12-Anomaly-Detection-SVD-III

October 20, 2016

1 Anomaly Detection (and SVD-III)

Today we'll discuss an important topic related to unsupervised learning: **anomaly detection.**

Anomalies are objects that are different from most other objects.

Anomalies are also called "outliers".

Furthermore, we usually expect that anomalies are different in a **qualitative** sense as well.

> An outlier is an observation that differs so much from other observations as to arouse suspicion that it was generated by a different mechanism
>
> – Douglas Hawkins

Why might we be interested in anomalies?

- **Fraud Detection** - stolen credit cards
- **Intrusion Detection** - attacks on computer systems
- **Public Health** - occurrence of disease in a particular area
- **Medicine** - a set of symptoms may indicate a disease

Anomaly detection presents a number of challenges.

It is an **unsupervised** method – so validation is hard * It is hard to know that your set of anomalies is correct * It is hard to know how many anomalies there are in the data

The main assumption made in anomaly detection:

There are many more "normal" observations than "abnormal" (anomalies) in the data.

Methodologically, anomaly detection proceeds as follows:

1. Build a profile of "normal" data objects
    - These can be patterns, summary statistics, or more complicated models
2. Use the "normal" profile to detect anomalies
    - These are observations whose characteristics differ significantly from the normal profile.

1.1 Approaches To Anomaly Detection

The idea that "normal behavior is what is most frequently observed" is the basis for most anomaly detection methods.

It suggests a number of approaches.

Model-Based Methods.

Here, we assume that a model for the data will describe most of the data. Data points that are not well described by the model are potentially anomalies.

1) Use the data to estimate the parameters of a probability distribution. For example, one might estimate a normal distribution from the data.

- Then an object that is very **unlikely** under the model may be an anomaly.

2) Model the data as a set of clusters (cluster the data).

- Then an object that does not strongly belong to any cluster may be an anomaly.

3) Model the data using a regression.

- Then an object that is far from its predicted value may be an anomaly.

Other Methods.

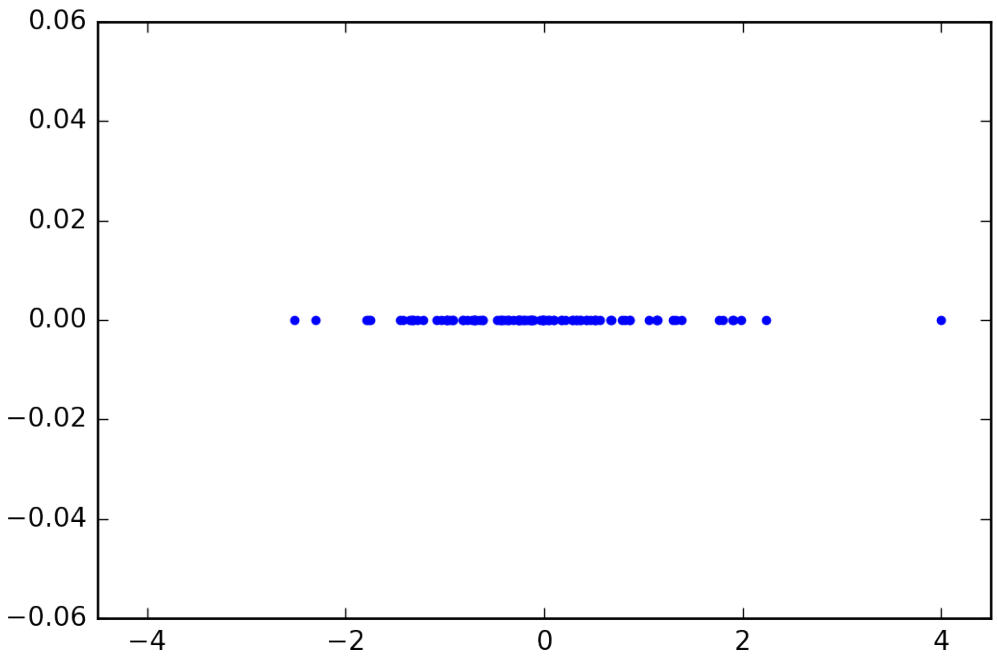
If you cannot build a model of the data, you can still:

1. Define an anomaly as one that is distant from all (or most) other objects.
2. Define an anomaly as one that is in an unusually-low-density region.

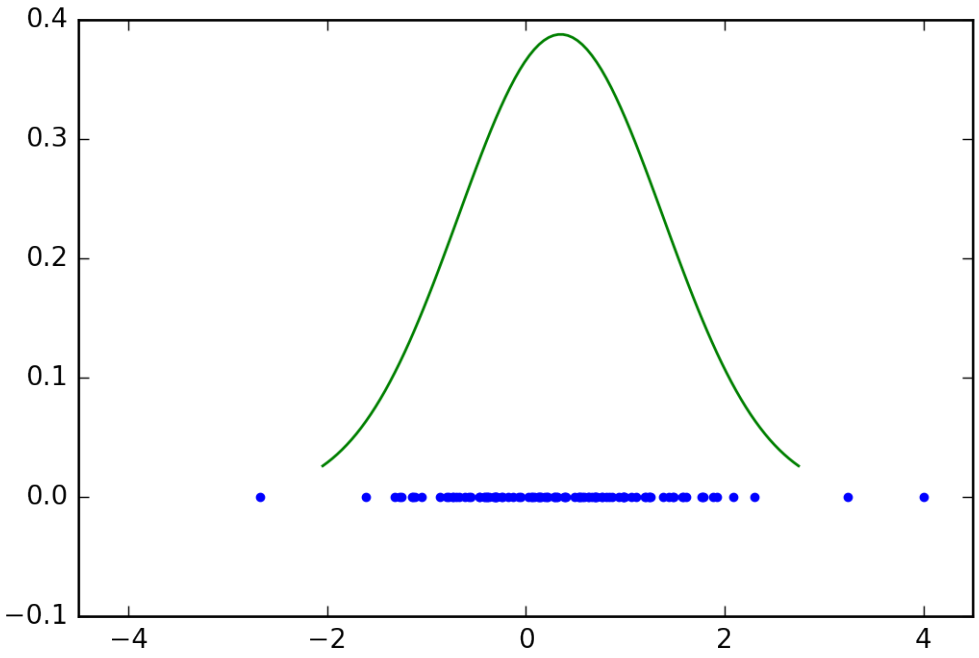
1.2 Model-Based Detection: 1-D Gaussian

To start, we will examine a very simple case: anomaly detection in 1-D.

```
In [359]: n_samples = 100
          data = np.random.randn(n_samples, 1)
          data = np.concatenate([data, np.array([[4]])])
          plt.plot(data, np.zeros(n_samples+1), '.')
          _ = plt.xlim([-4.5, 4.5])
```




```
In [333]: m_est = np.mean(data)
          std_est = np.std(data)

In [334]: import scipy.stats
          norm = scipy.stats.distributions.norm(m_est,std_est)

In [335]: plt.plot(data, np.zeros(n_samples+1), '.')
          plt.xlim([-4.5, 4.5])
          plt.ylim([-0.1,0.4])
          x = np.linspace(norm.ppf(0.01),
                          norm.ppf(0.99), 100)
          plt.plot(x, norm.pdf(x), '-')

Out[335]: [<matplotlib.lines.Line2D at 0x12781aac8>]
```



Let's calculate the probability of each data point under this model.

