Coding Theory

CSE 445/545

January 31, 2022

Please have a face mask on

Masking requirement

UB requires all students, employees and visitors – regardless of their vaccination status – to wear face coverings while inside campus buildings.

https://www.buffalo.edu/coronavirus/health-and-safety/health-safety-guidelines.html

Let’s do some introductions

Atri Rudra

319 Davis Hall
atri@buffalo.edu
645-2464
Office hours: Wed 3-3:50pm (virtual: see zoom link on piazza)
Fri, 11-11:50am (in-person)

Your awesome TA: Yunus Esencayi

Office hours: look out for piazza poll!

NO office hours this week

Lectures will be videotaped

Still take notes!

http://www.imdb.com/title/tt0363510/mediaviewer/rm2499681792

Handouts for today

Syllabus

- Linked from the course webpage

Feedback polls

- Up on piazza

Plug for feedback polls

Completing the form is voluntary & anonymous

Purpose of the form

- For me to get an idea of your technical background

One Stop Shop for the course

CSE 4/545 Syllabus Piazza Schedule Homeworks Mini Project Autolab Book

CSE 445/545: Coding Theory

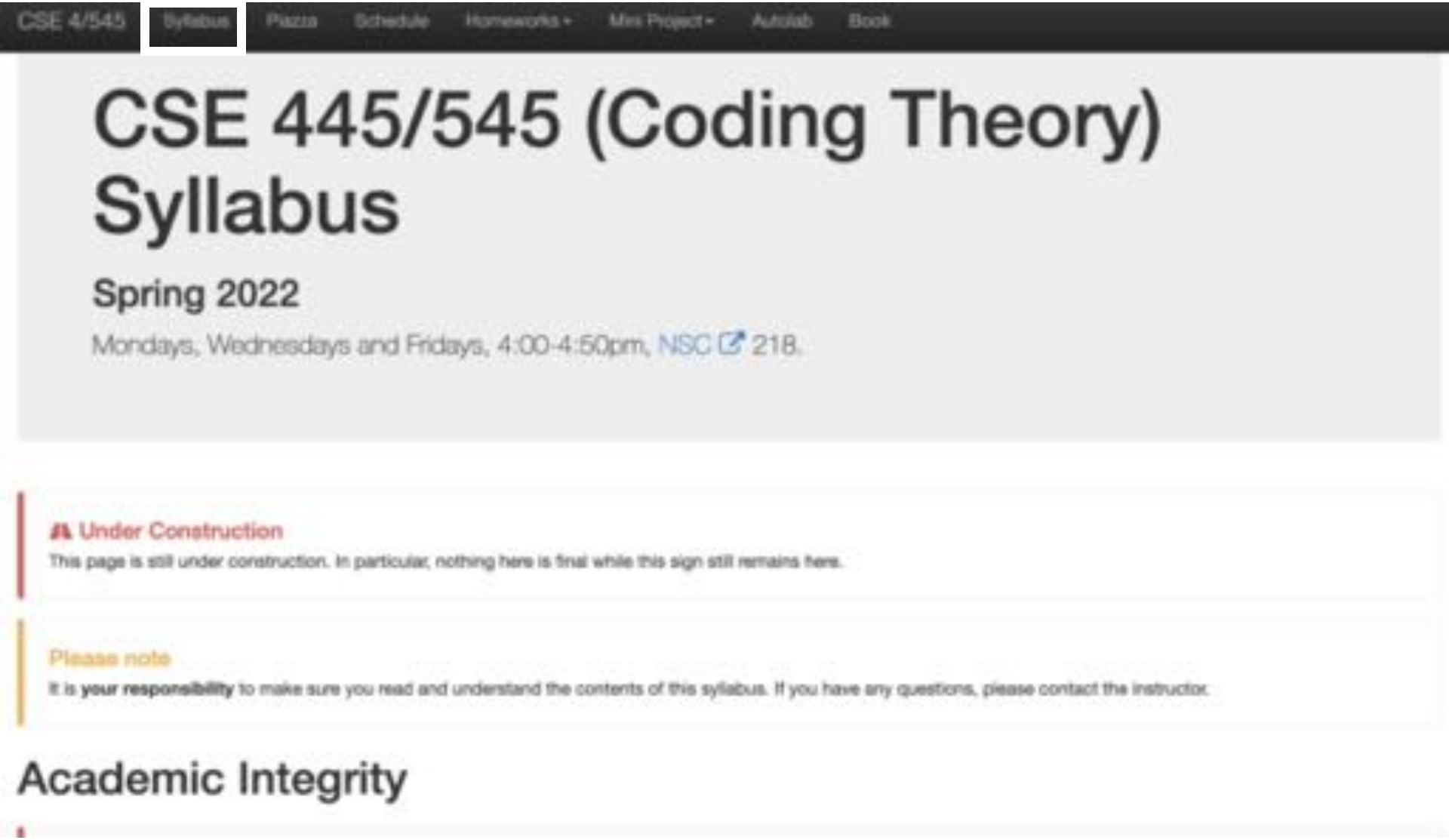
Spring 2022

https://cse.buffalo.edu/faculty/atri/courses/coding-theory/webpage/spr22/

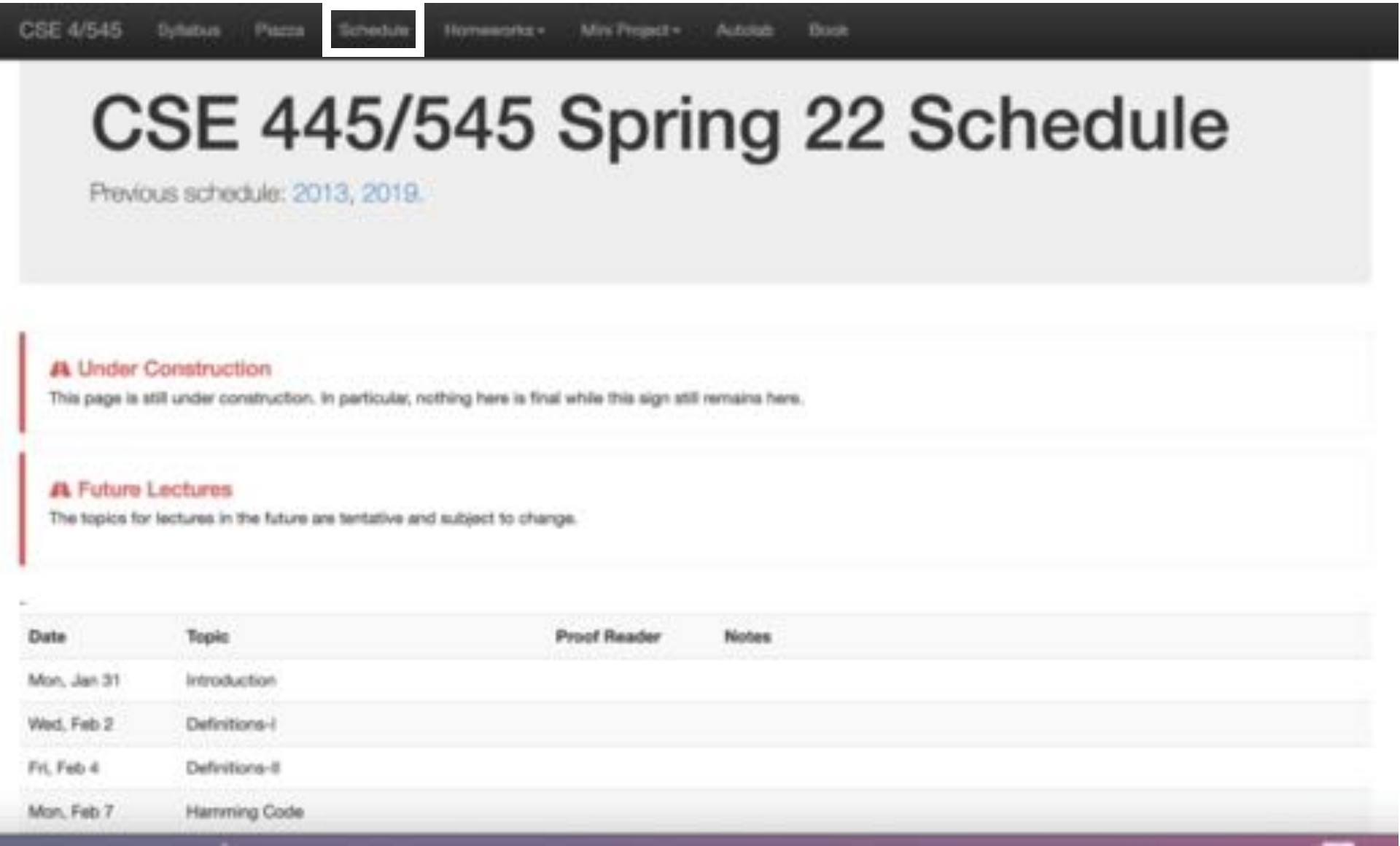
Under Construction

This page is still under construction. In particular, nothing here is final while this sign still remains here.

