

CS168: The Modern Algorithmic Toolbox

Lecture #7: Understanding and Using Principal Component Analysis (PCA)

Tim Roughgarden & Gregory Valiant*

May 6, 2020

1 A Toy Example

The following toy example gives a sense of the problem solved by principal component analysis (PCA) and many of the reasons why you might want to apply it to a data set — to visualize the data in a lower-dimensional space, to understand the sources of variability in the data, and to understand correlations between different coordinates of the data points.

Suppose you ask some friends to rate, on a scale of 1 to 10, four different foods: kale salad, Taco Bell, sashimi, and pop tarts, with the results shown in Table 1. So in our usual

	kale	taco bell	sashimi	pop tarts
Alice	10	1	2	7
Bob	7	2	1	10
Carolyn	2	9	7	3
Dave	3	6	10	2

Table 1: Your friends' ratings of four different foods.

notation, m (the number of data points) is 4, and n (the number of dimensions) is also 4. Note that, in contrast to the linear regression setting, the data points do not have “labels” of any sort (beyond the names of the people). Can we usefully visualize this data set in fewer than 4 dimensions? Can we understand the forces at work behind the differences in opinion of the various foods?

*©2015–2020, Tim Roughgarden and Gregory Valiant. Not to be sold, published, or distributed without the authors' consent.

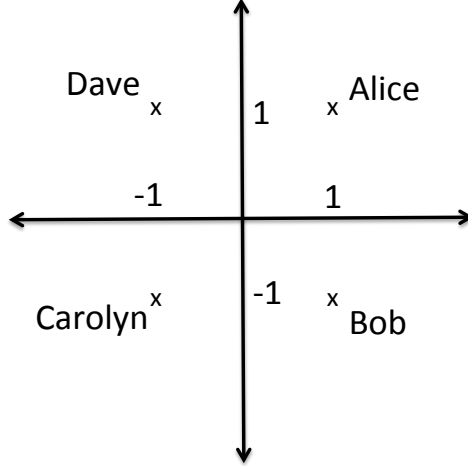


Figure 1: Visualizing 4-dimensional data in the plane.

The key observation is that each row (data point) can be approximately expressed as

$$\bar{\mathbf{x}} + a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2, \quad (1)$$

where

$$\bar{\mathbf{x}} = (5.5, 4.5, 5, 5.5)$$

is the average of the data points,

$$\mathbf{v}_1 = (3, -3, -3, 3),$$

$$\mathbf{v}_2 = (1, -1, 1, -1),$$

and (a_1, a_2) is $(1,1)$ for Alice, $(1,-1)$ for Bob, $(-1,-1)$ for Carolyn, and $(-1,1)$ for Dave (Figure 1). For example, $\mathbf{x} + \mathbf{v}_1 + \mathbf{v}_2 = (9.5, 0.5, 3, 7.5)$, which is approximately equal to Alice’s scores. Similarly, $\mathbf{x} - \mathbf{v}_1 - \mathbf{v}_2 = (1.5, 8.5, 7, 3.5)$, which is approximately equal to Carolyn’s scores.

What use is such an approximation? One answer is that it provides a way to visualize the data points, as in Figure 1. With more data points, we can imagine inspecting the resulting figure for clusters of similar data points.

A second answer is that it helps interpret the data. We think of each data point as having a “ v_1 -coordinate” (i.e., a_1) and a “ v_2 -coordinate” (a_2). What does the vector v_1 “mean?” The first and fourth coordinates both have a large positive value (and so are positively correlated) while the second and third coordinates have a large negative value (and so are positively correlated with each other and negatively correlated with the first and fourth coordinates). Noting that kale salad and pop tarts are vegetarian¹ while Taco Bell and sashimi are not, we can interpret the v_1 coordinate as indicating the extent to which someone has vegetarian preferences.² By similar reasoning, we can interpret the second vector v_2 as indicating the

¹Little-known fact: pop tarts — the unfrosted kinds, at least — are inadvertently vegan.

²Conversely, if we knew which friends were vegetarian and which were not, we could deduce which foods are most likely to be vegetarian.

extent to which someone is health-conscious. The fact that v_1 has larger coordinates than v_2 indicates that it is the stronger of the two effects.

We'll see that the vectors v_1 and v_2 , once normalized, correspond to the “top two principal components” of the data. The point of PCA is to compute approximations of the type (1) automatically, including for large data sets.