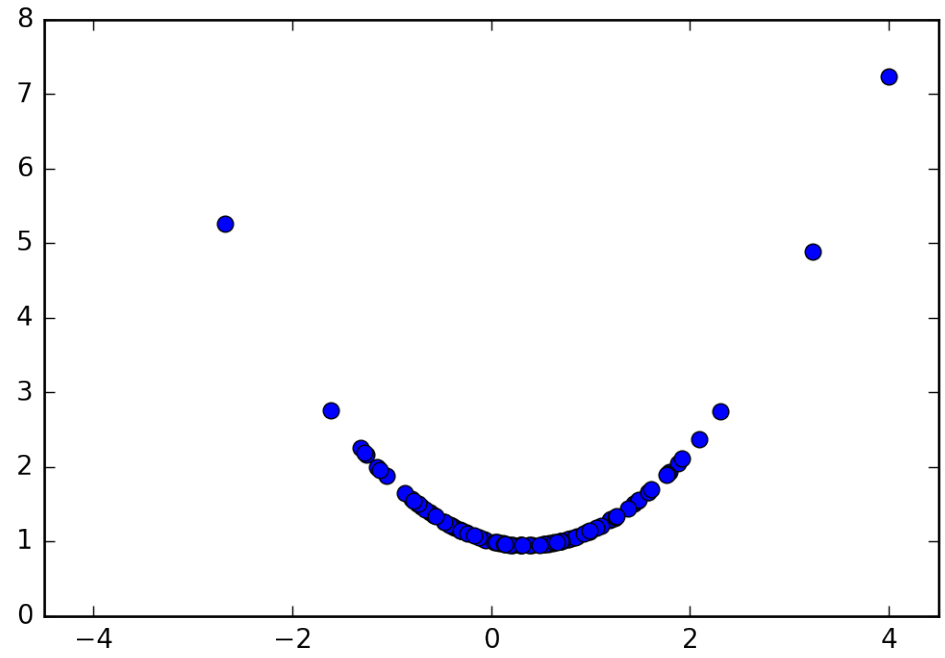
```
In [336]: prob_data = [norm.pdf(x) for x in data]
          prob_data

Out[336]: [array([ 0.35586371]),
           array([ 0.38405332]),
           array([ 0.31998378]),
           array([ 0.22258254]),
           array([ 0.38181181]),
           array([ 0.30423961]),
           array([ 0.36671907]),
           array([ 0.20829432]),
           array([ 0.38435306]),
           array([ 0.1453842]),
           array([ 0.21330611]),
           array([ 0.31735056]),
           array([ 0.32300979]),
           array([ 0.30005562]),
           array([ 0.25002792]),
           array([ 0.06343487]),
           array([ 0.38124]),
           array([ 0.38733416]),
           array([ 0.32031134]),
           array([ 0.35123213]),
           array([ 0.31790882]),
```

```
array([ 0.3421388]),
array([ 0.1279931]),
array([ 0.06407598]),
array([ 0.35615557]),
array([ 0.3870054]),
array([ 0.38737633]),
array([ 0.374997]),
array([ 0.25899721]),
array([ 0.19008675]),
array([ 0.35755962]),
array([ 0.38025708]),
array([ 0.21012747]),
array([ 0.34595562]),
array([ 0.11488642]),
array([ 0.26717281]),
array([ 0.29553423]),
array([ 0.10450771]),
array([ 0.3870355]),
array([ 0.31582103]),
array([ 0.22050806]),
array([ 0.18870867]),
array([ 0.37268154]),
array([ 0.3593369]),
array([ 0.3270606]),
array([ 0.29899668]),
array([ 0.38301593]),
array([ 0.31365956]),
array([ 0.00752139]),
array([ 0.15303872]),
array([ 0.37798633]),
array([ 0.2824442]),
array([ 0.23007124]),
array([ 0.23797648]),
array([ 0.36925539]),
array([ 0.33028357]),
array([ 0.27654793]),
array([ 0.36613085]),
array([ 0.29250655]),
array([ 0.12052511]),
array([ 0.14781635]),
array([ 0.15073728]),
array([ 0.28218642]),
array([ 0.37428972]),
array([ 0.36446507]),
array([ 0.37758731]),
array([ 0.37890561]),
array([ 0.38039248]),
array([ 0.31734158]),
```

```
 array([ 0.27371162]),
 array([ 0.23515813]),
 array([ 0.37282224]),
 array([ 0.37222839]),
 array([ 0.38707186]),
 array([ 0.26452091]),
 array([ 0.3483108]),
 array([ 0.36579354]),
 array([ 0.22260835]),
 array([ 0.38749815]),
 array([ 0.1117119]),
 array([ 0.1367452]),
 array([ 0.09285612]),
 array([ 0.37914097]),
 array([ 0.29619141]),
 array([ 0.00514608]),
 array([ 0.3295741]),
 array([ 0.3404523]),
 array([ 0.26290712]),
 array([ 0.37975232]),
 array([ 0.19308253]),
 array([ 0.26285536]),
 array([ 0.37044645]),
 array([ 0.1353215]),
 array([ 0.3843]),
 array([ 0.38745487]),
 array([ 0.18272435]),
 array([ 0.3061383]),
 array([ 0.14033611]),
 array([ 0.21308089]),
 array([ 0.31839047]),
 array([ 0.00071574])]
```

To make this easier to analyze, let's work with the (negative) log probability of the data:

```
In [337]: import math
          log_prob_data = [-math.log(x) for x in prob_data]
          plt.plot(data, log_prob_data, 'o')
          _ = plt.xlim([-4.5,4.5])
```



This plot makes clear that there is one point that is **very** unlikely under our model. We would be justified in identifying this as an anomaly.

In particular, the probability of the extreme point under this model is 0.00043222.

We would not expect to see a sample with this probability unless we sampled the distribution $1/0.0004322 = 2314$ times.

However we have only 101 data points.

An important point.

Notice that we estimated the mean and standard deviation of our model using **all** the data – including the point that we later decided was an anomaly.

Of course the correct parameter estimation should **not** have included the anomalous data point, if it truly "was generated by a different mechanism."

On one hand, our estimation approach gives us an approximation to the true distribution.

This approximation may be justified under the assumption that "most of the data points are not anomalies".