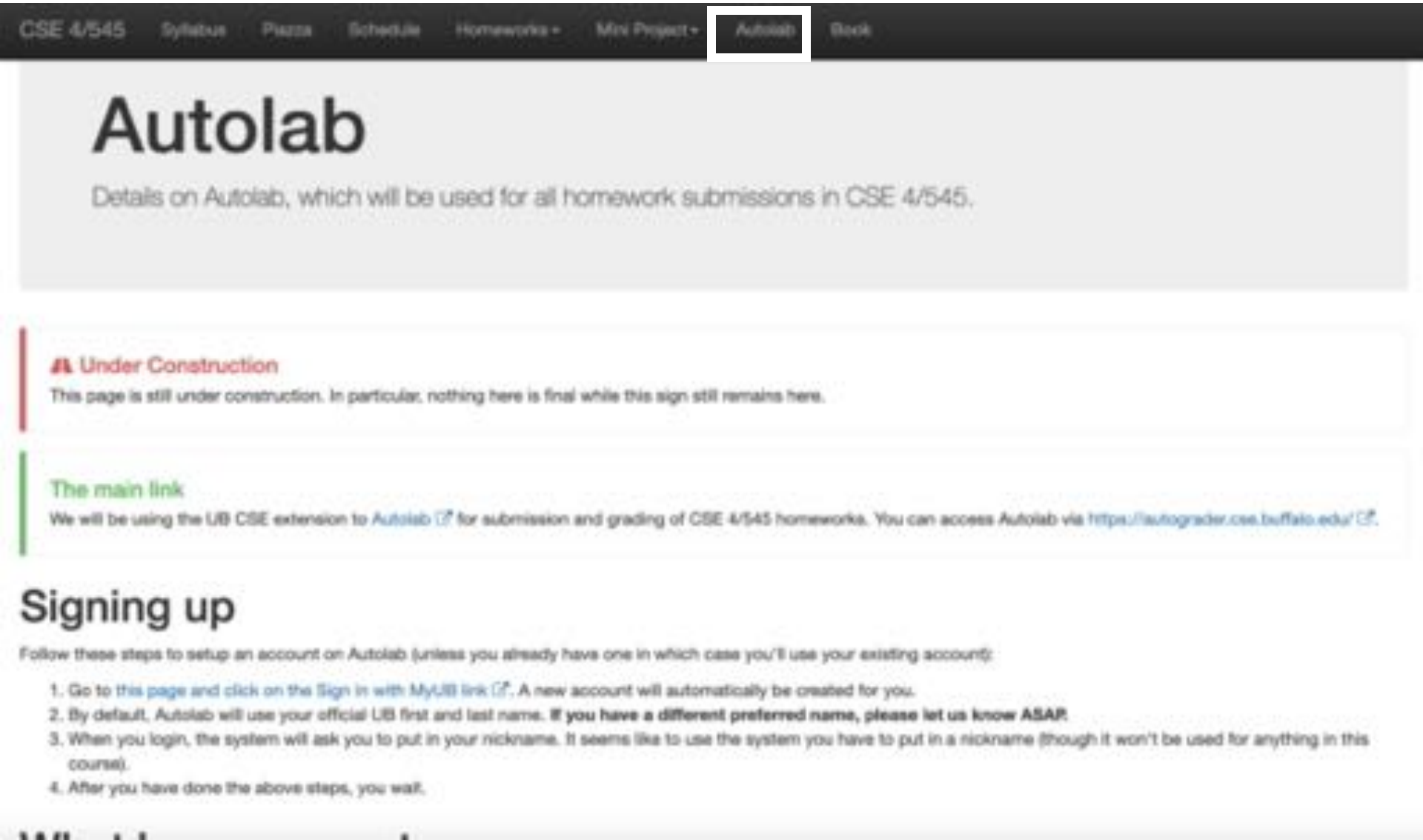
Syllabus


CSE 4/545
Syllabus
Piazza
Schedule
Homeworks
Mini Project
Autolab
Book
CSE 445/545 (Coding Theory) Syllabus
Spring 2022
Mondays, Wednesdays and Fridays, 4:00-4:50pm, NSC 218.
Under Construction
This page is still under construction. In particular, nothing here is final while this sign still remains here.
Please note
It is your responsibility to make sure you read and understand the contents of this syllabus. If you have any questions, please contact the instructor.
Academic Integrity

