Math 75 notes, Lecture 14 outline

P. Pollack and C. Pomerance

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

- We picked up again with a discussion of the four algorithmic problems of coding theory: encoding, decoding, recognizing codewords, and correction.
- We saw that a code may have more than one encoder and consequently more than one generator matrix. We proved that an $n \times m$ matrix G is a generator matrix for the (n, m)-linear code C if and only if the columns of G are linearly independent code words. (This is the proposition from p. 38 of the text.)
- We defined a *decoder* for an encoding $E\colon F^m \to F^n$ as a linear map from $F^n \to \mathbb{F}^m$ with the property that $D \circ E$ is the identity map on $\mathbb{F}^m$. In other words, a *decoder* for E is a left inverse of E. We mentioned that decoders always exist, and that they can be found (algorithmically) by a process of column-reduction.
- We defined a *check vector* for an (n, m)-linear code C as a vector $v \in F^n$ orthogonal to every code word x. We saw that the set of check vectors forms a subspace $C^\perp$ of F^n of dimension $n-m$, and that $C = (C^\perp)^\perp$, so that the code words are precisely those vectors orthogonal to all check vectors.
- We defined a *check matrix* for an (n, m)-linear code (see p. 39 of the text), and mentioned that each such matrix has at least $n - m$ rows. Indeed, a matrix is a check matrix if and only if its rows are check vectors which span $C^\perp$. (This last statement is a precise form of the proposition at the bottom of p. 42.)
- We started an example of computing a check matrix for a $(6, 3)$-linear code over $\mathbb{F}_2$ given to us in terms of an explicit basis.

Addendum to the lecture: Some examples of row reduction in action. Since the techniques from this last (incompletely worked out) example are useful in the solution of this week's homework, we present a complete solution here for reference purposes.

Recall that a matrix is said to be in *row reduced echelon form* if it satisfies the following four conditions:

1. All the rows consisting entirely of zeros are grouped together at the bottom.
2. Each nonzero row begins with a leading 1.
3. In any two consecutive nonzero rows, the leading 1 in the second row is to the right of the 1 in the first row.
4. Each leading 1 is the only nonzero element of its column.

It should be familiar to you from linear algebra that every matrix M can be put in reduced row echelon form by a sequence of elementary row operations. Moreover, this reduced row echelon form is unique.

We now return to the example from class.

Example 1. *Find a check matrix of minimal size for the* $(6,3)$*-linear code* C *over* $\mathbb{F}_2$ *with basis*

$$(1,1,1,0,0,1),(0,0,1,1,0,1),(0,0,0,0,1,1).$$

Solution: We noted in class that $C^\perp$ is exactly the set of vectors $x \in \mathbb{F}_2^6$ for which x^T belongs to the kernel (or null space) of the matrix

$$M := \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Note that M, which has for its rows the given basis of code words, is the transpose of a generator matrix for the code.

We begin by putting M in reduced row echelon form. Actually M is almost already there: we have only to add the second row to the first to obtain

$$\tilde{M} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

which is in reduced row echelon form. Elementary row operations leave the nullspace unchanged, so that $\tilde{M}$ has the same nullspace as M. For $x \in \mathbb{F}_2^6$, write $x = (x_1, x_2, x_3, x_4, x_5, x_6)$. Then

$$\tilde{M}x^T = \begin{bmatrix} x_1 + x_2 + x_4 \\ x_3 + x_4 + x_5 \\ x_5 + x_6 \end{bmatrix}.$$

In order for this to be zero, we need all the coordinates to vanish. In this case, the pivot variables (those variables corresponding to the position of the leading 1's in each row) can be solved for in terms of the non-pivot variables to yield

$$x_1 = x_2 + x_4, \quad x_3 = x_4 + x_6, \quad x_5 = x_6.$$

So for x^T to be in the nullspace, it is necessary and sufficient that x have the form

$$(x_2 + x_4, x_2, x_4 + x_6, x_4, x_6, x_6) = x_2(1,1,0,0,0,0) + x_4(1,0,1,1,0,0) + x_6(0,0,1,0,1,1)$$

for some $x_2, x_4, x_6 \in \mathbb{F}_2$. Since these three right-hand vectors are linearly independent, it follows that they form a basis for the null space, and hence a check matrix for our code C is given by

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

So we've found a check matrix with 3 rows. As noted in class, any check matrix for C has at least $n - m = 6 - 3 = 3$ rows, so this one has minimal size.

Note on an alternate approach: One can find the nullspace of M without putting M iun *reduced* row echelon form. It is enough that M be in row echelon form (i.e., it's not necessary that the leading 1 be the only nonzero element in each column). In this cast you work backwards: solve for the pivot variables starting with the last one (in this case x_5), working up.

We conclude by mentioning one more problem where row reduction is useful.

Example 2. *Find a basis for the* $(4,2)$*-linear code over* $\mathbb{F}_3$ *with check matrix*

$$M = \begin{bmatrix} 1 & 0 & -1 & 1 \\ 1 & -1 & 1 & 0 \end{bmatrix}.$$

Solution: Since M is the check matrix, we know that x is a codeword if and only if x^T is in the nullspace of M. Using $\rightsquigarrow$ to denote that one matrix comes from the previous by an elementary row operation, we have

$$M \rightsquigarrow \begin{bmatrix} 1 & 0 & -1 & 1 \\ 0 & -1 & -1 & -1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} = \tilde{M},$$

say. Now $\tilde{M}$ is in reduced row echelon form, and proceeding as above we easily find that $(1,-1,1,0)^T$ and $(-1,-1,0,1)^T$ are a basis for the nullspace. So $(1,-1,1,0)$ and $(-1,-1,0,1)$ are a basis for the code.