1.1 Goal of PCA

The goal of PCA is to approximately express each of m n -dimensional vectors³ $\mathbf{x}_1, \dots, \mathbf{x}_m \in \mathbb{R}^n$ as linear combinations of k n -dimensional vectors $\mathbf{v}_1, \dots, \mathbf{v}_k \in \mathbb{R}^n$, so that

$$\mathbf{x}_i \approx \sum_{j=1}^k a_{ij} \mathbf{v}_j$$

for each $i = 1, 2, \dots, m$. (In the toy example, $m = n = 4$ and $k = 2$.) PCA offers a formal definition of which k vectors are the “best” ones for this purpose. Next lecture, we'll see that there are also good algorithms for computing these vectors.

1.2 Relation to Dimensionality Reduction

The high-level goal of PCA should remind you of a couple of topics studied in previous lectures. First, recall Johnson-Lindenstrauss (JL) dimensionality reduction (Lecture #4), where the goal is also to re-express a bunch of high-dimensional points as low-dimensional points. Recall that this method maps a point \mathbf{x} to a point $(\langle \mathbf{x}, \mathbf{r}_1 \rangle, \dots, \langle \mathbf{x}, \mathbf{r}_k \rangle)$, where each \mathbf{r}_j is a random unit vector (independent standard Gaussians in each coordinate, then normalized).⁴ The same \mathbf{r}_j 's are used for all data points. PCA and JL dimensionality reduction are different in the following respects.

1. JL dimensionality reduction assumes that you care about the Euclidean distance between each pair of points — it is designed to approximately preserve these distances. PCA offers no guarantees about preserving pairwise distances.
2. JL dimensionality reduction is data-oblivious, in the sense that the random vectors $\mathbf{r}_1, \dots, \mathbf{r}_k$ are chosen without looking at the data points. PCA, by contrast, is deterministic, and the whole point is to compute vectors $\mathbf{v}_1, \dots, \mathbf{v}_k$ that “explain the data.”
3. For the above reason, the k coordinates used in JL dimensionality reduction have no intrinsic meaning, while those used in PCA are often meaningful (recall the toy example).

³Representing, for example: images (dimensions = pixels); measurements (dimensions = sensors); documents (dimensions = words); and so on.

⁴The notation $\langle \mathbf{x}, \mathbf{y} \rangle$ indicates the inner (or dot) product $\sum_{i=1}^n x_i y_i$ of the two vectors.

4. JL dimensionality reduction generally only gives good results when k is at least in the low hundreds. On the other hand, this value of k works for every data set of a given size. PCA can give meaningful results even when k is 1 or 2, but there are also data sets where it provides little interesting information (for any k).

1.3 Relation to Linear Regression

Both PCA and linear regression concern fitting the “best” k -dimensional subspace to a point set. One difference between the two methods is in the interpretation of the input data. With linear regression, each data point has a real-valued label, which can be interpreted as a special “label coordinate.” The goal of linear regression is to learn the relationship between this special coordinate and the other coordinates. This makes sense when the “label” is a dependent variable that is approximately a linear combination of all of the other coordinates (the independent variables). In PCA, by contrast, all coordinates are treated equally, and they are not assumed to be independent from one another. This makes sense when there is a set of latent (i.e., hidden/underlying) variables, and all of the coordinates of your data are (approximately) linear combinations of those variables.

Second, PCA and linear regression use different definitions of “best fit.” Recall that in linear regression the goal is to minimize the total squared error, where the error on a data point is the difference between the linear function’s prediction and the actual label of the data point. With one-dimensional data (together with labels), this corresponds to computing the line that minimizes the sum of the squared vertical distances between the line and the data points (Figure 2(a)). This reflects the assumption that the coordinate corresponding to labels is the important one. We define the PCA objective function formally below; for two-dimensional data, the goal is to compute the line that minimizes the sum of the squared *perpendicular* distances between the line and the data points (Figure 2(b)). This reflects the assumption that all coordinates play a symmetric role and so the usual Euclidean distance is most appropriate (e.g., rotating the point set just results in the “best-fit” line being rotated accordingly). On Mini-Project #4 you will learn more about which situations call for PCA and which call for linear regression.

