The Least Squares Solution of Linear Systems

Carlo Tomasi

March 1, 2022

As a refresher of prerequisite materials, Section 1 characterizes the existence and multiplicity of the solutions of a linear system in terms of the four fundamental spaces associated with the system's matrix and of the relationship of the right-hand side vector of the system to that subspace. Additional useful facts from linear algebra, including a definition of the four spaces and of the notion of orthogonal matrices, are collected in the Appendices for easy reference. Some of the Appendices also prove several of the results stated in this note.

As usual, Appendices are optional reading. However, *the non-proof materials in the Appendices to this note are course prerequisites, so you are expected to know them.*

Moving to a possibly new topic, Section 2 introduces the all-important concept of the Singular Value Decomposition (SVD). Sections 3 and 4 then show how to use the SVD to solve linear systems in the sense of least squares.

1 The Solutions of a Linear System

Let

$$A\mathbf{x} = \mathbf{b}$$

be an $m \times n$ system (m can be less than, equal to, or greater than n). Also, let

$$r = \text{rank}(A)$$

be the number of linearly independent rows or columns of A. Then,[1]

$$\begin{array}{lcl} \mathbf{b} \notin \text{range}(A) & \Rightarrow & \text{no solutions} \\ \mathbf{b} \in \text{range}(A) & \Rightarrow & \infty^{n-r} \text{ solutions} \end{array}$$

with the convention that $\infty^0 = 1$. Here, ∞^k is the cardinality of a k-dimensional affine vector space on the reals.

In the first case above, there can be no linear combination of the columns (no $\mathbf{x}$ vector) that gives $\mathbf{b}$, and the system is said to be *incompatible*. In the second, *compatible* case, three possibilities occur, depending on the relative sizes of r, m, n:

- When $r = n = m$, the system is *invertible*. This means that there is exactly one $\mathbf{x}$ that satisfies the system, since the columns of A span all of $\mathbf{R}^n$. Notice that invertibility depends only on A, not on $\mathbf{b}$.

[1] Here and elsewhere, the *range* of a matrix is synonymous to its *column space*. Appendix A recalls the definitions of the four fundamental spaces associated with a linear transformation.

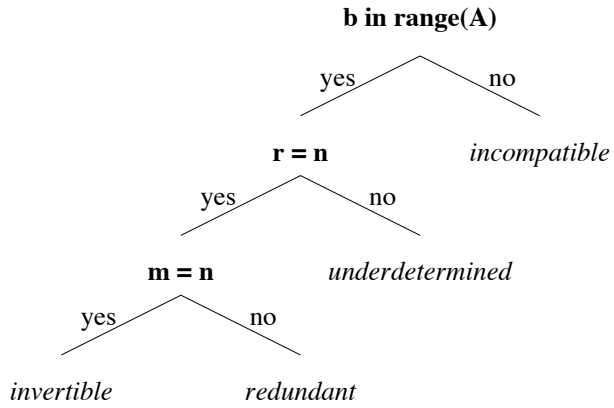

Figure 1: Types of linear systems.

- When $r = n$ and $m > n$, the system is *redundant*. There are more equations than unknowns, but since $\mathbf{b}$ is in the range of A there is a linear combination of the columns (a vector $\mathbf{x}$) that produces $\mathbf{b}$. In other words, the equations are compatible, and exactly one solution exists.[2]

- When $r < n$ the system is *underdetermined*. This means that the null space is nontrivial (*i.e.*, it has dimension $h > 0$), and there is a linear space of dimension $h = n - r$ of vectors $\mathbf{x}$ such that $A\mathbf{x} = 0$. Since $\mathbf{b}$ is assumed to be in the range of A, there are solutions $\mathbf{x}$ to $A\mathbf{x} = \mathbf{b}$, but then for any $\mathbf{y} \in \text{null}(A)$ also $\mathbf{x} + \mathbf{y}$ is a solution:

$$A\mathbf{x} = \mathbf{b}\,,\ A\mathbf{y} = 0 \ \Rightarrow\ A(\mathbf{x} + \mathbf{y}) = \mathbf{b}$$

  and this generates the $\infty^h = \infty^{n-r}$ solutions mentioned above.

Notice that if $r = n$ then n cannot possibly exceed m (or else the columns of A would form an n-dimensional subspace of an m-dimensional space with $m < n$, an impossibility), so the first two cases exhaust the possibilities for $r = n$. Also, r cannot exceed either m or n. All the cases are summarized in figure 1.

Thus, a linear system has either zero (incompatible), one (invertible or redundant), or more (underdetermined) solutions. In all cases, we can say that the set of solutions forms an *affine space*, that is, a linear space $\mathcal{L}$ plus a vector:

$$\mathcal{A} = \hat{\mathbf{x}} + \mathcal{L}\ .$$

Recall that the sum here means that the single vector $\hat{\mathbf{x}}$ is added to every vector of the linear space $\mathcal{L}$ to produce the affine space $\mathcal{A}$. For instance, if $\mathcal{L}$ is a plane through the origin (recall that all linear spaces must contain the origin), then $\mathcal{A}$ is a plane (not necessarily through the origin) that is parallel to $\mathcal{L}$.

In the underdetermined case, the geometric nature of $\mathcal{A}$ is obvious. However, the notation used above for affine spaces also applies to the incompatible case: in this case, $\mathcal{L}$ is the empty linear space, so $\hat{\mathbf{x}} + \mathcal{L}$ is empty as well, and $\hat{\mathbf{x}}$ is undetermined.

[2]Notice that the technical meaning of "redundant" has a stronger meaning than "with more equations than unknowns." The case $r < n < m$ is possible, has more equations (m) than unknowns (n), admits a solution if $\mathbf{b} \in \text{range}(A)$, but is called "underdetermined" because there are fewer (r) independent equations than there are unknowns (see next item). Thus, "redundant" means "with exactly one solution and with more equations than unknowns."

Please do not confuse the empty linear space (a space with no elements) with the linear space that contains only the zero vector (a space with one element). The latter yields either the invertible or the redundant case.

Of course, listing all possibilities does not provide an operational method for determining the type of linear system for a given pair $A, \mathbf{b}$. Section 2 introduces the Singular Value decomposition (SVD), a fundamental tool of linear algebra. The two subsequent Sections use the SVD to show how to determine the type of a system, and how to solve it. They also give meaning to the expression "solving the system" when no exact solution exists, which occurs most of the time in practice. Section 4, in particular, defines a concept of "solution" that is typically useful and interesting in the case $\mathbf{b} = \mathbf{0}$, when the exact solution is trivial and uninteresting.

2 The Singular Value Decomposition

Here is the main intuition captured by the Singular Value Decomposition (SVD) of a matrix:

> An $m \times n$ matrix A of rank r maps the r-dimensional unit hypersphere in row space(A) into an r-dimensional hyperellipse in range(A).

Thus, a hypersphere is stretched or compressed into a hyperellipse, which is a quadratic hypersurface that generalizes the two-dimensional notion of ellipse to an arbitrary number of dimensions. In three dimensions, the hyperellipse is an ellipsoid, in one dimension it is a pair of points. In all cases, the hyperellipse in question is centered at the origin.