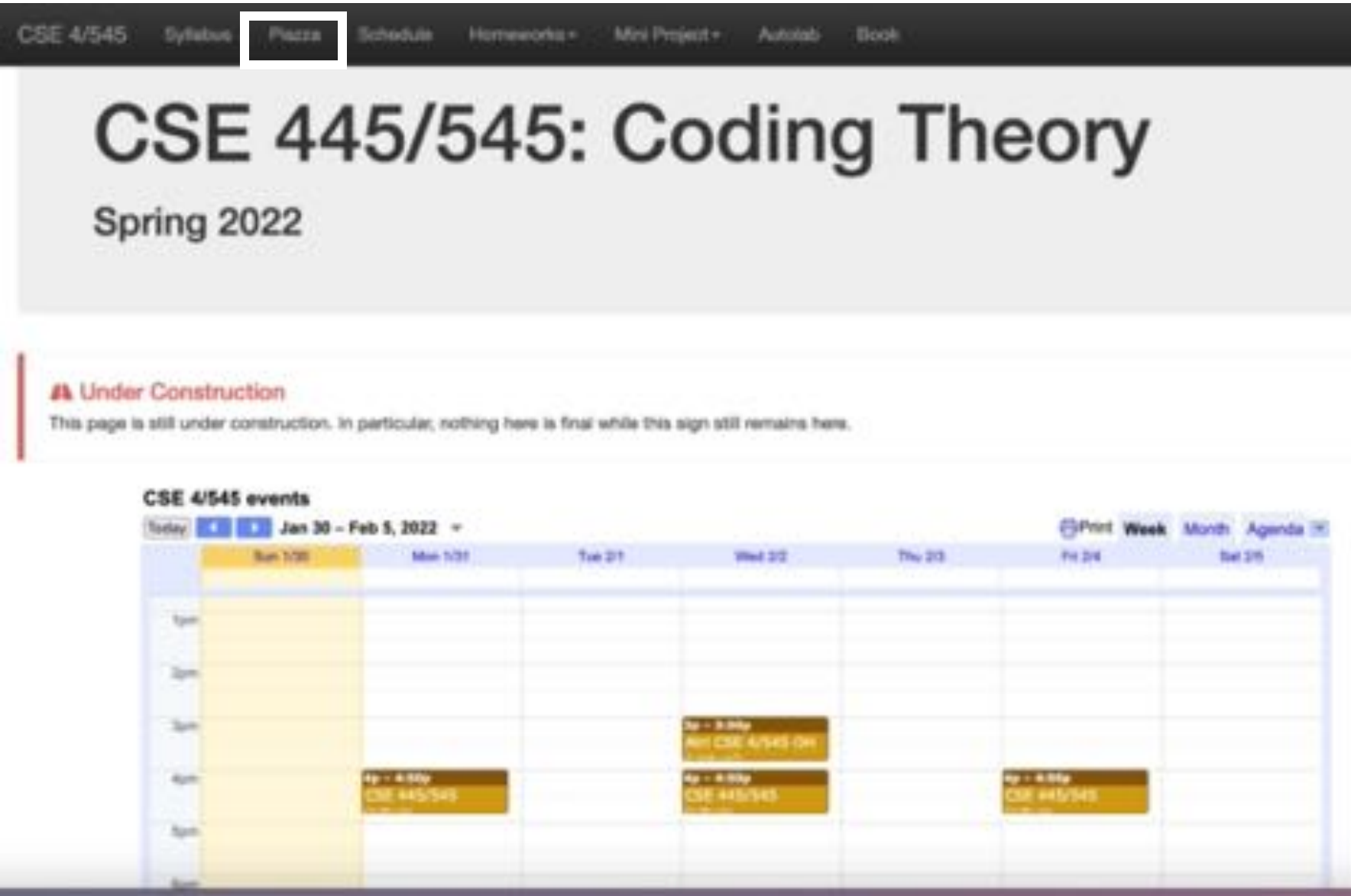
Schedule


CSE 4/545
Syllabus
Piazza
Schedule
Homeworks
Mini Project
Autolab
Book
CSE 445/545 Spring 22 Schedule
Previous schedule: 2013, 2019.
Under Construction
This page is still under construction. In particular, nothing here is final while this sign still remains here.
Future Lectures
The topics for lectures in the future are tentative and subject to change.
Date
Topic
Proof Reader
Notes
Mon, Jan 31
Introduction
Wed, Feb 2
Definitions-I
Fri, Feb 4
Definitions-II
Mon, Feb 7
Hamming Code