And since we don't know the anomalies in advance (of course) we cannot simply remove them before we estimate the parameters.

There are more sophisticated approaches to try to address this problem – we won't discuss them, but you should be aware that it is possible to do better than what we did here.

1.3 Extending to Multiple Dimensions

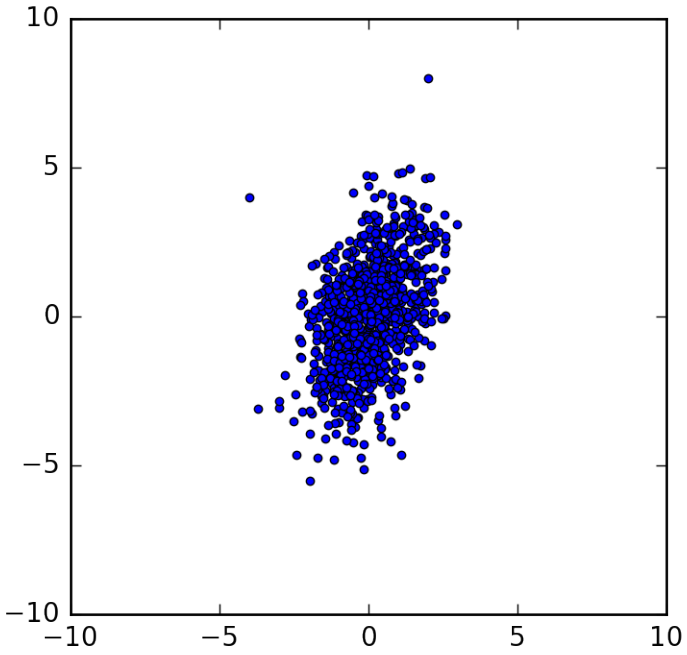
For data with multiple features we would like to take the same approach.

We would like to identify points as outliers if they have low probability under a **multivariate** Gaussian model.

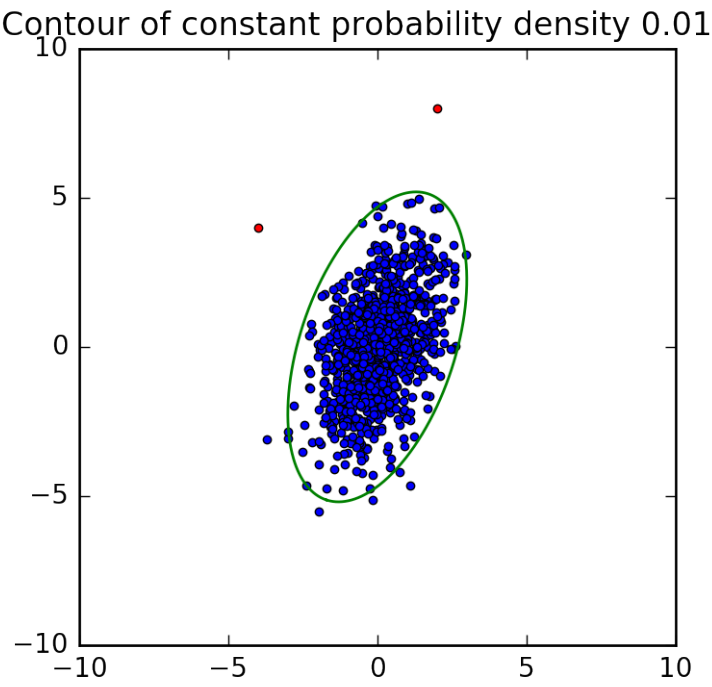
```
In [338]: n_samples = 1000
          cov = np.array([[1., 0.75],[0.75, 3]])
```

```
mean = np.array([0.,0])
apt1 = np.array([2,8])
apt2 = np.array([-4,4])
data = np.random.multivariate_normal(mean, cov, n_samples)
data = np.concatenate([data,np.array([apt1,apt2])])
```

In [339]:
```
plt.plot(data[:,0],data[:,1],'o',markersize=3)
plt.axis('square')
plt.xlim([-10,10])
_ = plt.ylim([-10,10])
```



In [340]:
```
theta = np.linspace(0,2*math.pi,500)
coords = np.array([np.sin(theta), np.cos(theta)])
cov = np.array([[1., 0.75],[0.75, 3]])
lam, evec = np.linalg.eig(cov)
c = evec @ np.diag(np.sqrt(lam))
coords = 3 * c @ coords
plt.plot(data[:-2,0],data[:-2,1],'o',markersize=3,color='b')
plt.plot(data[-2:,0],data[-2:,1],'o',markersize=3,color='r')
plt.plot(coords[0], coords[1], '-', color='g')
plt.axis('square')
plt.xlim([-10,10])
plt.ylim([-10,10])
_ = plt.title(r'Contour of constant probability density {:0.4f}'.format(r
```



Consider the following candidates for outliers: (2,8) and (-4,4).
These are marked in red.

```
In [341]: print('{} is {:0.3f} from the cluster center.'.format(apt1,np.linalg.norm
          print('{} is {:0.3f} from the cluster center.'.format(apt2,np.linalg.norm

[2 8] is 8.246 from the cluster center.
[-4  4] is 5.657 from the cluster center.
```

Which one is more of an outlier?

We have to take into account the **probability** of the point under the (presumed) multivariate Gaussian distribution.

Using standard (MLE) methods (on all the data), we estimate the Gaussian distribution to have mean

$$\mu = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

and covariance

$$\Sigma = \begin{bmatrix} 1 & 0.75 \\ 0.75 & 3 \end{bmatrix}$$

A convenient way to express the probability is via its negative log:

$$-\log(P[\mathbf{x}]) - C = (\mathbf{x} - \mu)^T \Sigma^{-1} (\mathbf{x} - \mu)$$

(C is a constant that does not depend on **x**.)

The expression on the right is called the **Mahalanobis distance.**

It is essentially the distance to the center of the Gaussian, scaled to take into account the **shape** of the Gaussian.

```
In [342]: p = np.array([apt1]).T
          mp = p.T @ np.linalg.inv(cov) @ p
          print('{} has Mahalanobis distance {:0.3f}.'.format(apt1,mp[0,0]))
          p = np.array([apt2]).T
          mp = p.T @ np.linalg.inv(cov) @ p
          print('{} has Mahalanobis distance {:0.3f}.'.format(apt2,mp[0,0]))
```

```
[2 8] has Mahalanobis distance 21.333.
[-4  4] has Mahalanobis distance 36.103.
```

Hence we can conclude that (-4, 4) is more of an outlier than (2, 8):

- Although it is closer to the cluster center in Euclidean distance,
- It is further from the cluster center in Mahalanobis distance.

1.4 High Dimensional Data

When our data objects have hundreds (or millions) of features, we can no longer build a distributional model.

For a dataset with 1,000 features, we need to build a 1,000 $\times$ 1,000 covariance matrix – which has a million elements.

