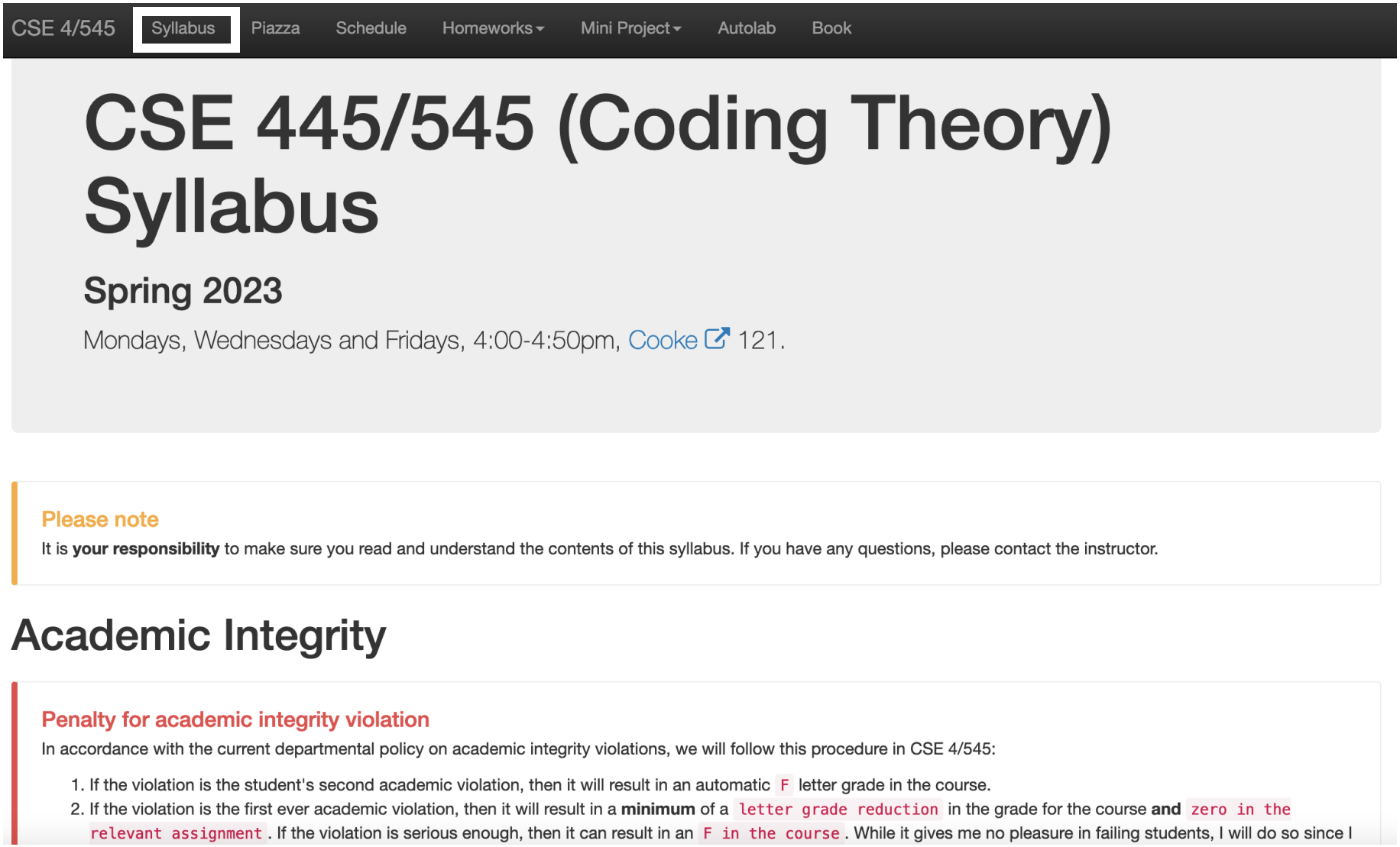
Coding Theory