For instance, the rank-2 matrix

$$A = \frac{1}{\sqrt{2}} \begin{bmatrix} \sqrt{3} & \sqrt{3} \\ -3 & 3 \\ 1 & 1 \end{bmatrix} \tag{1}$$

transforms the unit circle on the plane into an ellipse embedded in three-dimensional space. Figure 2 shows the map

$$\mathbf{b} = A\mathbf{x} \; .$$

There are two diametrically opposite points $\mathbf{v}_1$ and $-\mathbf{v}_1$ on the unit circle that are mapped into the two endpoints $\sigma_1\mathbf{u}_1$ and $-\sigma_1\mathbf{u}_1$ of the major axis of the ellipse. Similarly, two other diametrically opposite points $\mathbf{v}_2$ and $-\mathbf{v}_2$ on the unit circle are mapped into the two endpoints $\sigma_2\mathbf{u}_2$ and $-\sigma_2\mathbf{u}_2$ of the minor axis of the ellipse. The lines through these two pairs of points on the unit circle are always orthogonal to each other. This result can be generalized to any $m \times n$ matrix.

Simple and fundamental as this geometric fact may be, its proof by geometric means is cumbersome. It is, on the other hand, a straightforward consequence of the following fundamental theorem, proven in the Appendix, which states the existence of the SVD.

Theorem 2.1. *If A is a real $m \times n$ matrix then there exist orthogonal matrices*

$$\begin{aligned} U &= \begin{bmatrix} \mathbf{u}_1 & \cdots & \mathbf{u}_m \end{bmatrix} \in \mathcal{R}^{m \times m} \\ V &= \begin{bmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{bmatrix} \in \mathcal{R}^{n \times n} \end{aligned}$$

such that

$$U^T A V = \Sigma = \mathrm{diag}(\sigma_1, \ldots, \sigma_p) \in \mathcal{R}^{m \times n}$$

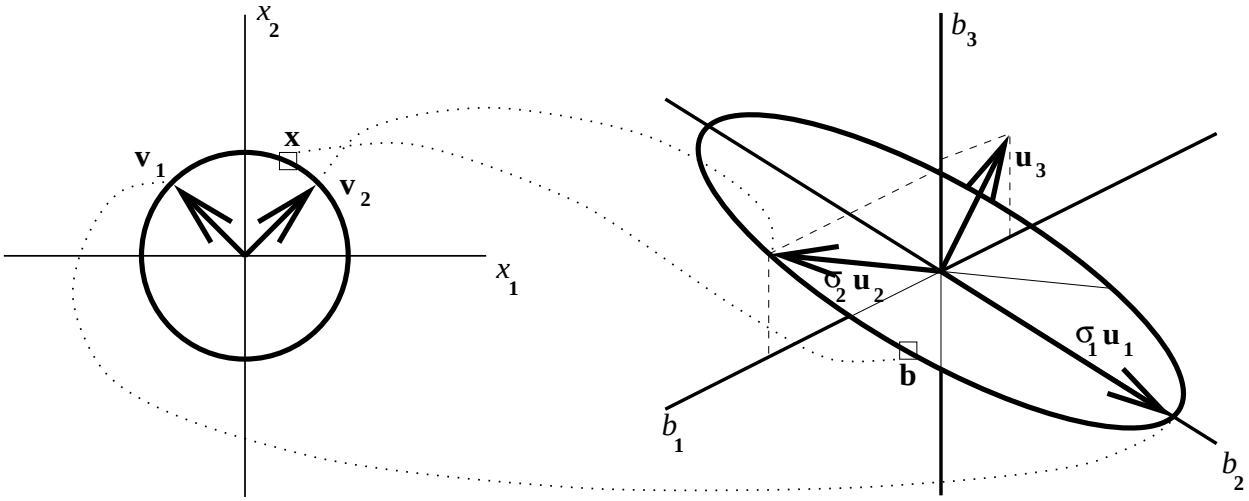

Figure 2: The matrix in equation (1) maps a circle on the plane into an ellipse in space. The two small boxes are corresponding points.

where $p = \min(m, n)$ *and* $\sigma_1 \geq \ldots \geq \sigma_p \geq 0$. *Equivalently,*

$$A = U\Sigma V^T \ .$$

The columns of V are the *right singular vectors* of A, and those of U are its *left singular vectors*. The diagonal entries of Σ are the *singular values* of A. The ratio

$$\kappa(A) = \sigma_1/\sigma_p \tag{2}$$

is the *condition number* of A, and is possibly infinite.

The singular value decomposition is "almost unique". There are two sources of ambiguity. The first is in the orientation of the singular vectors. By rewriting the equation $A = U\Sigma V^T$ in the following form,

$$A = \sum_{i=1}^{n} \sigma_i \mathbf{u}_i \mathbf{v}_i^T \ ,$$

we see that one can flip (change the sign of) any right singular vector $\mathbf{v}_i$, provided that the corresponding left singular vector $\mathbf{u}_i$ is flipped as well, and still obtain a valid SVD. Singular vectors must be flipped in pairs (a left vector and its corresponding right vector) because the singular values are required to be nonnegative. This is a trivial ambiguity. If desired, it can be removed by imposing, for instance, that the first nonzero entry of every left singular value be positive.

The second source of ambiguity is deeper. If the matrix A maps a hypersphere into another hypersphere, that is, a hyper-ellipsoid with equally long axes, then the axes of the latter are not uniquely defined. For instance, the identity matrix has an infinity of SVDs, all of the form

$$I = UIU^T$$

where U is any orthogonal matrix of suitable size. More generally, whenever two or more singular values coincide, the subspaces identified by the corresponding left and right singular vectors are unique, but any orthonormal basis can be chosen within, say, the right subspace and yield, together with the corresponding left singular vectors, a valid SVD. Except for these ambiguities, the SVD is unique.

Even in the general case, the singular values of a matrix A are the lengths of the semi-axes of the hyperellipse E defined by

$$E = \{A\mathbf{x} : \|\mathbf{x}\| = 1\} .$$

The SVD reveals a great deal about the structure of a matrix. If we define r by

$$\sigma_1 \geq \ldots \geq \sigma_r > \sigma_{r+1} = \ldots = 0 ,$$

that is, if σ_r is the smallest nonzero singular value of A, then

$$\text{rank}(A) = r$$

and the singular vectors provide orthonormal bases for the four fundamental spaces of A:

$$\begin{aligned} \text{null}(A) &= \text{span}\{\mathbf{v}_{r+1}, \ldots, \mathbf{v}_n\} \\ \text{range}(A) &= \text{span}\{\mathbf{u}_1, \ldots, \mathbf{u}_r\} \\ \text{row space}(A) &= \text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_r\} \\ \text{left null}(A) &= \text{span}\{\mathbf{u}_{r+1}, \ldots, \mathbf{u}_m\} . \end{aligned}$$

The sizes of the matrices in the SVD are as follows: U is $m \times m$, Σ is $m \times n$, and V is $n \times n$. Thus, Σ has the same shape and size as A, while U and V are square. However, if $m > n$, the bottom $(m-n) \times n$ block of Σ is zero, so that the last $m-n$ columns of U are multiplied by zero. Similarly, if $m < n$, the rightmost $m \times (n-m)$ block of Σ is zero, and this multiplies the last $n-m$ rows of V. This suggests a "small," equivalent version of the SVD. If $p = \min(m, n)$, we can define $U_p = U(:, 1:p)$, $\Sigma_p = \Sigma(1:p, 1:p)$, and $V_p = V(:, 1:p)$, and write

$$A = U_p \Sigma_p V_p^T$$

where U_p is $m \times p$, Σ_p is $p \times p$, and V_p is $n \times p$.

