Math 75 notes, Lecture 21 outline

P. Pollack and C. Pomerance

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

$$V(q,n,t) := \binom{n}{0}(q-1)^0 + \binom{n}{1}(q-1)^1 + \cdots + \binom{n}{t}(q-1)^t.$$

- We proved the Hamming bound (p. 289): If C is a code of length n on an alphabet A of size q, and $d(C) > 2r$, then $|C| \leq q^n/V(q,n,r)$. Equality holds exactly for r-perfect codes.

- We proved the Singleton bound (p. 290): If C is a linear code over $\mathbb{F}_q$ of length n and rank m, then $m \leq n - d(C) + 1$. Equality holds for MDS codes, such as the Reed-Solomon codes $\mathrm{RS}(k,t)$.

- We proved the Gilbert-Varshamov bound (Theorem, §18.5): If A is an alphabet of size q, then there is a code of length n over A with minimum distance $\geq d$ and $|C| \geq q^n/V(q,n,d-1)$.

- We showed that the Gilbert-Varshamov bound remains true for linear codes (Theorem, §18.6): There is a *linear code* over $\mathbb{F}_q$ of length n and distance $\geq d$ with $|C| \geq q^n/V(q,n,d-1)$.

- We defined the *relative minimum distance* $\delta(C)$ of a block code C (p. 293) as m/n, where m is the length of a real word and n is the block length.

- We defined a *bad* family of codes as one with the following property: It is impossible to choose an $\epsilon > 0$ and an infinite subcollection of codes from the family with the rate and minimum distance both at least ϵ for every code in the subcollection. (This is a somewhat more inclusive definition than the one given in the book on p. 294.) We saw that the Hamming codes form a bad family, and we stated (but did not prove) that the codes $\mathrm{BCH}(k,t)$ also form a bad family.

- We used the Gilbert-Varshamov bound for linear codes to produce a family of codes that is not bad. To do this, we fixed a positive $\delta < 1/2$ and chose the largest binary code of length n with minimum distance $\geq d = \lceil \delta n \rceil$. Clearly each code constructed in this way has minimum relative distance $\geq \delta$. Assuming the book's estimate for $V(q;n,d-1)$ (Lemma, p. 294), we showed that the rate of these code does not tend to zero with n; in fact,

  $$\liminf m/n \geq 1 - H(\delta) > 0,$$

  where

  $$H(\delta) = -\delta \log_2 \delta - (1-\delta)\log_2(1-\delta).$$

  So the collection of these codes (with lengths $n = 1, 2, 3, \ldots$) is not a bad family.