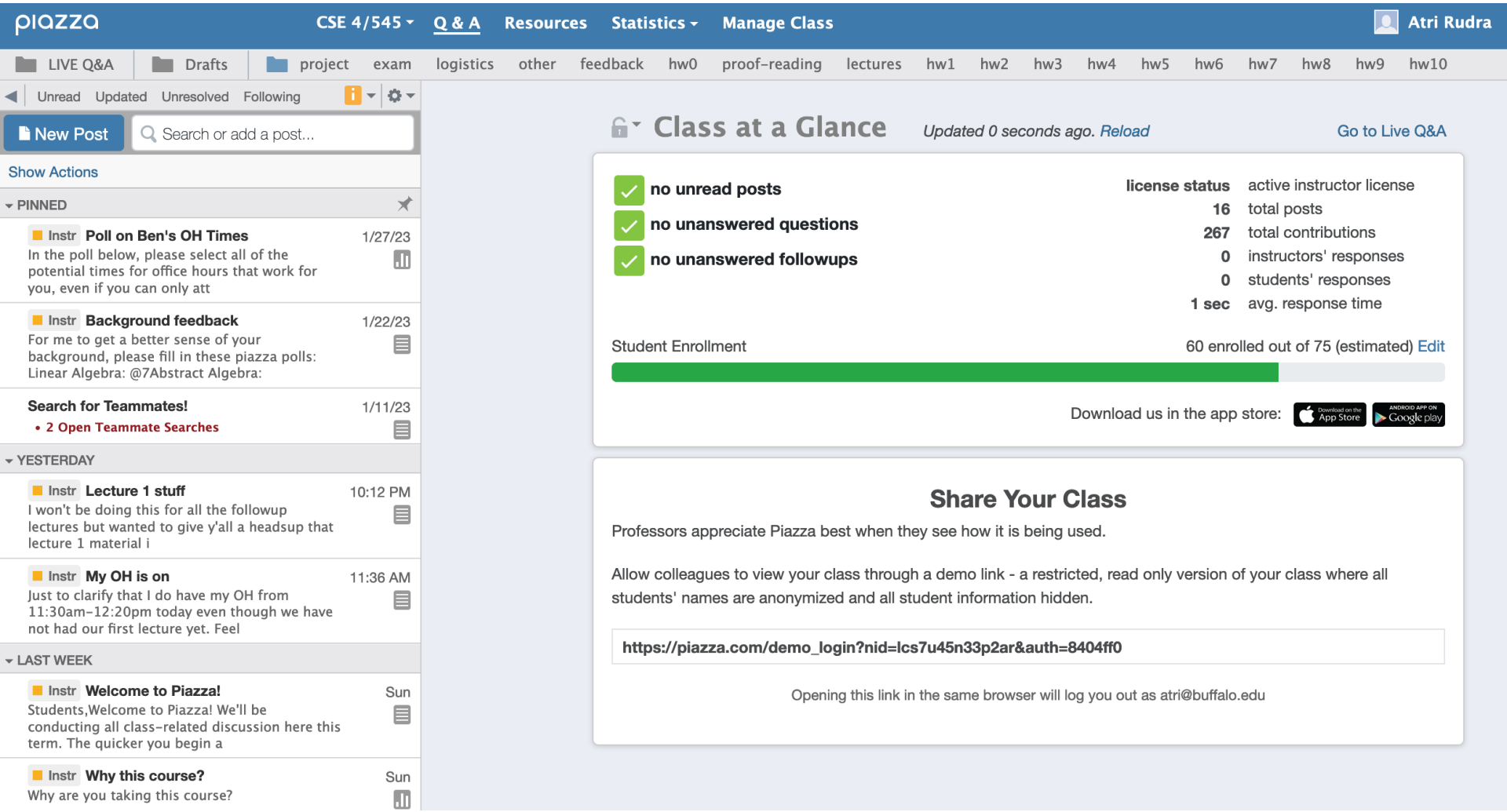
CSE 445/545

February 1, 2023