We have a problem of high dimensionality – and a natural approach is to consider dimensionality reduction.

SVD to the rescue again!

As we've seen, dimensionality reduction will work if the dataset shows low effective rank.

Let's consider how we might do anomaly detection when data has low effective rank.

Since * the principle of anomaly detection is that most objects are normal, and
the data has low effective rank,

one way to look for anomalies is to find objects that are **not** well described by the low rank model.

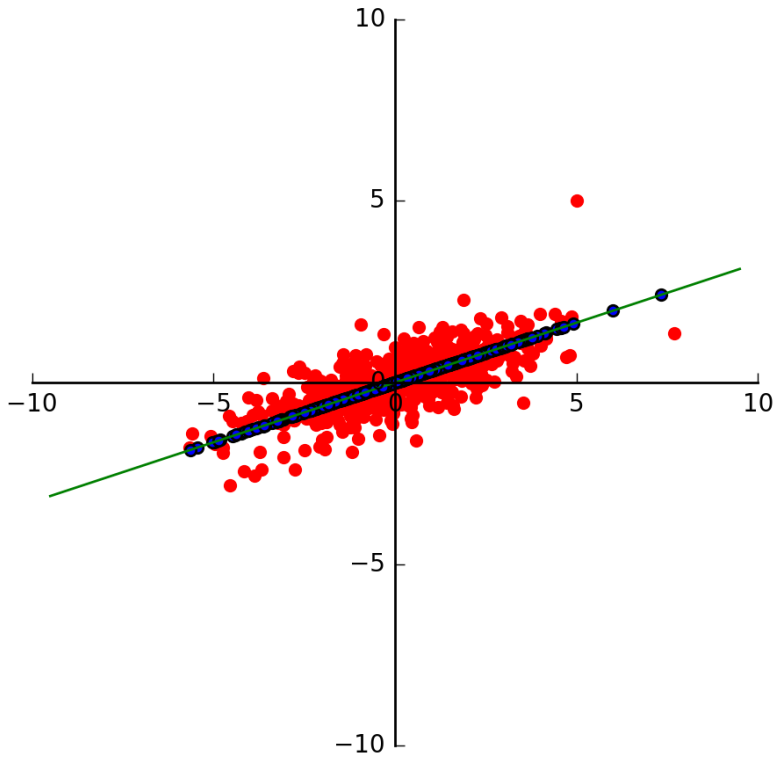
Let's start with our usual (toy) model in 2-D.

(Keeping in mind that this is to build intuition for the real problem, which is in high dimension.)

```
In [343]: n_samples = 500
          # Create correlated multivariate Gaussian samples
          C = np.array([[0.1, 0.6], [2., .6]])
          np.random.seed(1)
          X = np.random.randn(n_samples, 2) @ C + np.array([-6, 3])
          # Mean center
          Xc = X - np.mean(X,axis=0)
          # Create an anomalous data point
          apt = np.array([5,5])
```

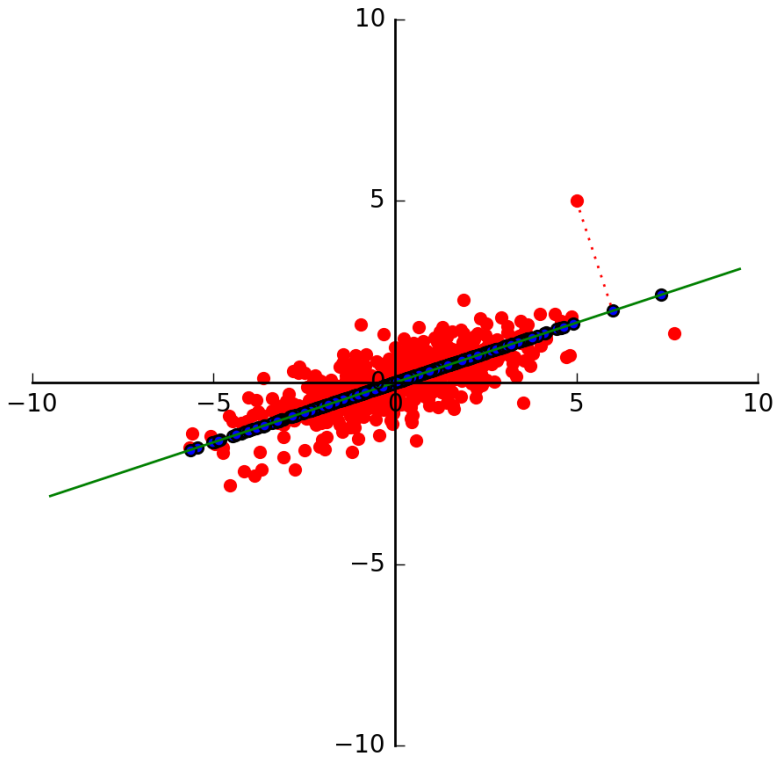
```
        Xc = np.concatenate([Xc, np.array([apt])],axis=0)
        # SVD of all data
        u, s, vt = np.linalg.svd(Xc,full_matrices=False)
        orthog_dir = np.array([-vt[0,1], vt[0,0]])
        # project points onto subspace
        scopy = s.copy()
        scopy[1] = 0.
        reducedX = u @ np.diag(scopy) @ vt
        apt_proj = reducedX[-1,:]
```

In [344]:
```
        # plot
        ax = ut.plotSetup(-10,10,-10,10,(8,8))
        ut.centerAxes(ax)
        plt.axis('equal')
        plt.scatter(Xc[:,0],Xc[:,1], color='r')
        plt.scatter(reducedX[:,0], reducedX[:,1])
        endpoints = np.array([[-10],[10]]) @ vt[[0],:]
        _ = plt.plot(endpoints[:,0], endpoints[:,1], 'g-')
```



Is there a point here that is not well described by the low-rank (rank-1) model? How would we quantify this fact?