Moreover, if $p - r$ singular values are zero, we can let $U_r = U(:, 1:r)$, $\Sigma_r = \Sigma(1:r, 1:r)$, and $V_r = V(:, 1:r)$, then we have

$$A = U_r \Sigma_r V_r^T = \sum_{i=1}^{r} \sigma_i \mathbf{u}_i \mathbf{v}_i^T ,$$

which is an even smaller, *minimal*, SVD (also known as the *tiny* SVD).

Finally, both the Frobenius norm

$$\|A\|_F = \sqrt{\sum_{i=1}^{m} \sum_{j=1}^{n} |a_{ij}|^2}$$

and the 2-norm

$$\|A\|_2 = \sup_{\mathbf{x} \neq 0} \frac{\|A\mathbf{x}\|}{\|\mathbf{x}\|} \tag{3}$$

of the matrix A are neatly characterized in terms of the SVD:

$$\begin{aligned} \|A\|_F &= \sqrt{\sigma_1^2 + \ldots + \sigma_p^2} \\ \|A\|_2 &= \sigma_1 \ . \end{aligned}$$

The Golub-Reinsch Algorithm The SVD was established by Eugenio Beltrami in 1873 [1]. Interestingly, he did *not* use matrix notation in his formulation or derivation. The SVD became one of the main tools in numerical linear algebra after 1970, when Gene Golub and Christian Reinsch published a numerically stable and efficient algorithm for its computation [3] based on an earlier version by Golub and Kahan [2].

The Golub-Reinsch algorithm works by repeatedly multiplying A by orthogonal matrices from the left and from the right. Since orthogonal matrices do not change the magnitudes of vectors, these multiplications do not amplify the numerical errors that derive from the use of finite-precision arithmetic. This fact is the reason for the stability of the algorithm.

3 The Pseudoinverse

One of the most important applications of the SVD is the solution of linear systems in the least squares sense. A linear system of the form

$$A\mathbf{x} = \mathbf{b} \tag{4}$$

arising from a real-life application may or may not admit a solution, that is, a vector $\mathbf{x}$ that satisfies this equation exactly. Often more measurements are available than strictly necessary, because measurements are unreliable. This leads to more equations than unknowns (the number m of rows in A is greater than the number n of columns), and equations are often mutually incompatible because they come from inexact measurements. Even when $m \leq n$ the equations can be incompatible, because of errors in the measurements that produce the entries of A. In these cases, it makes more sense to find a vector $\mathbf{x}$ that minimizes the norm

$$\|A\mathbf{x} - \mathbf{b}\|$$

of the *residual* vector

$$\mathbf{r} = A\mathbf{x} - \mathbf{b}$$

where the double bars henceforth refer to the Euclidean norm. Thus, $\mathbf{x}$ cannot exactly satisfy any of the m equations in the system, but it tries to satisfy all of them as closely as possible, as measured by the sum of the squares of the discrepancies between left- and right-hand sides of the equations.

In other circumstances, not enough measurements are available. Then, the linear system (4) is under-determined, in the sense that it has fewer *independent* equations than unknowns (its rank r is less than n).

Incompatibility and under-determinacy can occur together: the system admits no solution, and the least-squares solution is not unique. For instance, the system

$$\begin{aligned} x_1 + x_2 &= 1 \\ x_1 + x_2 &= 3 \\ x_3 &= 2 \end{aligned}$$

has three unknowns, but rank 2, and its first two equations are incompatible: $x_1 + x_2$ cannot be equal to both 1 and 3. A least-squares solution turns out to be $\mathbf{x} = [1\ 1\ 2]^T$ with residual

$$\mathbf{r} = A\mathbf{x} - \mathbf{b} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} - \begin{bmatrix} 1 \\ 3 \\ 2 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \\ 2 \end{bmatrix} - \begin{bmatrix} 1 \\ 3 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix},$$

which has norm $\sqrt{2}$ (admittedly, this is a rather high residual, but this is the best we can do for this problem, in the least-squares sense). However, any other vector of the form

$$\mathbf{x}' = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} + \alpha \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix}$$

is as good as $\mathbf{x}$. For instance, $\mathbf{x}' = [0\ 2\ 2]$, obtained for $\alpha = 1$, yields exactly the same residual as $\mathbf{x}$ (check this).

In summary, an exact solution to the system (4) may not exist, or may not be unique. An approximate solution, in the least-squares sense, always exists, but may fail to be unique.

If there are several least-squares solutions, all equally good (or bad), then one of them turns out to be shorter than all the others, that is, its norm $\|\mathbf{x}\|$ is smallest. One can therefore redefine what it means to "solve" a linear system so that there is always exactly one solution. This minimum-norm solution is the subject of the following theorem, which both establishes uniqueness and provides a recipe for the computation of the solution. The theorem is proven in an Appendix.

Theorem 3.1. *The minimum-norm least-squares solution to a linear system $A\mathbf{x} = \mathbf{b}$, that is, the shortest vector $\mathbf{x}$ that achieves the*

$$\min_{\mathbf{x}} \|A\mathbf{x} - \mathbf{b}\|,$$

is unique, and is given by

$$\hat{\mathbf{x}} = V\Sigma^\dagger U^T \mathbf{b} \tag{5}$$

where $A = U\Sigma V^T$ is the SVD of the rank-r matrix A and

$$\Sigma^\dagger = \begin{bmatrix} 1/\sigma_1 & & & & & 0 & \cdots & 0 \\ & \ddots & & & & & & \\ & & 1/\sigma_r & & & \vdots & & \vdots \\ & & & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & 0 & \cdots & 0 \end{bmatrix}.$$

The matrix

$$A^\dagger = V\Sigma^\dagger U^T$$

is called the *pseudoinverse* of A. The pseudo-inverse $\Sigma^\dagger$ of Σ is spelled out above in the case in which the $m \times n$ matrix A has no fewer rows than columns ($m \geq n$). Regardless of the relative size

of m and n, the matrix Σ is $m \times n$ (the same size of A) and the pseudo-inverse $\Sigma^\dagger$ of Σ is $n \times m$. When $m < n$, there are extra zero rows in $\Sigma^\dagger$, rather than extra zero columns:

$$\Sigma^\dagger = \begin{bmatrix} 1/\sigma_1 & & & & & \\ & \ddots & & & & \\ & & 1/\sigma_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \\ 0 & & \cdots & & & 0 \\ \vdots & & & & & \vdots \\ 0 & & \cdots & & & 0 \end{bmatrix}.$$

4 Least-Squares Solution of a Homogeneous Linear Systems

Theorem 3.1 holds regardless of the value of the right-hand side vector $\mathbf{b}$. When $\mathbf{b} = \mathbf{0}$, that is, when the system is *homogeneous*, the solution is trivial: the minimum-norm solution to

$$A\mathbf{x} = \mathbf{0} \tag{6}$$

is

$$\mathbf{x} = \mathbf{0}\,,$$

which happens to be an exact solution. Of course it is not necessarily the only solution (any vector in the null space of A is also a solution, by definition), but it is obviously the one with the smallest norm.