Autolab

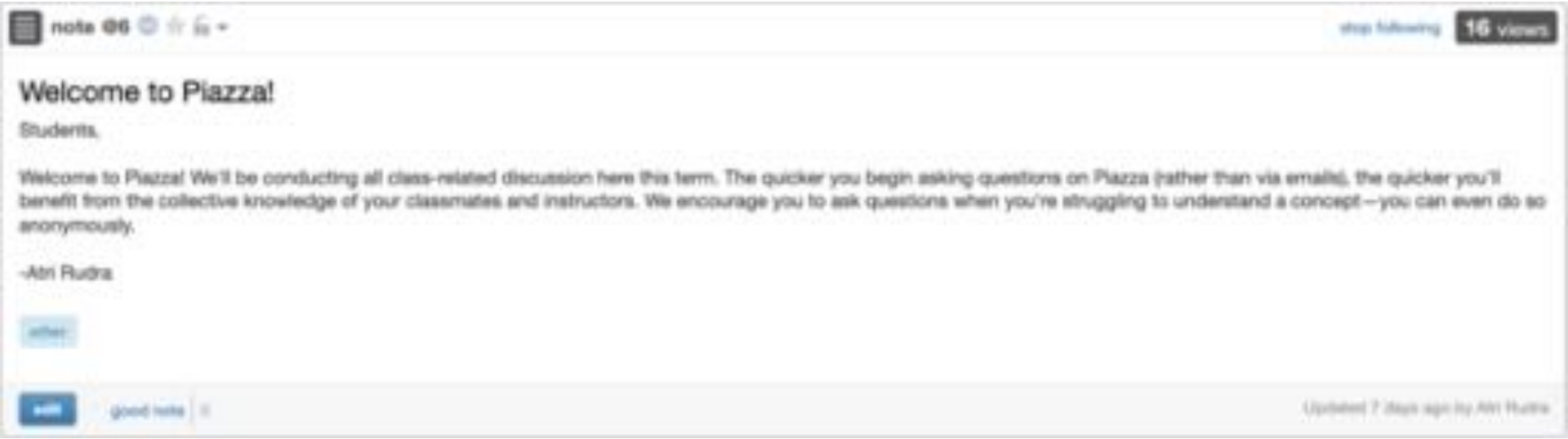

CSE 4/545
Syllabus
Piazza
Schedule
Homeworks
Mini Project
Autolab
Book
Autolab
Details on Autolab, which will be used for all homework submissions in CSE 4/545.
Under Construction
This page is still under construction. In particular, nothing here is final while this sign still remains here.
The main link
We will be using the UB CSE extension to Autolab for submission and grading of CSE 4/545 homeworks. You can access Autolab via https://autograder.cse.buffalo.edu/.
Signing up
Follow these steps to setup an account on Autolab (unless you already have one in which case you'll use your existing account):
1. Go to this page and click on the Sign in with MyUB link. A new account will automatically be created for you.
2. By default, Autolab will use your official UB first and last name. If you have a different preferred name, please let us know ASAP.
3. When you login, the system will ask you to put in your nickname. It seems like to use the system you have to put in a nickname (though it won't be used for anything in this course).
4. After you have done the above steps, you wait.

Piazza


CSE 4/545
Syllabus
Piazza
Schedule
Homeworks
Mini Project
Autolab
Book
CSE 445/545: Coding Theory
Spring 2022
Under Construction
This page is still under construction. In particular, nothing here is final while this sign still remains here.
CSE 4/545 events
Today
Jan 30 – Feb 5, 2022
Print
Week
Month
Agenda
Sun 1/30
Mon 1/31
Tue 2/1
Wed 2/2
Thu 2/3
Fri 2/4
Sat 2/5

Piazza for discussion

Please use your UB email ID to sign up



Feedback polls already up

Questions/Comments?

If something doesn’t work (e.g. you cannot post a comment), let me know

References

Draft of a book I'm writing
- With Guruswami+Sudan

Standard coding theory texts
- MacWilliams and Sloane
- van Lint
- Blahut
- Handbook of coding theory

Essential Coding Theory

Venkatesan Guruswami, Atri Rudra and Madhu Sudan

If you have any comments, please email them to atri@buffalo.edu

The plan is to put up a draft of the whole book sometime in 2022 (for real this time!).

Current Version

Below is a PDF of the book with the chapters that are now stable.

Draft of the book (January 30, 2022)

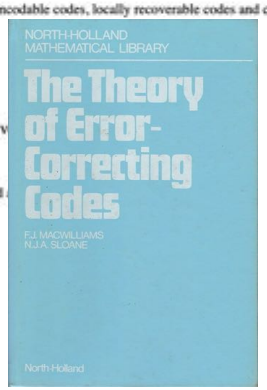
- (*Major changes from last version:* Added chapters on expander codes, linear time encodable codes, locally recoverable codes and co

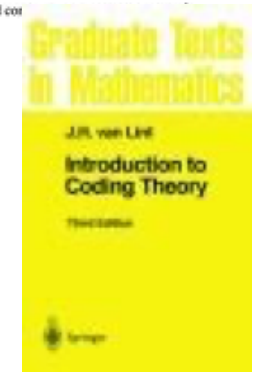
Warning: There are some dangling/missing links.

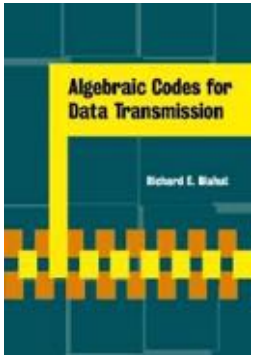
Previous Versions

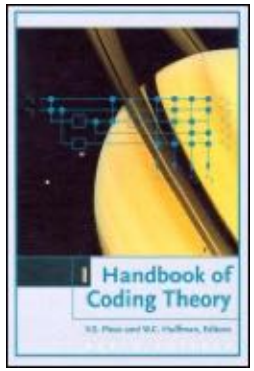
Listed below are previous versions of the book (in case you need an older v

- March 15, 2019.
  - (*Major changes from last version:* Added chapter on decoding RM code and
- December 18, 2018.
- July 27, 2018.
- Old version of the webpage that has separate chapter files.









Pre-requisites

No formal pre-requisites for 545/ CSE 331 for 445

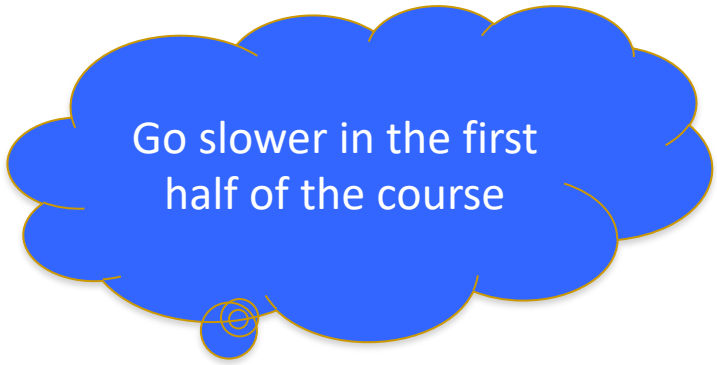
- Probably no one will have all the pre-req's

