
Outline

Recall: Looking for good codes

High info rate vs. high min distance

Hamming bound for arbitrary codes

Idea of **linear** codes

Gilbert-Varshamov bound for linear codes

Linear algebra \Leftrightarrow linear codes:

Linear combinations

Linear independence

Vector subspaces

Computational versions thereof?!

Review: Linear codes/algebra

In terms of linear algebra: linear codes of length n with alphabet \mathbf{F}_q are simply vector subspaces of the vector space \mathbf{F}_q^n of all column vectors of size n with entries in the field \mathbf{F}_q with q elements.

Yes, codes are just vector subspaces.

Definition: A linear combination of a collection of vectors v_1, \dots, v_t is any other vector w expressible as

$$w = c_1v_1 + c_2v_2 + \dots + c_tv_t$$

with scalars c_1, \dots, c_t .

Definition: A collection v_1, \dots, v_t of vectors is **linearly dependent** if there is some linear combination (not with all coefficients c_i s being 0) which is the zero vector:

$$0 = c_1v_1 + c_2v_2 + \dots + c_tv_t$$

Definition: A collection v_1, \dots, v_t of vectors is **linearly independent** if there is *no* linear combination (except with all coefficients 0) which is the zero vector.

Definition: A **vector subspace** of k^n is a set V of vectors of length n such that the **vector sum** of any two vectors in V is again in V , and any **scalar multiple** of a vector in V is again in V .

Definition: A set of vectors v_1, \dots, v_N **spans** a vector subspace V of k^n if every vector in V is a linear combination of the v_i 's.

Definition: A set of vectors v_1, \dots, v_k in a vector subspace V of k^n is a **basis** for V if the v_i *span* V and are *linearly independent*.

Proposition: For basis v_1, \dots, v_k of a vector subspace V , every vector $v \in V$ has a **unique** expression as a linear combination of the v_1, \dots, v_k .

Definition: The **dimension** of a vector subspace V of k^n is the number of elements in any basis for V .

Remark: It is important to note that the *dimension* of a vector subspace is **not** the *length* of the vectors in it.

Theorem: (see appendix) Dimension of vector subspaces is *well-defined*: any two bases have the same number of elements. ///

Row spaces, row reduction

Definition: The **row space** of an m -by- n matrix M is the vector subspace of k^n spanned by the *rows* of M .

Thus, a vector of length n is in the row space of M if and only if it is a linear combination of the rows of M .

(Analogously, the **column space** of an m -by- n matrix M is all linear combinations of columns of M .)

For computational purposes, we often describe a vector subspace of k^n as being the rowspace of a matrix. Thus, an m -by- n *matrix* can specify a vector subspace of k^n .

Elementary row operations are:

- Add scalar multiple of one row to another
- Multiply a row by a non-zero scalar
- Interchange two rows

Remark: *Elementary column operations* are analogous:

- Add scalar multiple of one column to another
- Multiply a column by a non-zero scalar
- Interchange two columns But we will not use column operations.

Remark: Row operations are *matrix multiplication* on the left by special matrices. For example, interchanging the second and third rows of

$$M = \begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix}$$

is achieved by left-multiplying M by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Adding t times the third row of M to the first row of M is left-multiplying M by

$$\begin{pmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

An m -by- n matrix M with entries M_{ij} is **(strongly) row reduced** if:

If all these entries in a row are 0, then there is no condition on this row.

If not all entries in the i^{th} row are 0, let j_i be the smallest integer so that $M_{ij_i} \neq 0$. This is the **leading entry** or **pivot** of the i^{th} row. Require that for every row index i

$$M_{ij_i} = 1$$

and

$$M_{i'j_i} = 0 \quad \text{for } i' \neq i$$

Further, we require that

$$j_i < j_{i'} \quad \text{for } i < i'$$

That is, the pivot in each row is 1, the entries above and below each pivot are 0s, and as we go down the rows, the leading entries occur further and further to the right.

Remark: A somewhat less labor-intensive version of **row reduced** is sometimes good enough for applications: we may drop the requirement that entries *above* pivots all be 0.

Example:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

is row reduced in the strong sense: the leading entry in the top row is in the first column and all other entries in the first column are 0. The leading entry in the second row is to the right of the top row's pivot, and all other entries in the second column are 0. The leading entry of the third row occurs in the fourth column, to the right of the first two pivots, and all other entries in that column are 0. The fact that the third column is *all* 0s is irrelevant. Also, the fifth and sixth columns are irrelevant.

Example:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

is *not* row reduced (in either sense): the leading entry in both first and third rows occurs in the first column.

Example:

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

is *not* row reduced, since the leading entries do *not* occur farther to the right as we move down.

Elementary row operations can be used to put a matrix into row-reduced form (in either the stronger or the weaker sense). The process of doing elementary row operations to put a matrix into row-reduced form is **row reduction**.

Example: (of strong row reduction) over the field \mathbf{F}_2 . Row reduce

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

In the first column there is a non-zero entry, but not in the first row, so *interchange* first and second rows, to get

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Since there is still a non-zero entry in the third row, subtract the first row from the third

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

The first column looks the way it should.

(recopy:)

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Treat the second column, below the first row. There are two 1s, in particular a 1 in the second row, so no interchange of rows is needed. Thus, the pivot in the second row occurs in the second column. There are two other non-zero entries in the second column (in first and third rows) so subtract the second row from first and third

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

The second column is done.

The third row has its leading entry not in the fourth column, and other entries of the fourth column are already 0s, so we are done.

Remark: The weaker row reduction does less work by not doing row operations to make entries *above* a pivot 0. This approximately cuts in half the total number of operations necessary, and is sometimes good enough.