2 Defining the Problem

2.1 Preprocessing

Before using PCA, it’s important to preprocess the data. First, the points $\mathbf{x}_1, \dots, \mathbf{x}_m$ should be centered around the origin, in the sense that $\sum_{i=1}^m \mathbf{x}_i$ is the all-zero vector. This is easy to enforce by subtracting (i.e., shifting) each point by the “sample mean” $\bar{\mathbf{x}} = \frac{1}{m} \sum_{i=1}^m \mathbf{x}_i$. (In the toy example, we had $\bar{\mathbf{x}} = (5.5, 4.5, 5, 5.5)$.) After finding the best-fit line for the shifted point set, one simply shifts the line back by the original sample mean to get the best-fit line for the original uncentered data set. This shifting trick makes the necessary linear algebra simpler and clearer.

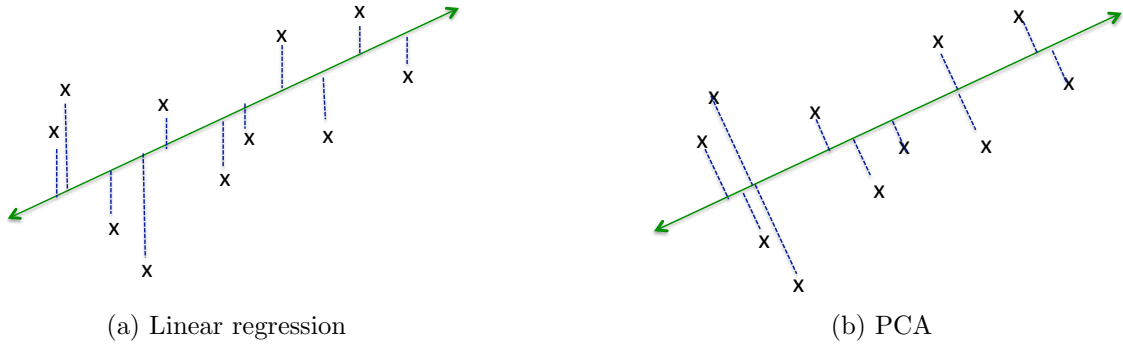


Figure 2: Linear regression minimizes the sum of squared vertical distances, while PCA minimizes the sum of squared perpendicular distances.

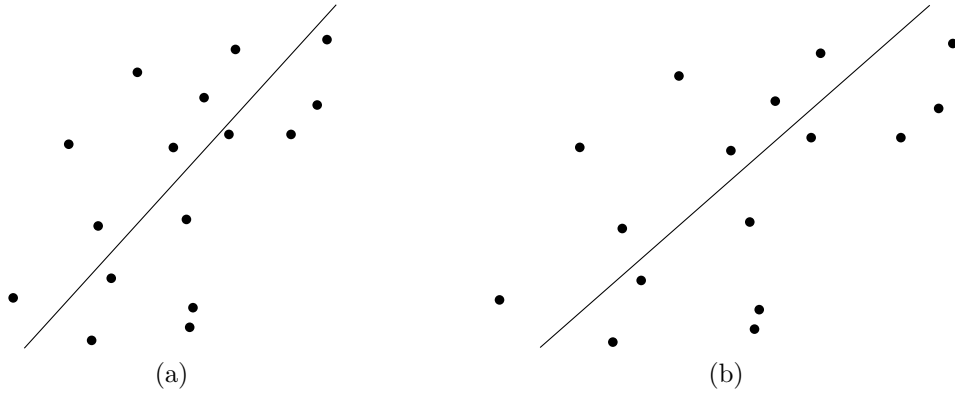


Figure 3: Scaling the x -axis yields a different best-fit line.

Second, in many applications it is important to scale each coordinate appropriately. The most common approach to this is: if $\mathbf{x}_1, \dots, \mathbf{x}_m$ is a point set centered at the origin, then for each coordinate $j = 1, 2, \dots, n$, divide the j th coordinate of every point by the “sample deviation” in that coordinate, $\sqrt{\sum_{i=1}^m x_{ij}^2}$. The motivation for this coordinate scaling is the fact that, without it, the result of PCA would be highly sensitive to the units in which each coordinate is measured. For example, changing units from miles to kilometers in some coordinate yields the “same” data set in some sense, and yet this change would scale up all values in this coordinate, which in turn would cause a different “best-fit” line to be computed.⁵ In some applications, like with images — where all coordinates are in the same units, namely pixel intensities — there is no need to do such coordinate scaling. (The same goes for the toy example in Section 1.)

⁵It should be geometrically clear, already in two dimensions, that stretching out one coordinate affects the best line through the points. See also Figure 3.