Mathematical maturity

- Comfortable with proofs
- Willing to pick up basics of new areas

Will spend one lecture on the pre-req's

- Linear Algebra
- Finite Fields
- Probability
- Algorithms/ Asymptotic Analysis



Grades and such like

Grading Policy

Here is the split of grades:

Course Component	% of grade
Mini project	45%
Homeworks	45%
Proof Reading	10%

Mini Project

Groups of size = 3

Create a Youtube video related to coding theory

Bunch of other details in syllabus

Deadlines

- `February 16, 2022.` You form groups of size **exactly three (3)** for the project by **11:59pm**. **One submission per group is needed to "register" the group.**

`March 2, 2022.` Your group submits topic for your video by **11:59pm**. **One submission per group is needed to "register" the group.**

`March 30, 2022.` You should submit your two-page report by **11:59pm** on Autolab.

`May 11, 2022.` You should submit your video by **11:59pm** on Autolab.

Proof-reading

Proof-read relevant part of the book

Once during the course

- Unless class size decreases below 40

Submit typos, suggestions for improvement

They are due in by 1pm before next lecture

Notes will be graded on timeliness & quality

Will ask for a volunteer

See syllabus for more details

Questions/Comments?

Check out the syllabus for more details

Homework

6 short ones (545)/ 5 short ones (445)

Collaboration generally allowed

- Work in groups of size at most 3
- Write up your own solutions
- Acknowledge your collaborators
- No source other than book and your notes
- Breaking these rules will be considered as cheating

More details when they are handed out

My homework philosophy for 4/545

NOT to make sure you understand what I teach in the lectures

Homework problems either

- Proofs that were not done in the class; or
- Material that is not covered in the class
  - Closely related to something that is

Questions/Comments?

Check out the syllabus for more details

Accessibility Resources

Information included in the syllabus

In short, let me know and consult with Accessibility Resources

Preferred Name

If you prefer using name diff from UB records

Let me know and we'll make a note of it.

Some comments

- Decide on a Video topic **early**
  - Different topics might need different prep. work
  - Come talk to me
- Homeworks might take time
  - Do not wait for the last moment

Academic Dishonesty

All your submissions must be your own work

Penalty:

- Minimum: An **grade reduction in course**
- Possible: **F** (or higher penalty) if warranted

YOUR responsibility to know what is cheating, plagiarism etc.

- If not sure, come talk to me

Excuses like "I have a job," "This was OK earlier/in my country," "This course is hard," etc. **WON'T WORK**

I DO NOT HAVE ANY PATIENCE WITH ANY CHEATING :

YOU WILL GET A GRADE REDUCTION IN THE COURSE

FOR YOUR FIRST MISTAKE

If grades are all you care about

You'll be fine if

- You do your assignments **honestly**
- Make a reasonable attempt at them

If you took CSE 331

I'm assuming you're in this class because you wanted to be here

Less scaffolding/support material

Am happy to give pointers but if you need to makeup on some background knowledge, I expect you to pick up the material on your own