Thus, $\mathbf{x} = \mathbf{0}$ is the unique minimum-norm solution to any homogeneous linear system. Although correct, this solution is not too interesting. In many applications, what is desired is a *nonzero* vector $\mathbf{x}$ that satisfies the system (6) as well as possible. Without any constraints on $\mathbf{x}$, we would fall back to $\mathbf{x} = \mathbf{0}$ again. For homogeneous linear systems, the meaning of a least-squares solution is therefore usually modified, once more, by imposing the constraint

$$\|\mathbf{x}\| = 1$$

on the solution. Unfortunately, the resulting constrained minimization problem does not necessarily admit a *unique* solution. The following theorem provides a recipe for finding this solution, and shows that there is in general a whole hypersphere of solutions.

Theorem 4.1. *Let*

$$A = U\Sigma V^T$$

be the singular value decomposition of the $m \times n$ matrix A, and let $r = \operatorname{rank}(A)$. Furthermore, define

$$i = \begin{cases} r+1 & \text{if } r < n \\ \min\{j \,|\, 1 \le j \le n \text{ and } \sigma_j = \sigma_n\} & \text{otherwise.} \end{cases}$$

In words, if A has a nontrivial null space, then i indexes the first column of V in the orthogonal basis of the null space of A. Otherwise, i indexes the first column of V whose corresponding singular value σ_i is equal to the smallest (and last) singular value σ_n.

Then, all vectors of the form

$$\mathbf{x} = \alpha_1 \mathbf{v}_i + \ldots + \alpha_k \mathbf{v}_n$$

with

$$k = n - i + 1 \quad \textit{and} \quad \alpha_1^2 + \ldots + \alpha_k^2 = 1$$

are unit-norm least-squares solutions to the homogeneous linear system

$$A\mathbf{x} = \mathbf{0},$$

that is, they achieve the

$$\min_{\|\mathbf{x}\|=1} \|A\mathbf{x}\| \ .$$

When $r = n$, the last singular value σ_n of A is nonzero, and it is very unlikely that other singular values have *exactly* the same numerical value as σ_n. Because of this, the most common case when $r = n$ is $n = i$ and therefore $k = 1$. When $r < n$, on the other hand, the matrix A may often have more than one singular value equal to zero. Either way, if $k = 1$, then the minimum-norm solution is unique, $\mathbf{x} = \mathbf{v}_n$. If $k > 1$, then $\mathbf{x} = \mathbf{v}_n$ is still *a* unit-norm least-squares solution. To summarize, while the theorem above shows how to express *all* solutions as a linear combination of the last k columns of V, the following weaker result holds as well, and is of significant practical importance.

Corollary 4.2. *Let*

$$A = U\Sigma V^T$$

be the singular value decomposition of the $m \times n$ matrix A, and let $r = \mathrm{rank}(A)$. Then, the last column of V,

$$\mathbf{x} = \mathbf{v}_n$$

is a (possibly not unique) unit-norm least-squares solutions to the homogeneous linear system

$$A\mathbf{x} = \mathbf{0},$$

that is

$$\min_{\|\mathbf{x}\|=1} \|A\mathbf{x}\| = \|A\mathbf{v}_n\| = \sigma_n \ .$$

In this expression, σ_n is the last singular value of A, and is equal to zero when $r < n$.

References

[1] E. Beltrami. Sulle funzioni bilineari. *Giornale di Matematiche ad Use degli Studenti Delle Università*, 11:98–106, 1973.

[2] G. H. Golub and W. Kahan. Calculating the singular values and pseudo-inverse of a matrix. *Journal of the Society for Industrial and Applied Mathematics - B*, 2(2):205–224, 1965.

[3] G. H. Golub and C. Reinsch. Singular value decomposition and least squares solutions. *Numerische Mathematik*, 14(5):403–420, 1970.

Appendices

A Linear Transformations

Linear transformations map spaces into spaces. It is important to understand exactly what is being mapped into what in order to determine whether a linear system has solutions, and if so how many.

Two vector spaces A and B are said to be *orthogonal* to one another when every vector in A is orthogonal to every vector in B. If vector space A is a subspace of $\mathbf{R}^m$ for some m, then the *orthogonal complement* of A is the set of all vectors in $\mathbf{R}^m$ that are orthogonal to all the vectors in A.

Notice that complement and orthogonal complement are very different notions. For instance, the complement of the xy plane in $\mathbf{R}^3$ is all of $\mathbf{R}^3$ except the xy plane, while the orthogonal complement of the xy plane is the z axis.

Results in this Appendix are given without proof, and more details on orthogonal matrices are recalled in Appendix B.

Theorem A.1. *If A is a subspace of $\mathbf{R}^m$ and $A^\perp$ is the orthogonal complement of A in $\mathbf{R}^m$, then*

$$\dim(A) + \dim(A^\perp) = m \ .$$

We can now start to talk about matrices in terms of the subspaces associated with them. The *null space* $\text{null}(A)$ of an $m \times n$ matrix A is the space of all n-dimensional vectors that are orthogonal to the rows of A. The *range* of A is the space of all m-dimensional vectors that are generated by the columns of A. Thus, $\mathbf{x} \in \text{null}(A)$ iff $A\mathbf{x} = 0$, and $\mathbf{b} \in \text{range}(A)$ iff $A\mathbf{x} = \mathbf{b}$ for some $\mathbf{x}$. This can be restated into the following immediate but very important statement:

Theorem A.2. *The matrix A transforms a vector $\mathbf{x}$ in its null space into the zero vector, and an arbitrary vector $\mathbf{x}$ into a vector in* $\text{range}(A)$.

The spaces orthogonal to $\text{null}(A)$ and $\text{range}(A)$ occur frequently enough to deserve names of their own. The space $\text{range}(A)^\perp$ is called the *left nullspace* of the matrix, and $\text{null}(A)^\perp$ is called the *rowspace* of A. A frequently used synonym for "range" is *column space*. It should be obvious from the meaning of these spaces that

$$\begin{aligned} \text{null}(A)^\perp &= \text{range}(A^T) \\ \text{range}(A)^\perp &= \text{null}(A^T) \end{aligned}$$

where A^T is the *transpose* of A, defined as the matrix obtained by exchanging the rows of A with its columns.

In summary, four spaces are associated with an $m \times n$ matrix A:

$\text{range}(A)$;
$\text{null}(A)$;
$\text{range}(A)^\perp = \text{left null}(A)$;
$\text{null}(A)^\perp = \text{row space}(A)$.

In order to count solutions to a linear system, it is important to establish how the dimensions of these spaces relate to each other. From theorem A.1, if null(A) has dimension h, then the space generated by the rows of A has dimension $r = n - h$, that is, A has $n - h$ linearly independent rows. It is not obvious that the space generated by the *columns* of A has also dimension $r = n - h$. Even more strongly, the following theorem holds:

Theorem A.3. *The matrix A establishes a one-to-one mapping between* row space(A) *and* range(A).

Thus, the two linear vector spaces row space(A) and range(A) are isomorphic to each other, and therefore have equal dimension. In summary, if we define

$r = \dim(\text{range}(A))$
$h = \dim(\text{null}(A))$

then theorems A.1 and A.3 yield the following:

$\dim(\text{left null}(A)) = \dim(\text{range}(A)^\perp) = m - r$
$\dim(\text{row space}(A)) = \dim(\text{null}(A)^\perp) = n - h = r$.