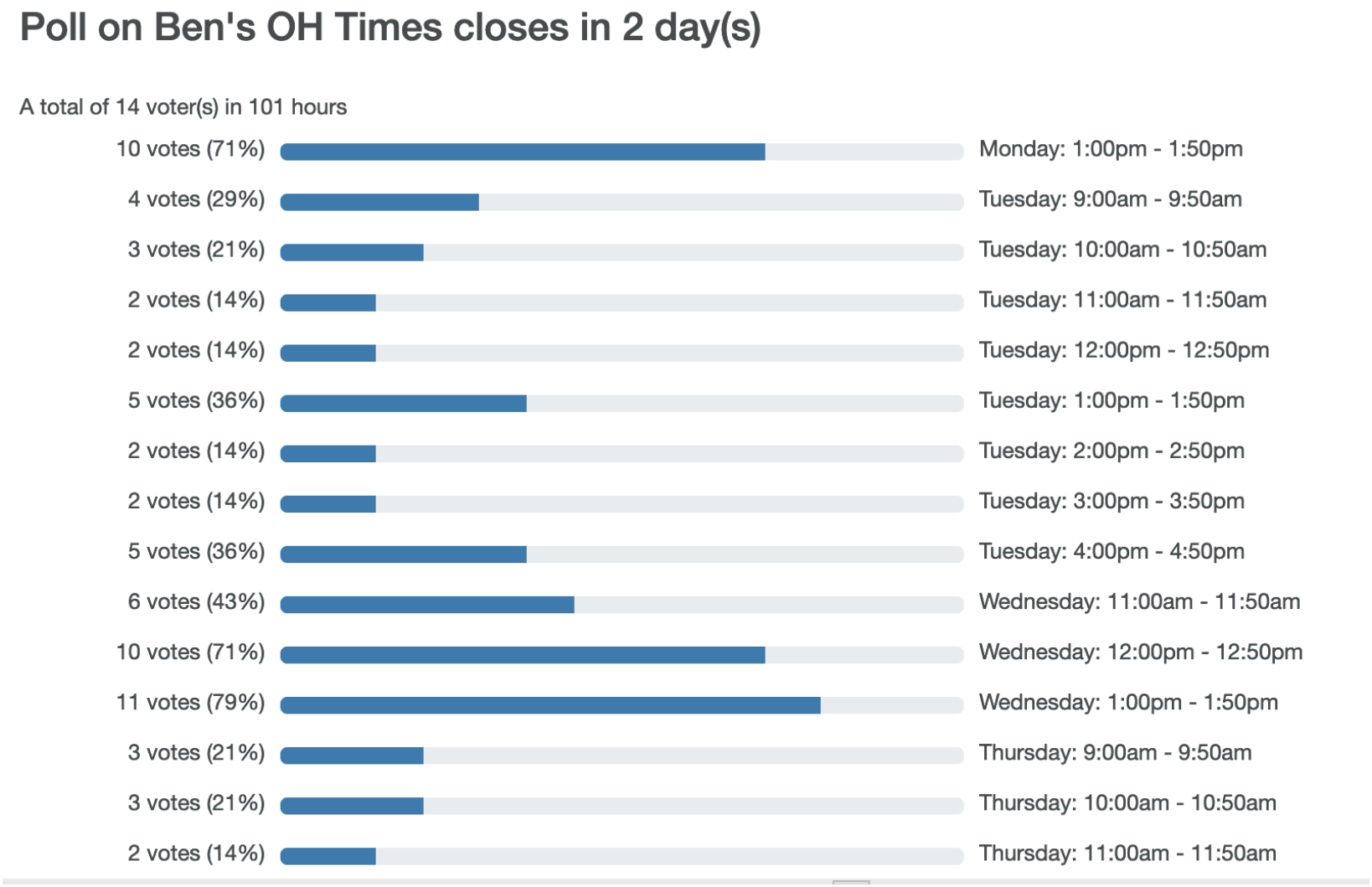
Make sure to check out the syllabus!



