MATH 525
Section 2.5: Bases for $C = \langle S \rangle$ and $C^{\perp}$

September 21, 2020

As usual, let $K = \{0, 1\}$ be the binary field and K^n the vector space over K consisting of all binary n-tuples.

Goals of Section 2.5: Given a subset $S \subseteq K^n$, determine:

1. a basis for $C = \langle S \rangle$, the subspace (or code) generated by S.
2. a basis for $C^{\perp}$, the dual of C.

Remark: All the matrices we will discuss have entries that belong to the field $K = \{0, 1\}$.

Recall: The elementary row operations on a matrix $k \times n$ are:

1. Interchange two rows;
2. Replace one row by the sum of itself and another row (remember to do that in K^n).

Elementary row operations on a matrix are *reversible*, in the sense that if matrix B can be obtained from matrix A via an elementary row operation, then A can also be obtained from B via an elementary row operation.

Definition

If matrix A can be obtained from matrix B by a sequence of elementary row operations, we say that *A and B are row equivalent*.

The **row echelon form** (REF) of a matrix:

1. All nonzero rows are above any rows of all zeros;
2. Each *leading entry* of a row (that is, the very first 1 of that row) is in a column to the right of the leading entry of the row above it;
3. All entries in a column below a leading entry are zeros.

Examples: $*$ is any element of the field $K = \{0, 1\}$.

$$\begin{bmatrix} 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

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

Important facts to remember from linear algebra:

1. It is always possible to transform any $k \times n$ matrix into echelon form by a finite sequence of elementary row operations (as listed on p. 3).
2. The row space of a matrix A, denoted by $\mathrm{Row}\, A$, is defined as the set of all linear combinations of the rows of A.
3. If we apply an elementary row operation to matrix A, the resulting matrix B has the same row space as A. Hence, if matrix C is an echelon form of A, then $\mathrm{Row}\, A = \mathrm{Row}\, C$.

An application of REF to coding theory

Problem: Let $S \subseteq K^n$. Find a basis for the code $C = \langle S \rangle$ (the code generated by S).

Recall that, by definition, C is the set of all linear combinations of elements in S.

Algorithm for solving the problem:

1. Write the elements of S as rows of a matrix A.
2. Find a REF of A and call it B.
3. The nonzero rows of B form a basis for C.

Example: Let $S = \{0101, 1001, 1100\}$. Find a basis for $C = \langle S \rangle$.

Solution: Let $A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$.

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

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

A basis for C is $\{1001, 0101\}$.

Reduced row echelon form (RREF): add the following condition to the list of conditions (1, 2, and 3) on slide #4:

4. Each leading 1 is the only nonzero entry in its column.

Example: Reduced row echelon form:

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

Theorem (Uniqueness of the reduced row echelon form)

Each matrix is row equivalent to exactly one *reduced row echelon matrix.*

Again: The RREF of a matrix is unique; the REF is not.

Example: Find the REF and RREF of

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

Solution:

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

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = B.$$

Matrix B is a REF of A.

To obtain the RREF of A, we proceed as follows:
(work on B upward and to the left, starting from the rightmost leading 1):

$$B = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \sim$$

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

Matrix C is the RREF of A.