This also implies the following result:

Corollary A.4. *The number r of linearly independent columns of any $m \times n$ matrix A is equal to the number of its independent rows.*

As a result, we can define the *rank* of A to be equivalently the number of linearly independent columns or of linearly independent rows of A:

$$r = \text{rank}(A) = \dim(\text{range}(A)) = n - \dim(\text{null}(A)) = n - h \ .$$

Note that if $A\mathbf{x} = \mathbf{b}$, then for any vector $\mathbf{y} \in \text{null}(A)$ we also have $A(\mathbf{x} + \mathbf{y}) = A\mathbf{x} + A\mathbf{y} = A\mathbf{x}$ because $A\mathbf{y} = 0$. Therefore, the matrix A maps vectors in R^n that differ only by a vector in null(A) to the same point. Since row space(A) is isomorphic to range(A), it is then convenient to take each point $\mathbf{x}_r$ of row space(A) as a representative of the *affine space*

$$\mathcal{A}(\mathbf{x}_r) = \mathbf{x}_r + \text{null}(A)$$

of points that all map to the single point $A\mathbf{x}_r$. The sum in the expression above means that the single vector $\mathbf{x}_r$ is added to every vector of the linear space null(A) to produce the affine space $\mathcal{A}(\mathbf{x}_r)$.

The foregoing discussion allows forming the picture of a linear mapping shown in figure 3.

As a brief aside, the picture of the isomorphism between the two linear spaces row space(A) and range(A) can be made stronger by observing that A also transforms any basis for row space(A) into a basis for range(A). This is not immediately obvious, since if $\mathbf{v}_1, \ldots, \mathbf{v}_r$ are a basis for row space(A) then $A\mathbf{v}_1, \ldots, A\mathbf{v}_r$ might conceivably be dependent, or fail to span all of range(A). However, this is not so:

Theorem A.5. *If the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_r$ are a basis for* row space(A)*, then the vectors $A\mathbf{v}_1, \ldots, A\mathbf{v}_r$ are a basis for* range(A).

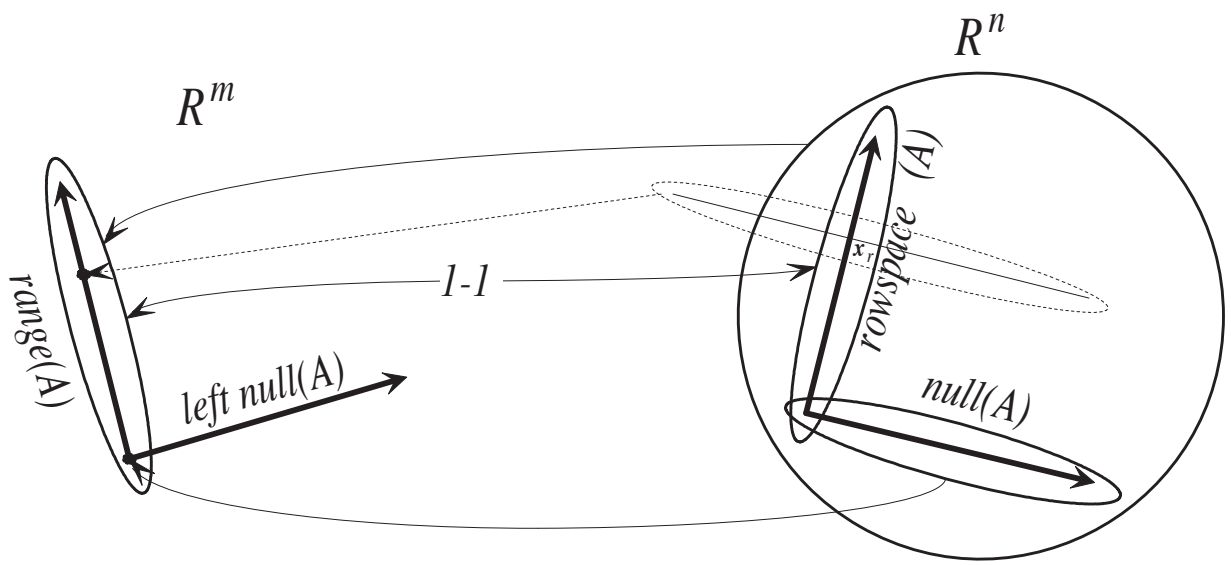

Figure 3: An $m \times n$ matrix A maps all of R^n to range(A) (top arrow), and null(A) to zero (bottom arrow). The row space and range of A are isomorphic to each other (*i.e.*, in 1-1 correspondence), and for each point $\mathbf{x}_r \in$ row space(A) there is an affine space $\mathbf{x}_r +$ null(A) of dimension $h =$ dim(null(A)) $= n -$ rank(A) that maps (dotted arrow) to the single point $A\mathbf{x}_r$.

B More on Orthogonal Matrices

Let $\mathcal{S}$ be an n-dimensional subspace of $\mathbf{R}^m$ (so that we necessarily have $n \leq m$), and let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be an orthonormal basis for $\mathcal{S}$. Consider a point P in $\mathcal{S}$. If the coordinates of P in $\mathbf{R}^m$ are collected in an m-dimensional vector

$$\mathbf{p} = \begin{bmatrix} p_1 \\ \vdots \\ p_m \end{bmatrix} ,$$

and since P is in $\mathcal{S}$, it must be possible to write $\mathbf{p}$ as a linear combination of the $\mathbf{v}_j$s. In other words, there must exist coefficients

$$\mathbf{q} = \begin{bmatrix} q_1 \\ \vdots \\ q_n \end{bmatrix}$$

such that

$$\mathbf{p} = q_1\mathbf{v}_1 + \ldots + q_n\mathbf{v}_n = V\mathbf{q}$$

where

$$V = \begin{bmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{bmatrix}$$

is an $m \times n$ matrix that collects the basis for $\mathcal{S}$ as its columns. Then for any $i = 1, \ldots, n$ we have

$$\mathbf{v}_i^T\mathbf{p} = \mathbf{v}_i^T \sum_{j=1}^{n} q_j\mathbf{v}_j = \sum_{j=1}^{n} q_j\mathbf{v}_i^T\mathbf{v}_j = q_i ,$$

since the $\mathbf{v}_j$ are orthonormal. This is important, and may need emphasis:

If

$$\mathbf{p} = \sum_{j=1}^{n} q_j \mathbf{v}_j$$

and the vectors of the basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *are orthonormal, then the coefficients* q_j *are the signed magnitudes of the projections of* $\mathbf{p}$ *onto the basis vectors:*

$$q_j = \mathbf{v}_j^T \mathbf{p} \; . \tag{7}$$

In matrix form,

$$\mathbf{q} = V^T \mathbf{p} \; . \tag{8}$$

Also, we can collect the n^2 equations

$$\mathbf{v}_i^T \mathbf{v}_j = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

into the following matrix equation:

$$V^T V = I \tag{9}$$

where I is the $n \times n$ identity matrix. A matrix V that satisfies equation (9) is said to be *orthogonal*. Thus, a matrix is orthogonal if its columns are orthonormal. Since the *left inverse* of a matrix V is defined as the matrix L such that

$$LV = I \; , \tag{10}$$

comparison with equation (9) shows that the left inverse of an orthogonal matrix V exists, and is equal to the transpose of V.

Of course, this argument requires V to be full rank, so that the solution L to equation (10) is unique. However, V is certainly full rank, because it is made of orthonormal columns.

Notice that $VR = I$ cannot possibly have a solution when $m > n$, because the $m \times m$ identity matrix has m linearly independent [3] columns, while the columns of VR are linear combinations of the n columns of V, so VR can have at most n linearly independent columns.