Apologies for any (small) bumps

The previous highest enrollment for the course was 12

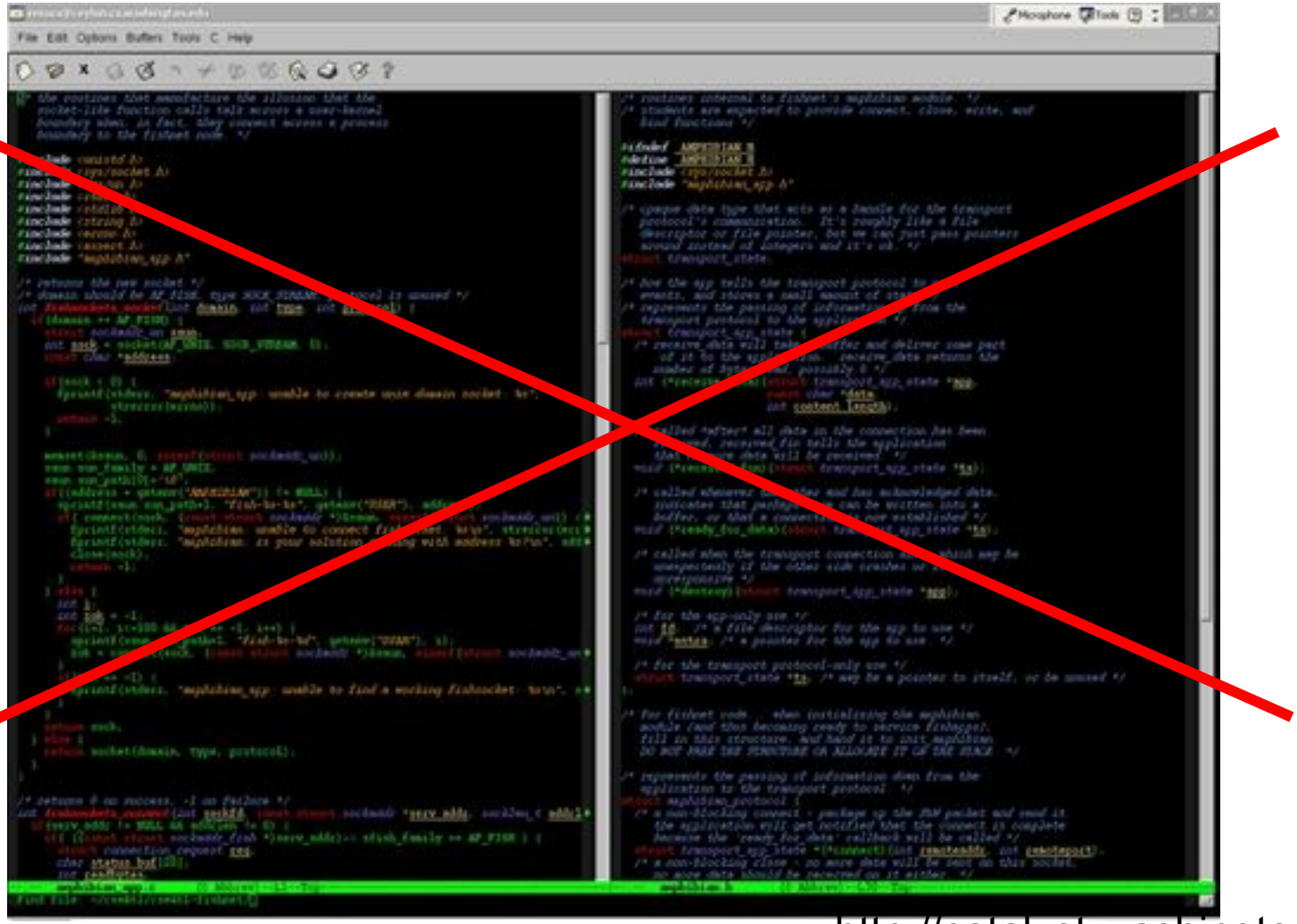
Please bear with if I need to smoothen some bumps in the course ☺

Questions/Comments?

Check out the syllabus for more details

Let the fun begin!

Coding theory



http://catalyst.washington.edu/

What does this say?

W*lcome to the cl*ss. I h*pe you w*ll h*ve as mu*h f*n as I wi*l hav* t*ach*ng it!

Welcome to the class. I hope you will have as much fun as I will have teaching it!

Why did the example work?

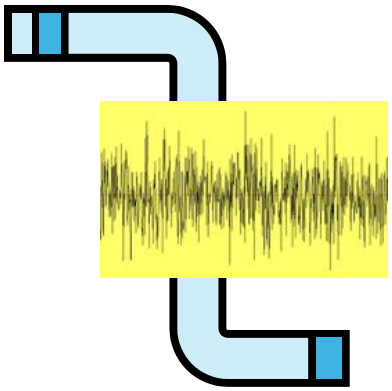
English has in built redundancy

Can tolerate “errors”

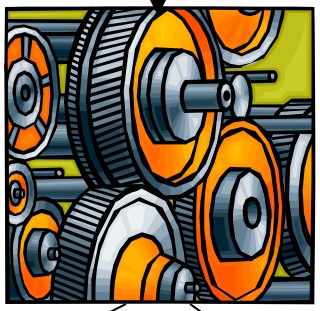
The setup

x

C(x)



y = C(x)+error



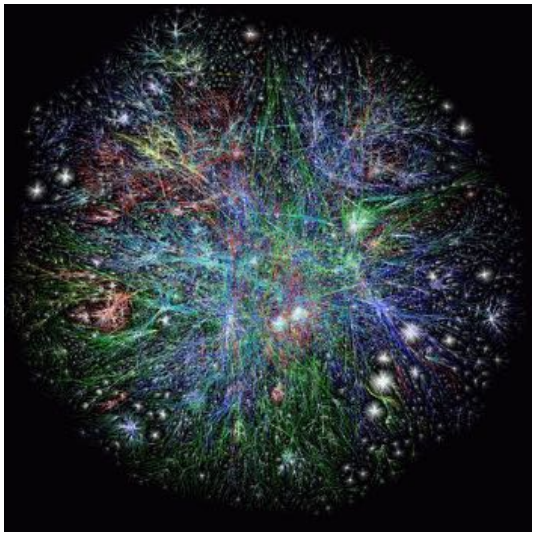
x

Give up

- Mapping **C**
  - Error-correcting code or just code
  - Encoding: $x \rightarrow C(x)$
  - Decoding: $y \rightarrow x$
  - C(x) is a codeword

Communication

- Internet
  - Checksum used in multiple layers of TCP/IP stack
- Cell phones
- Satellite broadcast
  - TV
- Deep space telecommunications
  - Mars Rover



Codes and 5G

UC San Diego News Center

October 11, 2018 | By Daniel Kane

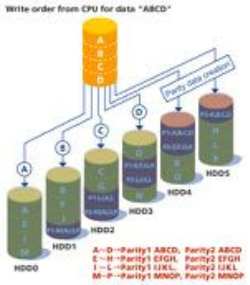
Samsung Licenses 5G Polar Coding Technology Developed by UC San Diego Engineers

Samsung and the University of California San Diego recently signed a major license agreement for the telecommunications industry, for a standard-essential error-correction technology developed by engineers from the Jacobs School of Engineering.