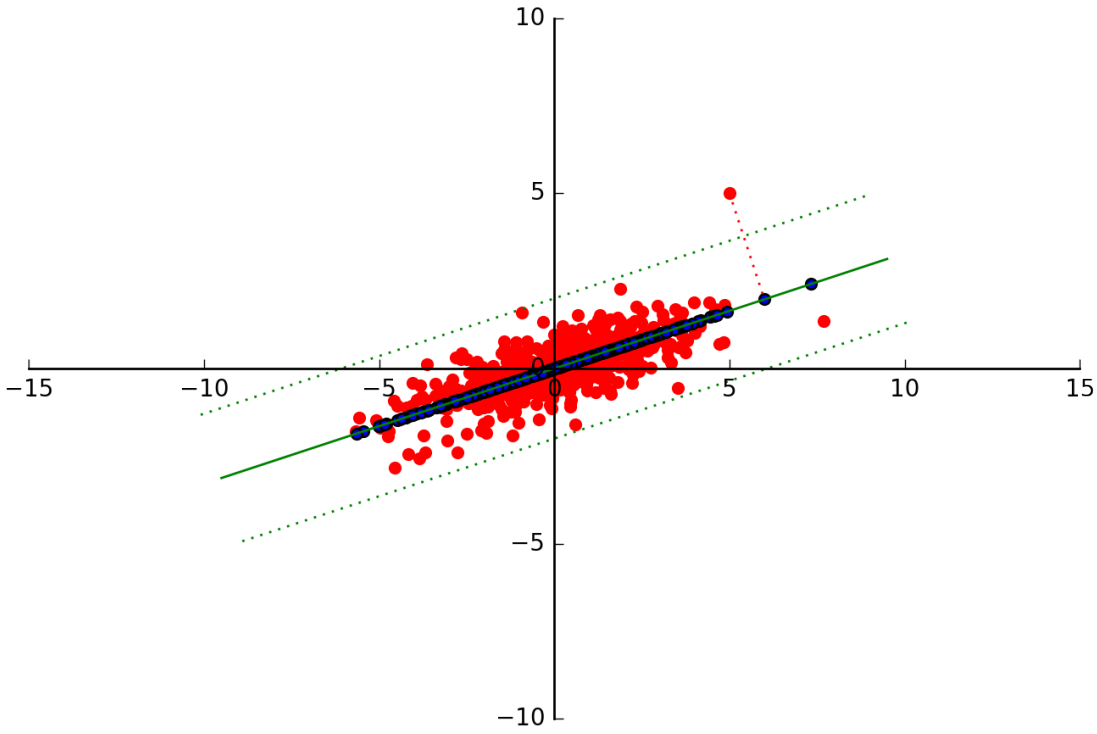
```
In [345]: # plot
          ax = ut.plotSetup(-10,10,-10,10,(8,8))
          ut.centerAxes(ax)
          plt.axis('equal')
          plt.scatter(Xc[:,0],Xc[:,1], color='r')
          plt.scatter(reducedX[:,0], reducedX[:,1])
          plt.plot([apt[0],apt_proj[0]],[apt[1],apt_proj[1]],'r:')
          endpoints = np.array([[-10],[10]]) @ vt[[0],:]
          _ = plt.plot(endpoints[:,0], endpoints[:,1], 'g-')
```



What is the distance of the anomalous point from the subspace?
It is simply the **length of the difference** between the point and its projection in the subspace.

```
In [346]: # plot
          ax = ut.plotSetup(-10,10,-10,10,(8,8))
          ut.centerAxes(ax)
          plt.axis('equal')
          plt.scatter(Xc[:,0],Xc[:,1], color='r')
          plt.scatter(reducedX[:,0], reducedX[:,1])
          plt.plot([apt[0],apt_proj[0]],[apt[1],apt_proj[1]],'r:')
          endpoints = np.array([[-10],[10]]) @ vt[[0],:]
          alpha = 1.9
          plt.plot(alpha*orthog_dir[0]+endpoints[:,0], alpha*orthog_dir[1]+endpoint
```

```
plt.plot(endpoints[:,0]-alpha*orthog_dir[0], endpoints[:,1]-alpha*orthog_
_ = plt.plot(endpoints[:,0], endpoints[:,1], 'g-')
```



So to do anomaly detection via the **subspace** method, we set a threshold on the distance of each point from the subspace.

1.5 Anomaly Detection via the Low-Rank Approximation

In practice, this is a simple process.

Given a data matrix A:

1. Compute the Singular value decomposition of A,

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

2. Compute a low-rank approximation to A,

$$N = U'\Sigma'(V')^T.$$

3. Compute the residuls not explained by N:

$$O = A - N.$$

4. Indentify the rows of O with largest ℓ_2 norm: these rows correspond to anomalies.

In this recipe, rows of O are the difference vectors between each point and its projection in the subspace.

So the ℓ_2 norm gives us the distance of each point from the subspace.

There are two unspecified steps in the process:

1. Selecting the columns of U to be used in forming N
2. Deciding how many of the largest rows of O are anomalies.

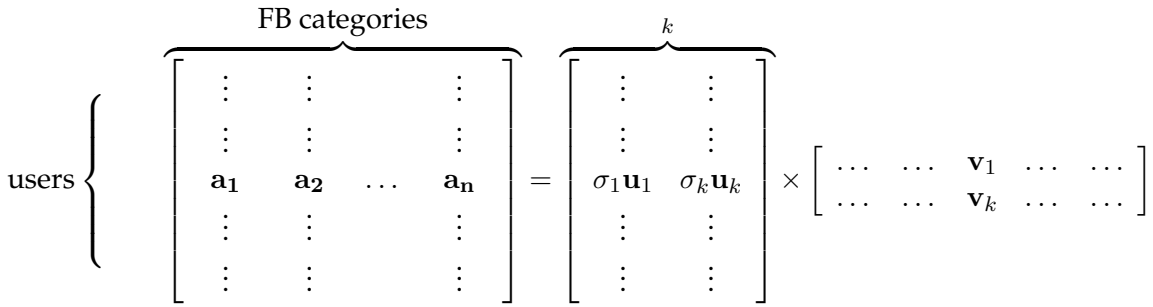
For 1, the general idea is to choose a k at the knee of the singular value plot.

For 2, there are statistical methods that generally work reasonably well. However, one can always just rank the points by their residual norm, which is what we'll do.

1.5.1 Example 1: Facebook Spatial Likes

This data consists of the number of 'Likes' during a six month period, for each of 9000 users across the 210 content categories that Facebook assigns to pages.

Rows are users, Columns are categories. A is 9000×210.



