Math 75 notes, Lecture 15 outline

P. Pollack and C. Pomerance

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

- We went over what it means for the generator matrix of a linear code to be in *standard form* (see p. 35), and we mentioned that both decoding and constructing a check matrix are trivial in this case. (See §3.11 on p. 41.)
- We defined the space of *cosets* V/W, where V is a vector space and W is a subspace.
- We proved that if C is an m-dimensional subspace of F^n, then there are precisely q^{n-m} distinct cosets of C in F^n (i.e., distinct elements of F^n/C).
- We constructed the *standard array* of a code (§4.1).
- We introduced the method of 'correcting' via the standard array, whereby one replaces a received word v by the code word at the head of its column. We saw that this is equivalent to replacing v by $v - e$, where e is the row leader of the row containing v. (See the proposition at the bottom of p. 53.)
- We saw (Theorem, §4.7) that if the row leaders were chosen to have minimal weight in their coset, then the standard array replaces each received word by a closest code word.
- We saw that the standard array can correct an error pattern $e \in F^n$, not a code word, exactly when e is a row leader. Consequently, a standard array can be constructed to correct all the k distinct error patterns $e_1, \ldots, e_k$ (none of which are code words) exactly when the e_i belong to distinct cosets. (See Theorem, §4.8, on p. 55.)
- We began to point out why, to correct via a standard array, it is enough to store the row leaders and their *syndromes*. Here the *syndrome* of a vector u with respect to the code C is the vector $(Hu^T)^T$, where H is a fixed check matrix for C. We didn't finish this, so please read the discussion in §4.9 of the text.