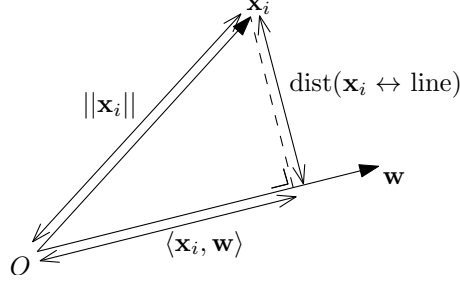


Figure 4: The geometry of the inner product.

2.2 The Objective Function

For clarity, we first discuss the special case of $k = 1$, where the goal is to fit the “best” line to a data set. Everything in this section generalizes easily to the case of general k (Section 2.3).

As foreshadowed above, PCA defines the “best-fit line” as the one that minimizes the average squared Euclidean distance between the line and the data points:

$$\operatorname{argmin}_{\mathbf{v}: \|\mathbf{v}\|=1} \frac{1}{m} \sum_{i=1}^m ((\text{distance between } \mathbf{x}_i \text{ and line spanned by } \mathbf{v})^2). \quad (2)$$

Note that we’re identifying a line (through the origin) with a unit vector \mathbf{v} in the same direction. Minimizing the Euclidean distances between the points and the chosen line should seem natural enough; the one thing you might be wondering about is why we square these distances before adding them up. One reason is that it ensures that the best-fit line passes through the origin. Another is a tight connection to variance maximization, discussed next.

Recall the geometry of projections and the inner product (Figure 4). In particular, $\langle \mathbf{x}_i, \mathbf{v} \rangle$ is the (signed) length of the projection of \mathbf{x}_i onto the line spanned by \mathbf{v} . Recall the Pythagorean Theorem: for a right triangle with sides a and b and hypotenuse c , $a^2 + b^2 = c^2$. Instantiating this for the right triangle shown in Figure 4, we have

$$(\text{dist}(\mathbf{x}_i \leftrightarrow \text{line}))^2 + \langle \mathbf{x}_i, \mathbf{v} \rangle^2 = \|\mathbf{x}_i\|^2. \quad (3)$$

The right-hand side of (3) is a constant, independent of the choice of line \mathbf{v} . Thus, there is a zero-sum game between the squared distance between a point \mathbf{x}_i and the line spanned by \mathbf{v} and the squared length of the projection of \mathbf{x}_i on this line — making one of these quantities bigger makes the other one smaller. This implies that the objective function of maximizing the squared projections — the *variance* of the projection of the point set — is equivalent to the original objective in (2):

$$\operatorname{argmax}_{\mathbf{v}: \|\mathbf{v}\|=1} \frac{1}{m} \sum_{i=1}^m \langle \mathbf{x}_i, \mathbf{v} \rangle^2. \quad (4)$$

The objective function of maximizing variance is natural in its own right, and the fact that PCA’s objective function admits multiple interpretations builds confidence that it’s performing a fundamental operation on the data. For example, imagine the data points

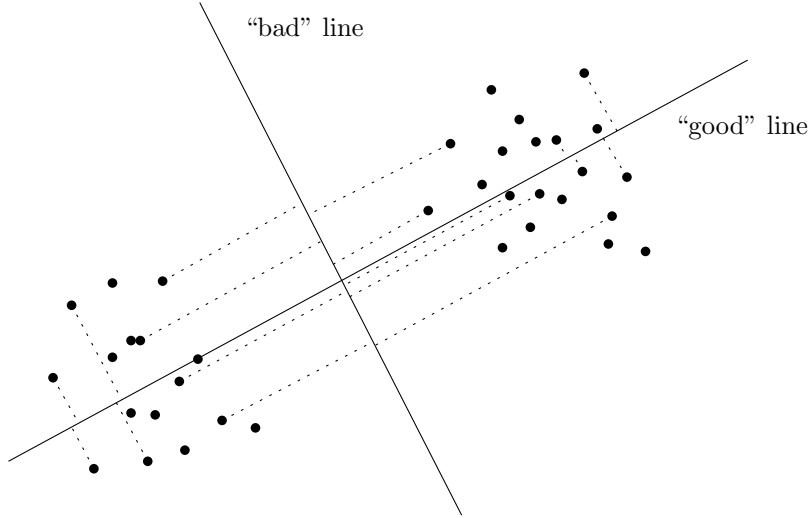


Figure 5: For the good line, the projection of the points onto the line keeps the two clusters separated, while the projection onto the bad line merges the two clusters.

fall into two well-separated clusters; see Figure 5 for an illustration but imagine a high-dimensional version that can't be so easily eyeballed. In this case, maximizing variance corresponds to preserving the separation between the two clusters post-projection. (With a poorly chosen line, the two clusters would project on top of one another, obscuring the structure in the data.)

