Math 75 notes, Lecture 12 outline

P. Pollack and C. Pomerance

References below are to Pretzel's *Error-correcting codes and finite fields*:

- Definitions of *alphabet* (p. 5), *word* (p. 13), *codes* and *block codes* (p. 13)
- Definition of *Hamming distance* (p. 15).
- Proposition: the Hamming distance is a metric on words of a given length (Proposition, p. 15)
- Definition of the *minimum distance* of a code (p. 17)
- Proposition: A code can detect any pattern of up to s errors if and only if its minimal distance is $\geq s+1$ (p. 17).
- Proposition: A code can correct any pattern of up to s errors if and only if its minimal distance is $\geq 2s+1$ (p. 18).
- Definition of a *linear code* and verification that the three examples from the introductory lecture are linear codes (p. 29).