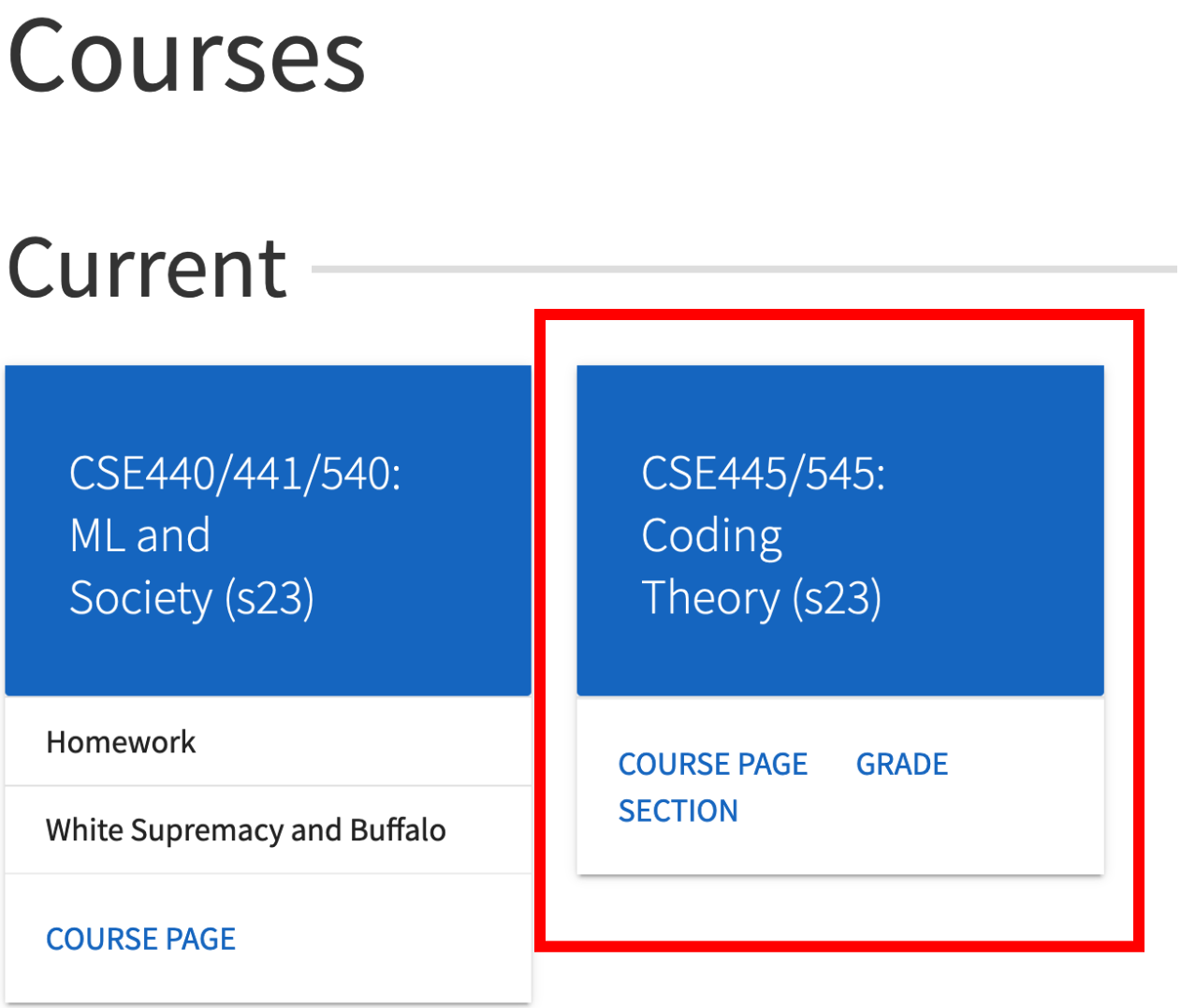
Let me know if you're not on piazza



By tonight fill in poll for Ben's office hours



Make sure you see 4/545 on Autolab



While applications are numerous…

This course (lectures and HWs) will 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

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

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

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

Questions/Comments?

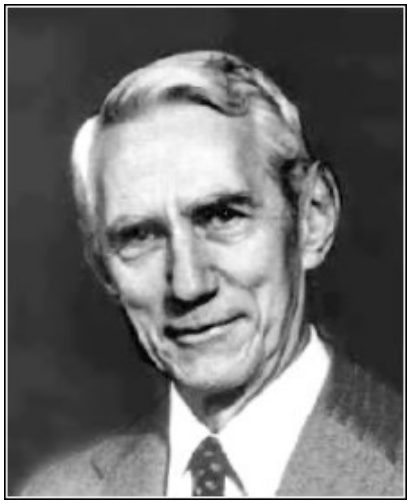
The birth of coding theory

Claude E. Shannon

"A Mathematical Theory of Communication"

1948

Gave birth to Information theory



Richard W. Hamming

"Error Detecting and Error Correcting Codes"

1950

Structure of the course

Part I: Combinatorics

What can and cannot be done with codes

Part II: Algorithms

How to use codes efficiently

Part III: Applications

Applications in (theoretical) Computer Science

Redundancy vs. Error-correction

Repetition code: Repeat every bit say 100 times

- Good error correcting properties
- Too much redundancy

Parity code: Add a parity bit

- Minimum amount of redundancy
- Bad error correcting properties
  - Two errors go completely undetected

Neither of these codes are satisfactory

1 1 1 0 0	1

1 0 0 0 0	1

Two main challenges in coding theory

Problem with parity example

- Messages mapped to codewords which do not differ in many places

Need to pick a lot of codewords that differ a lot from each other

Efficient decoding

- Naive algorithm: check received word with all codewords

The fundamental tradeoff

Correct as many errors as possible with as little redundancy as possible

Can one achieve the “optimal” tradeoff with *efficient* encoding and decoding ?

Rest (of the semester) on the board…