PCA effectively assumes that variance in the data corresponds to interesting information. One can imagine scenarios where such variance corresponds to noise rather than signal, in which case PCA may not produce illuminating results. (See Section 4 for more on PCA failure cases.)

2.3 Larger Values of k

The discussion so far focused on the $k = 1$ case (fitting a line to the data), but the case of larger k is almost the same. For general k , the objective functions of minimizing the squares of distances to a k -dimensional subspace and of maximizing the variance of the projections onto a k -dimensional subspace are again equivalent. So the PCA objective is now

$$\operatorname{argmax}_{k\text{-dimensional subspaces } S} \frac{1}{m} \sum_{i=1}^m (\text{length of } \mathbf{x}_i \text{'s projection on } S)^2. \quad (5)$$

To rephrase this objective in a more convenient form, recall the following basic linear algebra. First, vectors $\mathbf{v}_1, \dots, \mathbf{v}_k$ are *orthonormal* if they all have unit length ($\|\mathbf{v}_i\|_2 = 1$ for all i) and are orthogonal ($\langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0$ for all $i \neq j$). For example, the standard basis vectors (of the form $(0, 0, \dots, 0, 1, 0, \dots, 0)$) are orthonormal. Rotating these vectors gives more sets of orthonormal vectors.

The *span* of a collection $\mathbf{v}_1, \dots, \mathbf{v}_k \in \mathbb{R}^n$ of vectors is all of their linear combinations: $\{\sum_{j=1}^k \lambda_j \mathbf{v}_j : \lambda_1, \dots, \lambda_k \in \mathbb{R}\}$. If $k = 1$, then this span is a line through the origin; if $k = 2$ and $\mathbf{v}_1, \mathbf{v}_2$ are linearly independent (i.e., not multiples of each other) then the span is a plane (through the origin); and so on.

One nice fact about orthonormal vectors $\mathbf{v}_1, \dots, \mathbf{v}_k$ is that the squared projection length of a point onto the subspace spanned by the vectors is just the sum of the squares of its projections onto each of the vectors:

$$(\text{length of } \mathbf{x}_i \text{'s projection on span}(\mathbf{v}_1, \dots, \mathbf{v}_k))^2 = \sum_{j=1}^k \langle \mathbf{x}_i, \mathbf{v}_j \rangle^2. \quad (6)$$

(For intuition, consider first the case where $\mathbf{v}_1, \dots, \mathbf{v}_k$ are all standard basis vectors, so $\langle \mathbf{x}_i, \mathbf{v}_j \rangle$ just picks out one coordinate of \mathbf{x}_i). This identity is *not* true if the \mathbf{v}_j 's are not orthonormal (e.g., imagine if $k = 2$ and $\mathbf{v}_1, \mathbf{v}_2$ are linearly independent but nearly the same vector).

Combining (5) and (6), we can state the objective of PCA for general k in its standard form: compute orthonormal vectors $\mathbf{v}_1, \dots, \mathbf{v}_k$ to maximize

$$\frac{1}{m} \sum_{i=1}^m \underbrace{\sum_{j=1}^k \langle \mathbf{x}_i, \mathbf{v}_j \rangle^2}_{\text{squared projection length}}. \quad (7)$$

The resulting k orthonormal vectors are called the *top k principal components* of the data.⁶

To recap, the formal definition of the problem solved by PCA is:

Given $\mathbf{x}^1, \dots, \mathbf{x}^m \in \mathbb{R}^n$ and a parameter $k \geq 1$, compute orthonormal vectors $\mathbf{v}_1, \dots, \mathbf{v}_k \in \mathbb{R}^n$ to maximize (7).

Next lecture we discuss computational methods for finding the top k principal components. We conclude this lecture with use cases and “non-use cases” (i.e., failure modes) of PCA. Given a black-box that computes principal components, what would you do with it?