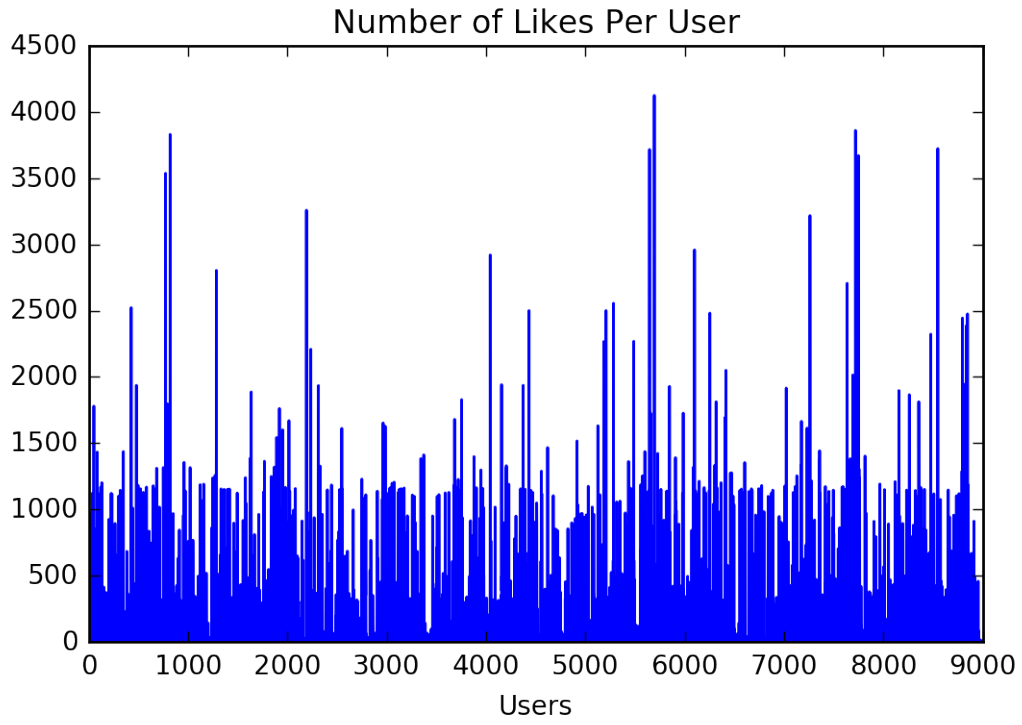
$$A = U\Sigma V^T$$

```
In [347]: data = np.loadtxt('data/social/spatial_data.txt')
          data[:10]
```

```
Out[347]: array([[ 0.,  0.,  0., ...,  0.,  0.,  0.],
                 [ 0.,  0.,  0., ...,  0.,  0.,  0.],
                 [ 1.,  0.,  0., ...,  0.,  2.,  8.],
                 ...,
                 [ 0.,  0.,  0., ...,  0.,  0.,  0.],
                 [ 0.,  0.,  0., ...,  0.,  0.,  1.],
                 [ 0.,  0.,  0., ...,  0.,  0.,  0.]])
```

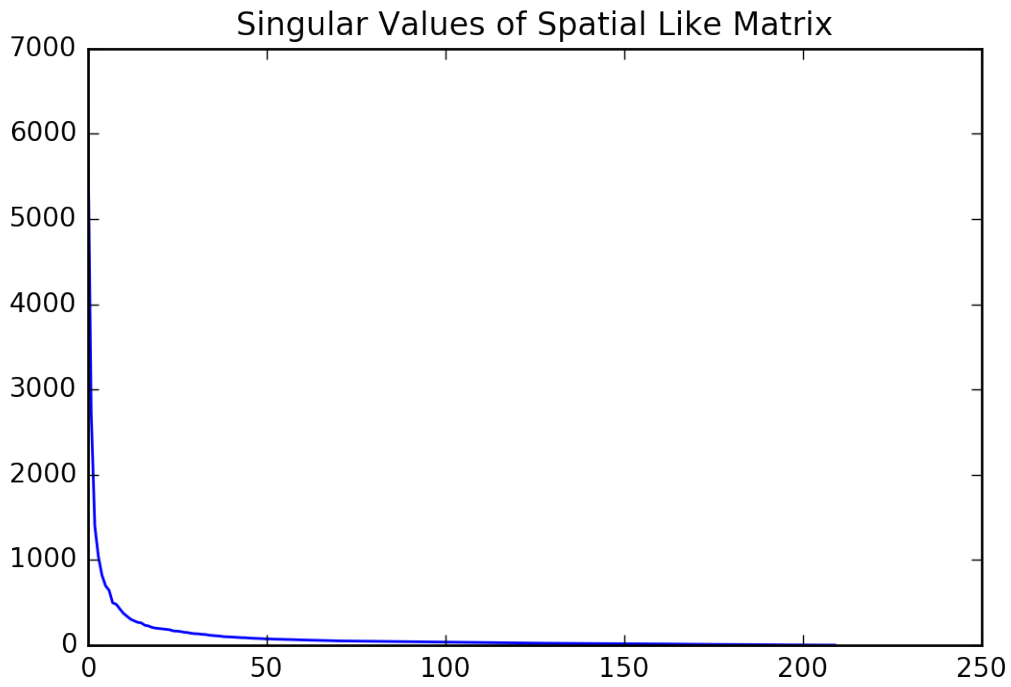
First we'll look at the total number of likes for each user (the row sums).

```
In [348]: FBSpatial = data[:,1:]
          FBSnorm = np.linalg.norm(FBSpatial,axis=1,ord=1)
          plt.plot(FBSnorm)
          plt.title('Number of Likes Per User')
          _ = plt.xlabel('Users')
```



Now let's check whether the low rank approximation holds.

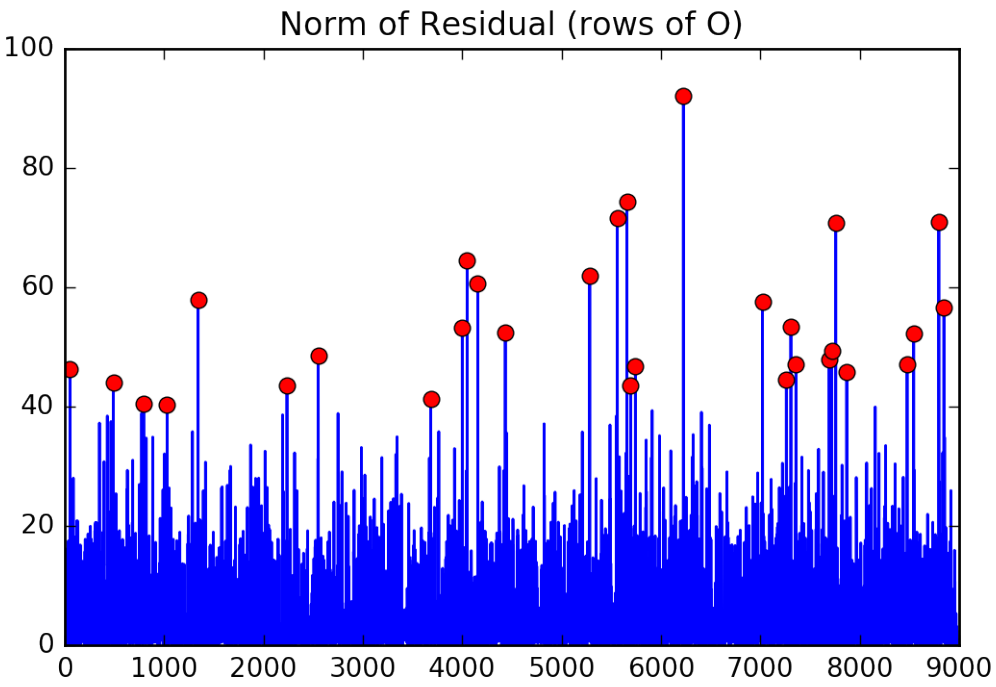
```
In [360]: u,s,vt = np.linalg.svd(FBSpatial,full_matrices=False)
          plt.plot(s)
          _ = plt.title('Singular Values of Spatial Like Matrix')
```