This result is obiously still valid when V is $m \times m$ and has orthonormal columns, since equation (9) still holds. However, for square, full-rank matrices ($r = m = n$), the distinction between left and right inverse vanishes. To see this, let L and R be the left and right inverse of a square, full-rank matrix A:

$$LA = I \quad \text{and} \quad AR = I \; .$$

Then, we can write

$$L = LI = L(AR) = (LA)R = IR = R \quad \text{so that} \quad L = R$$

as promised. Thus, if V is orthogonal and square, equation (9) yields

$$VV^T = V^T V = I \; .$$

Since the matrix VV^T contains the inner products between the *rows* of V (just as $V^T V$ is formed by the inner products of its *columns*), the argument above shows that the rows of a *square* orthogonal matrix are orthonormal as well. We can summarize this discussion as follows:

[3] Nay, orthonormal.

Theorem B.1. *The left inverse of an orthogonal $m \times n$ matrix V with $m \geq n$ exists and is equal to the transpose of V:*

$$V^T V = I \ .$$

In particular, if $m = n$, the matrix $V^{-1} = V^T$ is also the right inverse of V:

$$V \text{ square} \quad \Rightarrow \quad V^{-1}V = V^T V = VV^{-1} = VV^T = I \ .$$

Sometimes, when $m = n$, the geometric interpretation of equation (8) causes confusion, because two interpretations of it are possible. In the interpretation given above, the point P remains the same, and the underlying reference frame is changed from the elementary vectors $\mathbf{e}_j$ (that is, from the columns of I) to the vectors $\mathbf{v}_j$ (that is, to the columns of V). Alternatively, equation (8) can be seen as a transformation, in a fixed reference system, of point P with coordinates $\mathbf{p}$ into a different point Q with coordinates $\mathbf{q}$. This, however, is relativity, and should not be surprising: If you spin clockwise on your feet, or if you stand still and the whole universe spins counterclockwise around you, the result is the same.[4]

Consistently with either of these geometric interpretations, we have the following result:

Theorem B.2. *The norm of a vector $\mathbf{x}$ is not changed by multiplication by an orthogonal matrix V:*

$$\|V\mathbf{x}\| = \|\mathbf{x}\| \ .$$

The proof is a one-liner, so it is included here:

$$\|V\mathbf{x}\|^2 = \mathbf{x}^T V^T V\mathbf{x} = \mathbf{x}^T\mathbf{x} = \|\mathbf{x}\|^2 \ .$$

We conclude this section with an obvious but useful consequence of orthogonality. First, define the *projection* $\mathbf{p}$ of a point $\mathbf{b} \in \mathbf{R}^n$ *onto a subspace* C as the point in C that is closest to $\mathbf{b}$. The following theorem, proven in the Appendix, shows how to project a point onto the range of an orthogonal matrix, and how the point and its projection relate to each other.

Theorem B.3. *Let U be an orthogonal matrix. Then the matrix UU^T projects any vector $\mathbf{b}$ onto* range(U)*. Furthermore, the difference vector between $\mathbf{b}$ and its projection $\mathbf{p}$ onto* range(U) *is orthogonal to* range(U)*:*

$$U^T(\mathbf{b} - \mathbf{p}) = \mathbf{0} \ .$$

C Proofs

Theorem B.3

Let U be an orthogonal matrix. Then the matrix UU^T projects any vector $\mathbf{b}$ onto range(U)*. Furthermore, the difference vector between $\mathbf{b}$ and its projection $\mathbf{p}$ onto* range(U) *is orthogonal to* range(U)*:*

$$U^T(\mathbf{b} - \mathbf{p}) = \mathbf{0} \ .$$

[4] At least geometrically. One solution may be more efficient than the other in other ways.

Proof. A point $\mathbf{p}$ in range(U) is a linear combination of the columns of U:

$$\mathbf{p} = U\mathbf{x}$$

where $\mathbf{x}$ is the vector of coefficients (as many coefficients as there are columns in U). The squared distance between $\mathbf{b}$ and $\mathbf{p}$ is

$$\|\mathbf{b} - \mathbf{p}\|^2 = (\mathbf{b} - \mathbf{p})^T(\mathbf{b} - \mathbf{p}) = \mathbf{b}^T\mathbf{b} + \mathbf{p}^T\mathbf{p} - 2\mathbf{b}^T\mathbf{p} = \mathbf{b}^T\mathbf{b} + \mathbf{x}^T U^T U\mathbf{x} - 2\mathbf{b}^T U\mathbf{x} \; .$$

Because of orthogonality, $U^T U$ is the identity matrix, so

$$\|\mathbf{b} - \mathbf{p}\|^2 = \mathbf{b}^T\mathbf{b} + \mathbf{x}^T\mathbf{x} - 2\mathbf{b}^T U\mathbf{x} \; .$$

The derivative of this squared distance with respect to $\mathbf{x}$ is the vector

$$2\mathbf{x} - 2U^T\mathbf{b}$$

which is zero iff

$$\mathbf{x} = U^T\mathbf{b} \; ,$$

that is, when

$$\mathbf{p} = U\mathbf{x} = UU^T\mathbf{b}$$

as promised.

For this value of $\mathbf{p}$ the difference vector $\mathbf{b} - \mathbf{p}$ is orthogonal to range(U), in the sense that

$$U^T(\mathbf{b} - \mathbf{p}) = U^T(\mathbf{b} - UU^T\mathbf{b}) = U^T\mathbf{b} - U^T\mathbf{b} = \mathbf{0} \; .$$

Theorem 2.1

If A is a real $m \times n$ matrix then there exist orthogonal matrices

$$\begin{aligned} U &= \left[\begin{array}{ccc} \mathbf{u}_1 & \cdots & \mathbf{u}_m \end{array} \right] \in \mathcal{R}^{m \times m} \\ V &= \left[\begin{array}{ccc} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{array} \right] \in \mathcal{R}^{n \times n} \end{aligned}$$

such that

$$U^T A V = \Sigma = \mathrm{diag}(\sigma_1, \ldots, \sigma_p) \in \mathcal{R}^{m \times n}$$

where $p = \min(m, n)$ and $\sigma_1 \geq \ldots \geq \sigma_p \geq 0$. Equivalently,

$$A = U\Sigma V^T \; .$$

Proof. Let $\mathbf{x}$ and $\mathbf{y}$ be unit vectors in $\mathbf{R}^n$ and $\mathbf{R}^m$, respectively, and consider the bilinear form

$$z = \mathbf{y}^T A\mathbf{x} \; .$$

The set

$$\mathcal{S} \; = \; \{\mathbf{x}, \mathbf{y} \mid \mathbf{x} \in \mathbf{R}^n, \; \mathbf{y} \in \mathbf{R}^m, \; \|\mathbf{x}\| = \|\mathbf{y}\| = 1\}$$

is compact, so that the scalar function $z(\mathbf{x}, \mathbf{y})$ must achieve a maximum value on $\mathcal{S}$, possibly at more than one point [5]. Let $\mathbf{u}_1$, $\mathbf{v}_1$ be two unit vectors in $\mathbf{R}^m$ and $\mathbf{R}^n$ respectively where this maximum is achieved, and let σ_1 be the corresponding value of z:

$$\max_{\|\mathbf{x}\|=\|\mathbf{y}\|=1} \mathbf{y}^T A\mathbf{x} = \mathbf{u}_1^T A\mathbf{v}_1 = \sigma_1 \ .$$

It is easy to see that $\mathbf{u}_1$ is parallel to the vector $A\mathbf{v}_1$. If this were not the case, their inner product $\mathbf{u}_1^T A\mathbf{v}_1$ could be increased by rotating $\mathbf{u}_1$ towards the direction of $A\mathbf{v}_1$, thereby contradicting the fact that $\mathbf{u}_1^T A\mathbf{v}_1$ is a maximum. Similarly, by noticing that

$$\mathbf{u}_1^T A\mathbf{v}_1 = \mathbf{v}_1^T A^T \mathbf{u}_1$$

and repeating the argument above, we see that $\mathbf{v}_1$ is parallel to $A^T\mathbf{u}_1$.