3 Use Cases

3.1 Data Visualization

3.1.1 A General Recipe

PCA is commonly used to visualize data. In this use case, one typically takes k to be 1, 2, or 3. Given data points $\mathbf{x}_1, \dots, \mathbf{x}_m \in \mathbb{R}^n$, here is the approach:

⁶In the toy example, the two vectors $(3, -3, -3, 3)$ and $(1, -1, 1, -1)$, once normalized to be unit vectors, are close to the top two principal components. The actual principal components have messier numbers so we don't report them here. Try computing them with one line of Matlab code!

1. Perform PCA to get the top k principal components $\mathbf{v}_1, \dots, \mathbf{v}_k \in \mathbb{R}^n$.
2. For each data point \mathbf{x}_i , define its “ \mathbf{v}_1 -coordinate” as $\langle \mathbf{x}_i, \mathbf{v}_1 \rangle$, its “ \mathbf{v}_2 -coordinate” as $\langle \mathbf{x}_i, \mathbf{v}_2 \rangle$, and so on. This associates k coordinates with each data point \mathbf{x}_i , according to the extent to which it points in the same direction as each of the top k principal components. (So a large positive coordinate means that \mathbf{x}_i is close to the same direction as \mathbf{v}_j , while a large negative coordinate means that \mathbf{x}_i points in the opposite direction.)
3. Plot the point \mathbf{x}_i in \mathbb{R}^k as the point $(\langle \mathbf{x}_i, \mathbf{v}_1 \rangle, \dots, \langle \mathbf{x}_i, \mathbf{v}_k \rangle)$.⁷

This is more or less what we did with our toy example in Figure 1, although the scaling was different because our vectors \mathbf{v}_1 and \mathbf{v}_2 were not unit vectors.

What is the “meaning” of the point $(\langle \mathbf{x}_i, \mathbf{v}_1 \rangle, \dots, \langle \mathbf{x}_i, \mathbf{v}_k \rangle)$? Recall that one way to think about PCA is as a method for approximating a bunch of data points as linear combinations of the same k vectors. PCA uses the vectors $\mathbf{v}_1, \dots, \mathbf{v}_k$ for this purpose, and the coordinates $(\langle \mathbf{x}_i, \mathbf{v}_1 \rangle, \dots, \langle \mathbf{x}_i, \mathbf{v}_k \rangle)$ specify the linear combination of these vectors that most closely approximate \mathbf{x}_i (with respect to Euclidean distance). That is, PCA approximates each \mathbf{x}_i as

$$\mathbf{x}_i \approx \sum_{j=1}^k \langle \mathbf{x}_i, \mathbf{v}_j \rangle \mathbf{v}_j.$$

3.1.2 Interpreting the Results

Both the \mathbf{v}_j ’s and the projections of the \mathbf{x}_i ’s onto them can be interesting. Here are some things to look at:

1. Look at the data points with the largest (most positive) and smallest (most negative) projections $\langle \mathbf{x}_i, \mathbf{v}_1 \rangle$ on the first principal component. Does this suggest a potential “meaning” for the component? Are there data points clustered together at either of the two ends, and if so, what do these have in common?
2. Plot all points according to their k coordinate values (i.e., projection lengths onto the top k principal components). Do any interesting clusters pop out (e.g., with $k = 2$, in any of the four corners)? For example, by looking at pairs that have similar second coordinates — both pairs with similar first coordinates, and pairs with very different first coordinates — it is often possible to obtain a rough interpretation of the second principal component.
3. Looking at the coordinates of a principal component — the linear combination of the original data point attributes that it uses — can also be helpful. (E.g., see the Eigenfaces application below.)

⁷Alternatively, it can sometimes be illuminating to plot points using a subset of the top k principal components — the first and third components, say.

[illegible]

3.1.3 Do Genomes Encode Geography?

Novembre et al. [1] considered a data set comprising 1387 Europeans (the rows). Each person’s genome was examined in the same 200,000 “SNPs” (the columns) — positions that tend to exhibit gene mutation.⁸ So in one of these positions, maybe 90% of all people have a “C,” while 10% have an “A.” In a nutshell, Novembre et al. [1] apply PCA to this data set (with $m \approx 1400$, $n \approx 200,000$, and $k = 2$) and plot the data according to the top two principal components \mathbf{v}_1 and \mathbf{v}_2 (using the exact same recipe as in Section 3.1.1, with the x - and y -axes corresponding to \mathbf{v}_1 and \mathbf{v}_2).⁹ See Figure 6).

⁸You'll work with a similar data set on Mini-Project #4.