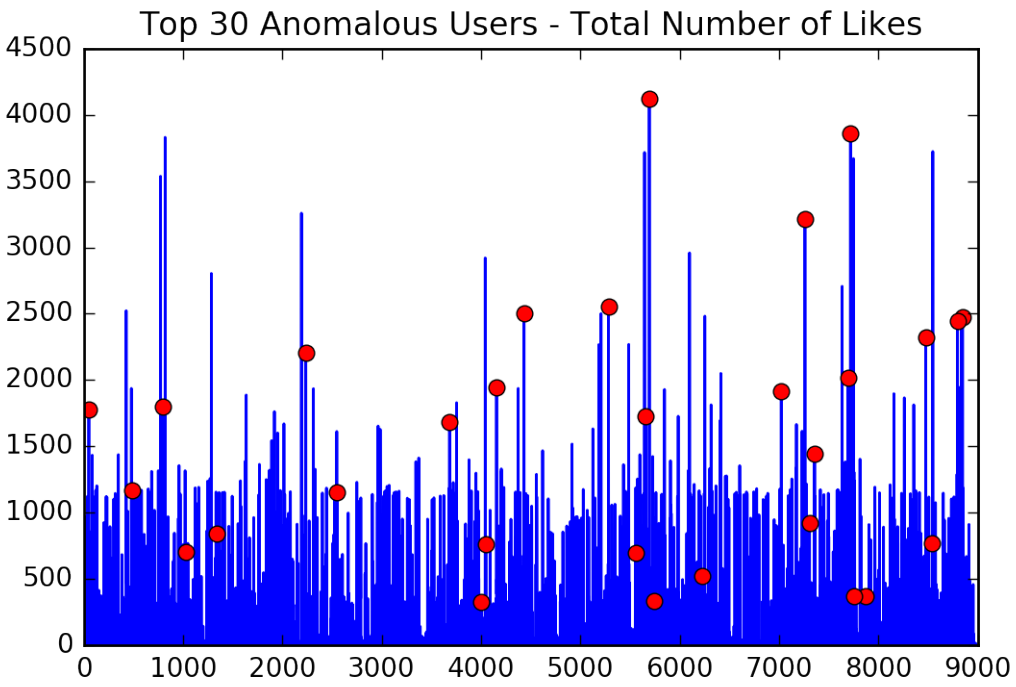
We'll approximate this data as having effective rank 25.
Now let's

1. Separate the portion of the data lying in the normal space from the anomalous space,
2. Identify the top 30 anomalous users (having the largest residual component), and
3. Plot their total number of likes against the set of all users.

```
In [350]: scopy = s.copy()
          scopy[25:] = 0.
          N = u @ np.diag(scopy) @ vt
          O = FBSpatial - N
          Onorm = np.linalg.norm(O,axis=1)
          anomSet = np.argsort(Onorm)[-30:]
          plt.plot(Onorm)
          plt.plot(anomSet,Onorm[anomSet],'ro')
          _ = plt.title('Norm of Residual (rows of O)')
```

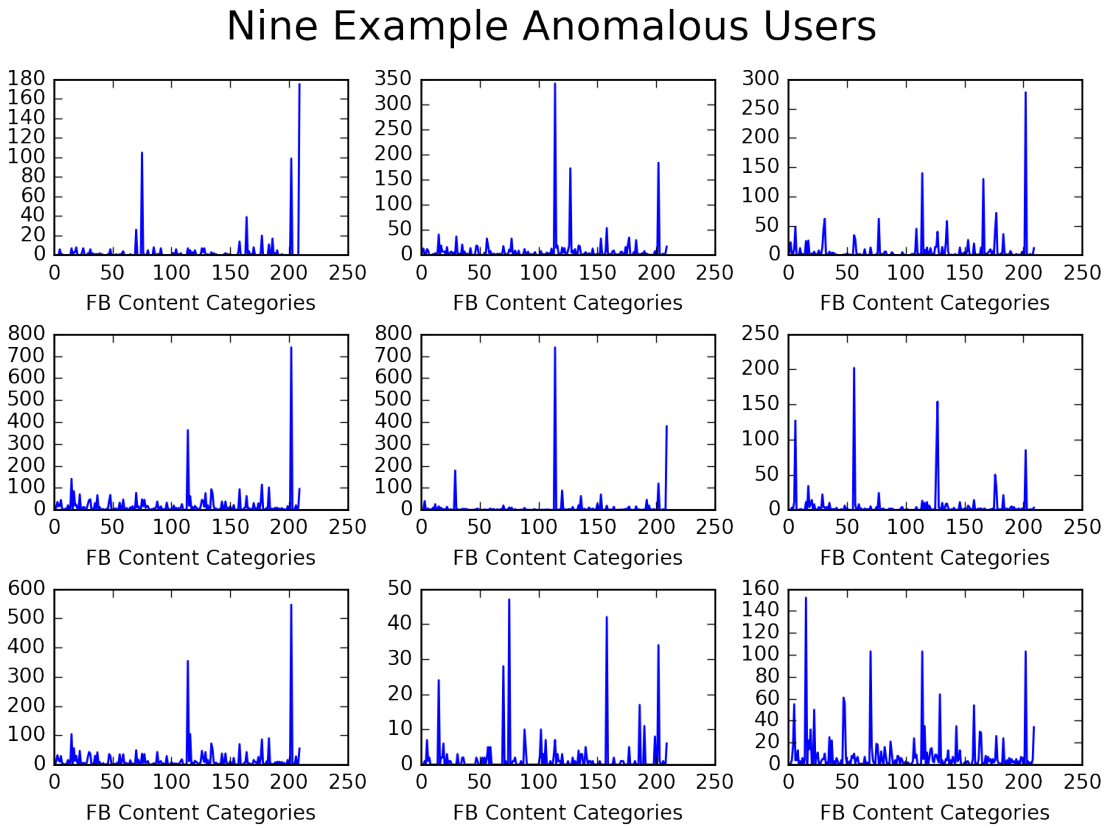



```
In [351]: # large = np.nonzero(Onorm>100))
          # get top 30 anomalies
          anomSet = np.argsort(Onorm)[-30:]
          plt.plot(FBSnorm)
          plt.plot(anomSet,FBSnorm[anomSet],'ro')
          _ = plt.title('Top 30 Anomalous Users - Total Number of Likes')
```