“Unusual” applications

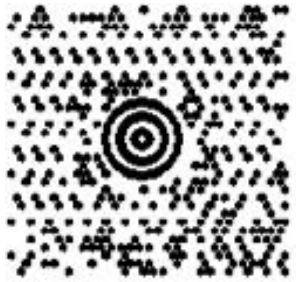
Data Storage

- CDs and DVDs
- RAID
- ECC memory



Paper bar codes

- UPS (MaxiCode)



Codes are all around us

While applications are numerous…

This course will basically focus ONLY on proofs

where in the above "$|E(\mathbf{m})$" is short for "being conditioned on $E(\mathbf{m})$ being transmitted" and the inequality follows from the union bound (Proposition 3.1.5) and the fact that D is MLD.

Noting that $\Delta(E(\mathbf{m}'),\mathbf{y}) \le \Delta(E(\mathbf{m}),\mathbf{y}) \le (p+\varepsilon')n$ (see Figure 6.6), by (6.9) we have

$$\begin{aligned}
\mathbb{E}_E\left[\mathbb{1}_{D(\mathbf{y})\neq\mathbf{m}}\right] &\le \sum_{\mathbf{m}'\neq\mathbf{m}} \Pr\left[E(\mathbf{m}') \in B\left(\mathbf{y},(p+\varepsilon')n\right) | E(\mathbf{m})\right] \\
&= \sum_{\mathbf{m}'\neq\mathbf{m}} \frac{\left|B\left(\mathbf{y},(p+\varepsilon')n\right)\right|}{2^n} && (6.10)\\
&\le \sum_{\mathbf{m}'\neq\mathbf{m}} \frac{2^{H(p+\varepsilon')n}}{2^n} && (6.11)\\
&< 2^k \cdot 2^{-n(1-H(p+\varepsilon'))} \\
&\le 2^{n(1-H(p+\varepsilon))-n(1-H(p+\varepsilon'))} && (6.12)\\
&= 2^{-n(H(p+\varepsilon)-H(p+\varepsilon'))}. && (6.13)
\end{aligned}$$

In the above, (6.10) follows from the fact that the choice for $E(\mathbf{m}')$ is independent of $E(\mathbf{m})$. (6.11) follows from the upper bound on the volume of a Hamming ball (Proposition 3.3.3), while (6.12) follows from our choice of k.

Using (6.13) in (6.8), we get

$$\begin{aligned}
\mathbb{E}_E\left[\Pr_{\mathbf{e}\sim\mathrm{BSC}_p}\left[D(E(\mathbf{m})+\mathbf{e})\neq\mathbf{m}\right]\right] &\le e^{-(\varepsilon')^2 n/2} + 2^{-n(H(p+\varepsilon)-H(p+\varepsilon'))} \sum_{\mathbf{y}\in B(E(\mathbf{m}),(p+\varepsilon')n)} \Pr\left[\mathbf{y}|E(\mathbf{m})\right] \\
&\le e^{-(\varepsilon')^2 n/2} + 2^{-n(H(p+\varepsilon)-H(p+\varepsilon'))} \le 2^{-\delta' n}, && (6.14)
\end{aligned}$$

where the second inequality follows from the fact that

$$\sum_{\mathbf{y}\in B(E(\mathbf{m}),(p+\varepsilon')n)} \Pr\left[\mathbf{y}|E(\mathbf{m})\right] \le \sum_{\mathbf{y}\in\{0,1\}^n} \Pr\left[\mathbf{y}|E(\mathbf{m})\right] = 1$$

and the last inequality follows for large enough n, say $\varepsilon' = \varepsilon/2$ and by picking $\delta' > 0$ to be small enough. (See Exercise 6.3.)

Thus, we have shown that for any arbitrary $\mathbf{m}$ the average (over the choices of E) decoding error probability is small. However, we still need to show that the decoding error probability is exponentially small for *all* messages *simultaneously*. Towards this end, as the bound holds for each $\mathbf{m}$, we have

$$\mathbb{E}_{\mathbf{m}}\left[\mathbb{E}_E\left[\Pr_{\mathbf{e}\sim\mathrm{BSC}_p}\left[D(E(\mathbf{m})+\mathbf{e})\neq\mathbf{m}\right]\right]\right] \le 2^{-\delta' n}.$$

Other applications of codes

Outside communication/storage domain

Tons of applications in theory

- Complexity Theory
- Cryptography
- Algorithms