10

longitude (rotated 16° counter-clockwise). That is, *their genome “knows” where they’re from!* This suggests that many Europeans have bred locally for long enough for geographic information to be reflected in their DNA.

Is this conclusion obvious in hindsight? Not really. For example, if you repeat the experiment using U.S. data, the top principal components correspond more to waves of immigration than to anything geographic. So in this case the top principal components reflect temporal rather than spatial effects.

There are competing mathematical models for genetic variation. Some of these involve spatial decay, while others are based on multiple discrete and well-differentiated groups. The study of Novembre et al. [1] suggests that the former models are much more appropriate for Europeans.

3.2 Data Compression

One famous “killer application” of PCA in computer science is the Eigenfaces project [2]. Here, the data points are a bunch of images of faces — all framed in the same way, under the same lighting conditions. Thus n is the number of pixels (around 65K) and each dimension encodes the intensity of one pixel. It turns out that using only the top 100–150 principal components is enough to represent almost all of the images with high accuracy — far less than the 65K needed for exactly representing all of the images.¹⁰ Each of these principal components can be viewed as an image and in many cases interpreted directly. (By contrast, in the previous example, we couldn’t interpret the top two principal components by inspection — we needed to plot the data points first.) For example, one principal component may indicate the presence or absence of glasses, another the presence or absence of a mustache, and so on. (See the figures in [2], available from the course Web site.) These techniques have been used in face recognition, which boils down to a nearest-neighbor-type computation in the low-dimensional space spanned by the top principal components. There have of course been lots of advances in face recognition since the 1991 publication of [2], but PCA remains a key building block in modern approaches to the problem.

4 Failure Cases

When and why does PCA fail?

1. You messed up the scaling/normalizing. PCA is sensitive to different scalings/normalizations of the coordinates. Much of the artistry of getting good results from PCA involves choosing an appropriate scaling for the different data coordinates, and perhaps additional preprocessing of the data (like outlier removal).
2. Non-linear structure. PCA is all about finding linear structure in your data. If your data has some low-dimensional, but non-linear structure, e.g., you have two data coor-

¹⁰We’ll see next lecture that principal components are in fact eigenvectors of a suitable matrix — hence the term “Eigenfaces.”

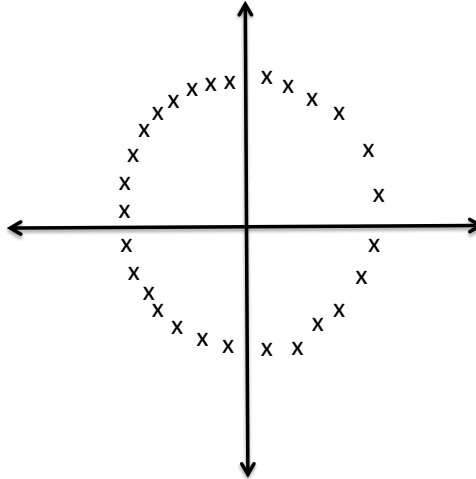


Figure 7: GPS data from a ferris wheel. PCA is not designed to discover nonlinear structure.

dinates, x, y , with $y \approx x^2$, then PCA will not find this.¹¹ Similarly for GPS data from someone on a ferris wheel (Figure 7) — the data is one dimensional (each point can be specified by an angle) but this dimension will not be identified by PCA.

3. Non-orthogonal structure. It is nice to have coordinates that are interpretable, like in our toy example (Section 1) and our Europe example (Section 3.1.3). Even if your data is essentially linear, the fact that the principal components are all orthogonal will often mean that after the top few components, it will be almost impossible to interpret the meanings of the components. In the Europe example, the third and later components are forced to be orthogonal to the latitude and longitude components. This is a rather artificial constraint to put on an interpretable feature.

References

- [1] John Novembre, Toby Johnson, Katarzyna Bryc, Zoltan Kutalik, Adam R. Boyko, Adam Auton, Amit Indap, Karen S. King, Sven Bergmann, Matthew R. Nelson, Matthew Stephens, and Carlos D. Bustamante. Genes mirror geography within Europe. *Nature*, 456:98–101, 2008.
- [2] M. Turk and A. Pentland. Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, 3(1):71–86, 1991.

¹¹As mentioned in the context of linear regression last lecture, you can always add extra non-linear dimensions to your data, like coordinates x^2, y^2, xy , etc., and then PCA this higher-dimensional data. This idea doesn't always work well with PCA, however.