put '5251' in the subject line of email, to not get *spam-filtered*.

- I do email as fast as I can. If I have not responded to your email it means I've been veeeerrrry busy, too busy to answer all my email! *Sending multiple copies or coming to my office will not solve that problem... :-)*

Course outline

A Little Counting

A Little Probability

Information and Entropy

Codes:

- Example: non-unique decoding
- uniquely-decodable codes
- prefix codes
- Kraft-Macmillan inequality

Noiseless Coding Theorem

- Example: Huffman Coding

Noisy Coding Theorem

Cyclic Redundancy Checks

- The finite field $\mathbf{F}_2 = GF(2) = \mathbf{Z}/2$
- Polynomials with coefficients in $\mathbf{Z}/2$
- Introduce Primitive Polynomials

A Nonlinear Example

- Illustrate the clumsiness of minimum-distance decoding with unstructured code

Some Number Theory and Algebra

Integers (as more familiar analogue of $\mathbf{F}_p[x]$)

Primes and factorization

Euclidean algorithm

\mathbf{Z}/m as entity in its own right

(review "equivalence relation")

Intro to Linear Codes

check matrix

Hamming distance

$$d(x, y) = d(x - y, 0)$$

minimum distance = $1 + k$

when every k columns of check
matrix are linearly independent

Bounds for Codes

Hamming bound

Singleton bound

Gilbert-Varshamov bound

Finite fields

easiest is $\mathbf{F}_2 = GF(2) = \mathbf{Z}/2$

often just $\mathbf{F}_p = GF(p) = \mathbf{Z}/p$ with p prime
inverses-mod- p as novel item

prime-power order fields $\mathbf{F}_{p^n} = GF(p^n)$ exist

These are **not** $\mathbf{Z}/p^n!$ (except when $n = 1$)

Polynomials (coefficients in \mathbf{R} , $\mathbf{Z}/2$, etc.)
with coefficients in a **field**
work nicely (like \mathbf{Z})
examples of non-unique factorization, etc.,
with coefficients in \mathbf{Z}/m , m composite

Cyclic Codes
(uses $\mathbf{F}_2[x]$ modulo $x^n - 1$)

Cyclotomic polynomials
definitions
Primitive roots: proofs

Primitive polynomials

More on finite fields:
computationally modeled as $F_p[x]/(\text{irred})$
(choice of model does matter in applications...)

Vandermonde determinants

Reed-Solomon, BCH Codes

Concatenated Codes, Justesen Codes

Curves and Codes
(aiming at sketch of geometric Goppa codes)