The vectors $\mathbf{u}_1$ and $\mathbf{v}_1$ can be extended into orthonormal bases for $\mathbf{R}^m$ and $\mathbf{R}^n$, respectively. Collect these orthonormal basis vectors into orthogonal matrices U_1 and V_1. Then

$$U_1^T A V_1 = S_1 = \begin{bmatrix} \sigma_1 & \mathbf{0}^T \\ \mathbf{0} & A_1 \end{bmatrix} \ .$$

In fact, the first column of AV_1 is $A\mathbf{v}_1 = \sigma_1\mathbf{u}_1$, so the first entry of $U_1^T AV_1$ is $\mathbf{u}_1^T\sigma_1\mathbf{u}_1 = \sigma_1$, and its other entries are $\mathbf{u}_j^T A\mathbf{v}_1 = 0$ because $A\mathbf{v}_1$ is parallel to $\mathbf{u}_1$ and therefore orthogonal, by construction, to $\mathbf{u}_2, \ldots, \mathbf{u}_m$. A similar argument shows that the entries after the first in the first row of S_1 are zero: the row vector $\mathbf{u}_1^T A$ is parallel to $\mathbf{v}_1^T$, and therefore orthogonal to $\mathbf{v}_2, \ldots, \mathbf{v}_n$, so that $\mathbf{u}_1^T A\mathbf{v}_2 = \ldots = \mathbf{u}_1^T A\mathbf{v}_n = 0$.

The matrix A_1 has one fewer row and column than A. We can repeat the same construction on A_1 and write

$$U_2^T A_1 V_2 = S_2 = \begin{bmatrix} \sigma_2 & \mathbf{0}^T \\ \mathbf{0} & A_2 \end{bmatrix}$$

so that

$$\begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U_2^T \end{bmatrix} U_1^T A V_1 \begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & V_2 \end{bmatrix} = \begin{bmatrix} \sigma_1 & 0 & \mathbf{0}^T \\ 0 & \sigma_2 & \mathbf{0}^T \\ \mathbf{0} & \mathbf{0} & A_2 \end{bmatrix} \ .$$

This procedure can be repeated until A_k vanishes (zero rows or zero columns) to obtain

$$U^T A V = \Sigma$$

where U^T and V are orthogonal matrices obtained by multiplying together all the orthogonal matrices used in the procedure, and

$$\Sigma = \mathrm{diag}(\sigma_1, \ldots, \sigma_p) \ .$$

Since matrices U and V are orthogonal, we can premultiply the matrix product in the theorem by U and postmultiply it by V^T to obtain

$$A = U\Sigma V^T \ ,$$

[5] Actually, at least at two points: if $\mathbf{u}_1^T A\mathbf{v}_1$ is a maximum, so is $(-\mathbf{u}_1)^T A(-\mathbf{v}_1)$.

which is the desired result.

It only remains to show that the elements on the diagonal of Σ are nonnegative and arranged in nonincreasing order. To see that $\sigma_1 \geq \ldots \geq \sigma_p$ (where $p = \min(m, n)$), we can observe that the successive maximization problems that yield $\sigma_1, \ldots, \sigma_p$ are performed on a sequence of sets each of which contains the next. To show this, we just need to show that $\sigma_2 \leq \sigma_1$, and induction will do the rest. We have

$$\begin{aligned}
\sigma_2 &= \max_{\|\hat{\mathbf{x}}\|=\|\hat{\mathbf{y}}\|=1} \hat{\mathbf{y}}^T A_1 \hat{\mathbf{x}} = \max_{\|\hat{\mathbf{x}}\|=\|\hat{\mathbf{y}}\|=1} \begin{bmatrix} 0 & \hat{\mathbf{y}} \end{bmatrix}^T S_1 \begin{bmatrix} 0 \\ \hat{\mathbf{x}} \end{bmatrix} \\
&= \max_{\|\hat{\mathbf{x}}\|=\|\hat{\mathbf{y}}\|=1} \begin{bmatrix} 0 & \hat{\mathbf{y}} \end{bmatrix}^T U_1^T A V_1 \begin{bmatrix} 0 \\ \hat{\mathbf{x}} \end{bmatrix} = \max_{\substack{\|\mathbf{x}\| = \|\mathbf{y}\| = 1 \\ \mathbf{x}^T \mathbf{v}_1 = \mathbf{y}^T \mathbf{u}_1 = 0}} \mathbf{y}^T A \mathbf{x} \leq \sigma_1 \ .
\end{aligned}$$

To explain the last equality above, consider the vectors

$$\mathbf{x} = V_1 \begin{bmatrix} 0 \\ \hat{\mathbf{x}} \end{bmatrix} \quad \text{and} \quad \mathbf{y} = U_1 \begin{bmatrix} 0 \\ \hat{\mathbf{y}} \end{bmatrix} \ .$$

The vector $\mathbf{x}$ is equal to the unit vector $[0\ \hat{\mathbf{x}}]^T$ transformed by the orthogonal matrix V_1, and is therefore itself a unit vector. In addition, it is a linear combination of $\mathbf{v}_2, \ldots, \mathbf{v}_n$, and is therefore orthogonal to $\mathbf{v}_1$. A similar argument shows that $\mathbf{y}$ is a unit vector orthogonal to $\mathbf{u}_1$. Because $\mathbf{x}$ and $\mathbf{y}$ thus defined belong to subsets (actually sub-spheres) of the unit spheres in $\mathbf{R}^n$ and $\mathbf{R}^m$, we conclude that $\sigma_2 \leq \sigma_1$.

The σ_i are nonnegative because all these maximizations are performed on unit hyper-spheres. The σ_is are maxima of the function $z(\mathbf{x}, \mathbf{y})$ which always assumes both positive and negative values on any hyper-sphere: If $z(\mathbf{x}, \mathbf{y})$ is negative, then $z(-\mathbf{x}, \mathbf{y})$ is positive, and if $\mathbf{x}$ is on a hyper-sphere, so is $-\mathbf{x}$.