Remark: The term *row reduced* is ambiguous, and you must look at context to guess whether it means *strongly* or *weakly* row reduced. For many purposes it does not matter.

Remark: Most often row-reduction-based algorithms are done with floating-point real numbers, where analysis of precision is critical. But here (and with finite fields in general) we in effect do not have any round-off error.

Problem: Are vectors

$$\begin{aligned}v_1 &= (v_{11}, v_{12}, \dots, v_{1,n}) \\v_2 &= (v_{21}, v_{22}, \dots, v_{2,n}) \\v_3 &= (v_{31}, v_{32}, \dots, v_{3,n}) \\&\dots \\v_m &= (v_{m1}, v_{m2}, \dots, v_{m,n})\end{aligned}$$

linearly independent? That is, are there scalars c_1, \dots, c_m in k not all 0, such that

$$c_1 v_1 + \dots + c_m v_m = 0 \text{ (zero vector)}$$

Method: Row reduce the m -by- n matrix formed with these vectors as rows. If any row of the reduced matrix is (all) 0, then the vectors were linearly *dependent*. If *no* row is all 0, then the vectors were linearly *independent*.

Example: Are the vectors

$$v_1 = (1, 1, 0, 1)$$

$$v_2 = (1, 0, 1, 1)$$

$$v_3 = (1, 1, 0, 0)$$

$$v_4 = (1, 1, 1, 1)$$

$$v_5 = (0, 1, 1, 0)$$

linearly independent, or not? Create a 5-by-4 matrix with the vectors as rows, and row-reduce it.

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \xrightarrow{\text{subs row 1}} \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

$$\xrightarrow{\text{subs row 2}} \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Though we're not done with row reduction, a row is all 0, so would stay that way. We conclude that the rows are *linearly dependent*.

Remark: From linear algebra (see appendix) *if the number of vectors is greater than the dimension, then there is a linear dependency.*

Thus, in the previous example the 5 vectors in 4-space would *have* to be linearly dependent.

Remark: The previous method does not *find* a linear dependence relation, but only determines that one exists. To *find* the coefficients, proceed as follows. Given vectors

$$\begin{aligned}v_1 &= (v_{11}, v_{12}, \dots, v_{1,n}) \\v_2 &= (v_{21}, v_{22}, \dots, v_{2,n}) \\v_3 &= (v_{31}, v_{32}, \dots, v_{3,n}) \\&\dots \\v_m &= (v_{m1}, v_{m2}, \dots, v_{m,n})\end{aligned}$$

again form a matrix with these as rows

$$M = \begin{pmatrix} v_{11} & v_{12} & \dots & v_{1,n} \\ v_{21} & v_{22} & \dots & v_{2,n} \\ v_{31} & v_{32} & \dots & v_{3,n} \\ & \dots & & \\ v_{m1} & v_{m2} & \dots & v_{m,n} \end{pmatrix}$$

The m -by- m **identity matrix** I_m has 1s on the **diagonal** and 0s off the diagonal:

$$I_m = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & & & & \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

Form the **augmented matrix** from M by sticking an m -by- m **identity matrix** onto its right end:

$$\widetilde{M} = \begin{pmatrix} v_{11} & \dots & v_{1,n} & 1 & 0 & 0 & \dots & 0 \\ v_{21} & \dots & v_{2,n} & 0 & 1 & 0 & \dots & 0 \\ v_{31} & \dots & v_{3,n} & 0 & 0 & 1 & \dots & 0 \\ \dots & & & & & & & \\ v_{m1} & \dots & v_{m,n} & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

We will row-reduce the augmented matrix to find the coefficients of a linear dependency relation, if any.

Do row operations until M (as part of \widetilde{M}) has one or more rows which are all 0s, *if possible*. (The identity matrix stuck onto M on the right will never have this property. (Weak row reduction suffices.)

Suppose the row-reduced version of \widetilde{M} is

$$\widetilde{M}_{\text{red}} = (M_{\text{red}} \quad A)$$

where M_{red} is the reduced version of M , and the m -by- m matrix A is what I_m turns into.

Let w_i be the left n entries of the i^{th} row of M_{red} . Then

$$A \begin{pmatrix} v_1 \\ v_2 \\ \dots \\ v_m \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \\ \dots \\ w_m \end{pmatrix}$$

If $m > n$ at least the last $m - n$ of the w_i s will be the zero vector. For example w_m will certainly be the length- n zero vector. That is,

$$a_{m1}v_1 + a_{m2}v_2 + a_{m3}v_3 + \dots + a_{mm}v_m = (0, \dots, 0)$$

We will have found a linear combination of the vectors v_i which is zero.

Example: Find a linear dependence relation among binary vectors

1101, 1011, 1100, 1111, 0110

Stack them up into a matrix

$$M = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

and form the augmented matrix by sticking a 5-by-5 identity matrix onto the right:

$$\widetilde{M} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Do (weak) row reduction.

We already have the pivot in the first row.

Subtract the first row from the second, third,

and fourth (not fifth) to make the other entries in the first column 0:

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

The pivot in the second row is already fine. Make all *lower* entries in the second column 0 by subtracting as necessary:

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

To get a pivot into the right spot in the third column interchange the third and fourth rows:

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

No subtractions are necessary. In the fourth column the pivot is already ok, and no subtractions are necessary. Likewise, in the fifth column the pivot is ok, and no subtractions are necessary.

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Looking at the left 4 columns of this reduced matrix (the original vectors were length 4):

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

we have a row of 0s on the bottom. Thus, taking the bottom row 11001 of the *right* part of the large reduced matrix as coefficients for a linear combination of the original vectors, we have (as expected)

$$1 \cdot 1101 + 1 \cdot 1011 + 0 \cdot 1100 + 0 \cdot 1111 + 1 \cdot 0110 = 0000$$