Theorem 3.1

The minimum-norm least-squares solution to a linear system $A\mathbf{x} = \mathbf{b}$, that is, the shortest vector $\mathbf{x}$ that achieves the

$$\min_{\mathbf{x}} \|A\mathbf{x} - \mathbf{b}\| \ ,$$

is unique, and is given by

$$\hat{\mathbf{x}} = V \Sigma^\dagger U^T \mathbf{b} \tag{11}$$

where $A = U \Sigma V^T$ is the SVD of the rank-r matrix A and

$$\Sigma^\dagger = \begin{bmatrix}
1/\sigma_1 & & & & & 0 & \cdots & 0 \\
& \ddots & & & & & & \\
& & 1/\sigma_r & & & \vdots & & \vdots \\
& & & 0 & & & & \\
& & & & \ddots & & & \\
& & & & & 0 & \cdots & 0
\end{bmatrix} \ .$$

Proof. The minimum-norm least-squares solution to

$$A\mathbf{x} = \mathbf{b}$$

is the shortest vector $\mathbf{x}$ that minimizes

$$\|A\mathbf{x} - \mathbf{b}\|$$

that is,

$$\|U\Sigma V^T\mathbf{x} - \mathbf{b}\| \ .$$

This can be written as

$$\|U(\Sigma V^T\mathbf{x} - U^T\mathbf{b})\| \tag{12}$$

because U is an orthogonal matrix, $UU^T = I$. But orthogonal matrices do not change the norm of vectors they are applied to, so that the last expression above equals

$$\|\Sigma V^T\mathbf{x} - U^T\mathbf{b}\|$$

or, with $\mathbf{y} = V^T\mathbf{x}$ and $\mathbf{c} = U^T\mathbf{b}$,

$$\|\Sigma\mathbf{y} - \mathbf{c}\| \ .$$

In order to find the solution to this minimization problem, let us spell out the last expression. We want to minimize the norm of the following vector:

$$\begin{bmatrix} \sigma_1 & 0 & & \cdots & & 0 \\ 0 & \ddots & & \cdots & & 0 \\ & & \sigma_r & & & \\ \vdots & & & 0 & & \vdots \\ & & & & \ddots & \\ 0 & & & & & 0 \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_r \\ y_{r+1} \\ \vdots \\ y_n \end{bmatrix} - \begin{bmatrix} c_1 \\ \vdots \\ c_r \\ c_{r+1} \\ \vdots \\ c_m \end{bmatrix} \ .$$

The last $m - r$ differences are of the form

$$\mathbf{0} - \begin{bmatrix} c_{r+1} \\ \vdots \\ c_m \end{bmatrix}$$

and do not depend on the unknown $\mathbf{y}$. In other words, there is nothing we can do about those differences: if some or all the c_i for $i = r+1, \ldots, m$ are nonzero, we will not be able to zero these differences, and each of them contributes a *residual* $|c_i|$ to the solution. Each of the first r differences, on the other hand, can be zeroed exactly by letting $y_i = c_i/\sigma_i$ for the i-th difference. In addition, in these first r differences, the last $n - r$ components of $\mathbf{y}$ are multiplied by zeros, so they have no effect on the solution. Thus, there is freedom in their choice. Since we look for the minimum-norm solution, that is, for the shortest vector $\mathbf{x}$, we also want the shortest $\mathbf{y}$, because $\mathbf{x}$ and $\mathbf{y}$ are related by an orthogonal transformation. We therefore set $y_{r+1} = \ldots = y_n = 0$. In summary, the desired $\mathbf{y}$ has the following components:

$$\begin{aligned} y_i &= \frac{c_i}{\sigma_i} \quad \text{for } i = 1, \ldots, r \\ y_i &= 0 \quad \text{for } i = r+1, \ldots, n \ . \end{aligned}$$

When written as a function of the vector $\mathbf{c}$, this is

$$\mathbf{y} = \Sigma^+ \mathbf{c} \; .$$

Notice that there is no other choice for $\mathbf{y}$, which is therefore unique: minimum residual forces the choice of $y_1, \ldots, y_r$, and minimum-norm solution forces the other entries of $\mathbf{y}$. Thus, the minimum-norm, least-squares solution to the original system is the unique vector

$$\mathbf{x} = V\mathbf{y} = V\Sigma^+ \mathbf{c} = V\Sigma^+ U^T \mathbf{b}$$

as promised. The residual, that is, the norm of $\|A\mathbf{x} - \mathbf{b}\|$ when $\mathbf{x}$ is the solution vector, is the norm of $\Sigma\mathbf{y} - \mathbf{c}$, since this vector is related to $A\mathbf{x} - \mathbf{b}$ by an orthogonal transformation (see equation (12)). In conclusion, the square of the residual is

$$\|A\mathbf{x} - \mathbf{b}\|^2 = \|\Sigma\mathbf{y} - \mathbf{c}\|^2 = \sum_{i=r+1}^{m} c_i^2 = \sum_{i=r+1}^{m} (\mathbf{u}_i^T \mathbf{b})^2$$

which is the projection of the right-hand side vector $\mathbf{b}$ onto the left null space of A.

Theorem 4.1

Let

$$A = U\Sigma V^T$$

be the singular value decomposition of the $m \times n$ matrix A, and let $r = \text{rank}(A)$. Furthermore, define

$$i = \begin{cases} r+1 & \text{if } r < n \\ \min \{ j \,|\, 1 \le j \le n \text{ and } \sigma_j = \sigma_n \} & \text{otherwise.} \end{cases}$$

In words, if A has a nontrivial null space, then i indexes the first column of V in the orthogonal basis of the null space of A. Otherwise, i indexes the first column of V whose corresponding singular value σ_i is equal to the smallest (and last) singular value σ_n.

Then, all vectors of the form

$$\mathbf{x} = \alpha_1 \mathbf{v}_i + \ldots + \alpha_k \mathbf{v}_n$$

with

$$k = n - i + 1 \quad \text{and} \quad \alpha_1^2 + \ldots + \alpha_k^2 = 1$$

are unit-norm least-squares solutions to the homogeneous linear system

$$A\mathbf{x} = \mathbf{0},$$

that is, they achieve the

$$\min_{\|\mathbf{x}\|=1} \|A\mathbf{x}\| \; .$$

Proof. The reasoning is similar to that for the previous theorem. The unit-norm least-squares solution to

$$A\mathbf{x} = \mathbf{0}$$

is the vector $\mathbf{x}$ with $\|\mathbf{x}\| = 1$ that minimizes

$$\|A\mathbf{x}\|$$

that is,

$$\|U\Sigma V^T\mathbf{x}\| \ .$$

Since orthogonal matrices do not change the norm of vectors they are applied to, this norm is the same as

$$\|\Sigma V^T\mathbf{x}\|$$

or, with $\mathbf{y} = V^T\mathbf{x}$,

$$\|\Sigma\mathbf{y}\| \ .$$

Since V is orthogonal, $\|\mathbf{x}\| = 1$ translates to $\|\mathbf{y}\| = 1$. We thus look for the unit-norm vector $\mathbf{y}$ that minimizes the norm (squared) of $\Sigma\mathbf{y}$, that is,

$$\sigma_1^2 y_1^2 + \ldots + \sigma_n^2 y_n^2 \ .$$

This is obviously achieved by concentrating all the (unit) mass of $\mathbf{y}$ where the σs are smallest, that is by letting

$$y_1 = \ldots = y_{i-1} = 0. \tag{13}$$

From $\mathbf{y} = V^T\mathbf{x}$ we obtain $\mathbf{x} = V\mathbf{y} = y_1\mathbf{v}_1 + \ldots + y_n\mathbf{v}_n$, so that equation (13) is equivalent to

$$\mathbf{x} = \alpha_1\mathbf{v}_i + \ldots + \alpha_k\mathbf{v}_n$$

with $\alpha_1 = y_i, \ldots, \alpha_k = y_n$, and the unit-norm constraint on $\mathbf{y}$ yields

$$\alpha_1^2 + \ldots + \alpha_k^2 = 1 \ .$$