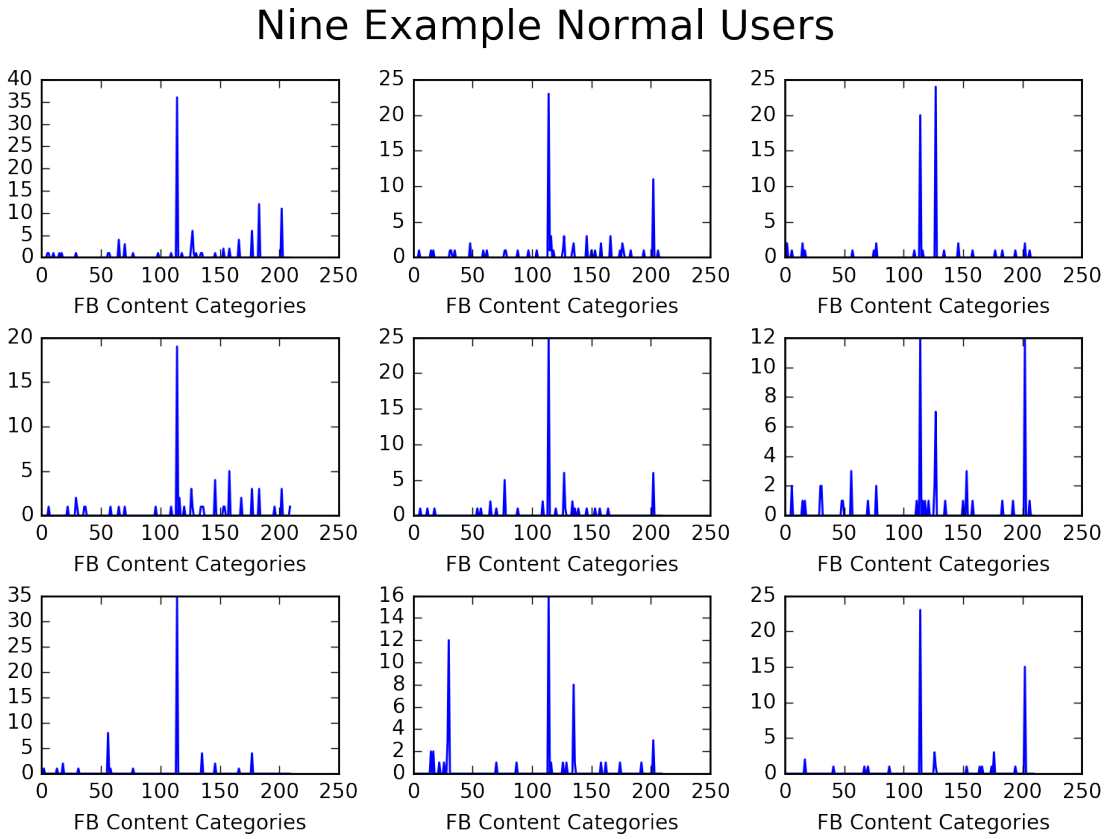
Next we'll pick out nine anomalous users and look at their pattern of likes across the 210 categories.

```
In [352]: plt.figure(figsize=(9,6))
          for i in range(1,10):
              ax = plt.subplot(3,3,i)
              plt.plot(FBSpatial[anomSet[i-1],:])
              plt.xlabel('FB Content Categories')
          plt.subplots_adjust(wspace=0.25,hspace=0.45)
          _ = plt.suptitle('Nine Example Anomalous Users',size=20)
```



And let's do the same for nine normal users.

```
In [353]: # choose non-anomalous users
          set = np.argsort(Onorm)[0:7000]
          # that have high overall volume
          max = np.argsort(FBSnorm[set])[::-1]
          plt.figure(figsize=(9,6))
          for i in range(1,10):
              ax = plt.subplot(3,3,i)
              plt.plot(FBSpatial[set[max[i-1]],:])
              plt.xlabel('FB Content Categories')
          plt.subplots_adjust(wspace=0.25,hspace=0.45)
          _ = plt.suptitle('Nine Example Normal Users',size=20)
```



1.5.2 Example 2: Facebook Temporal LIkes

This data consists of the number of 'Likes' for each of 9000 users, over 6 months, on a daily basis Rows are users, Columns are days.

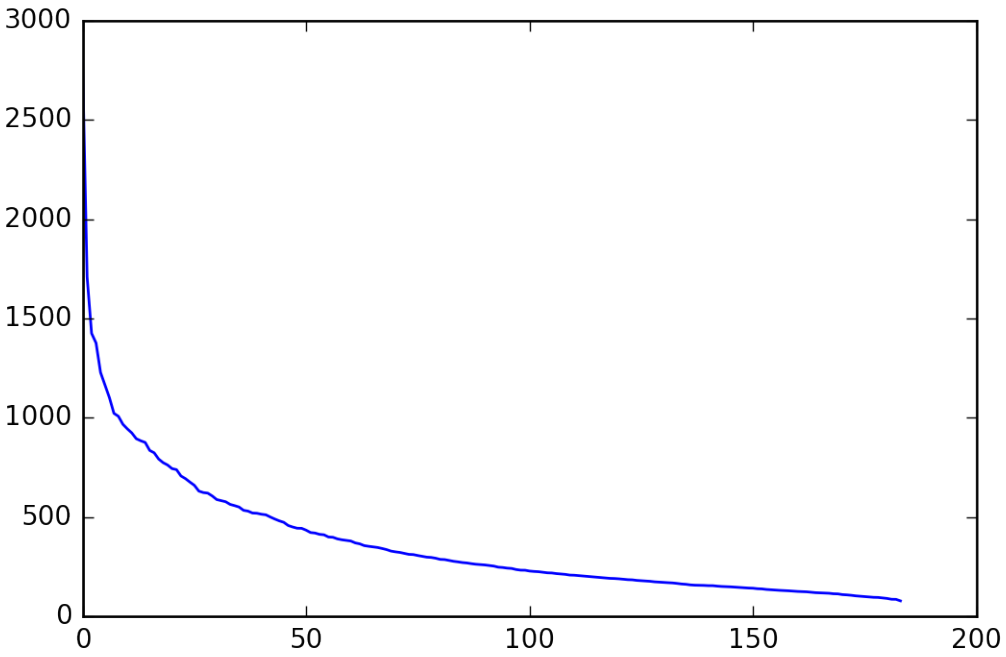
$$\text{users} \left\{ \overbrace{\begin{bmatrix} \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ \mathbf{a_1} & \mathbf{a_2} & \dots & \mathbf{a_n} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \end{bmatrix}}^{\text{days}} \right. = \overbrace{\begin{bmatrix} \vdots & \vdots \\ \vdots & \vdots \\ \sigma_1 \mathbf{u}_1 & \sigma_k \mathbf{u}_k \\ \vdots & \vdots \\ \vdots & \vdots \end{bmatrix}}^{k} \times \begin{bmatrix} \dots & \dots & \mathbf{v}_1 & \dots & \dots \\ \dots & \dots & \mathbf{v}_k & \dots & \dots \end{bmatrix}$$

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

First we'll look at the singular values.

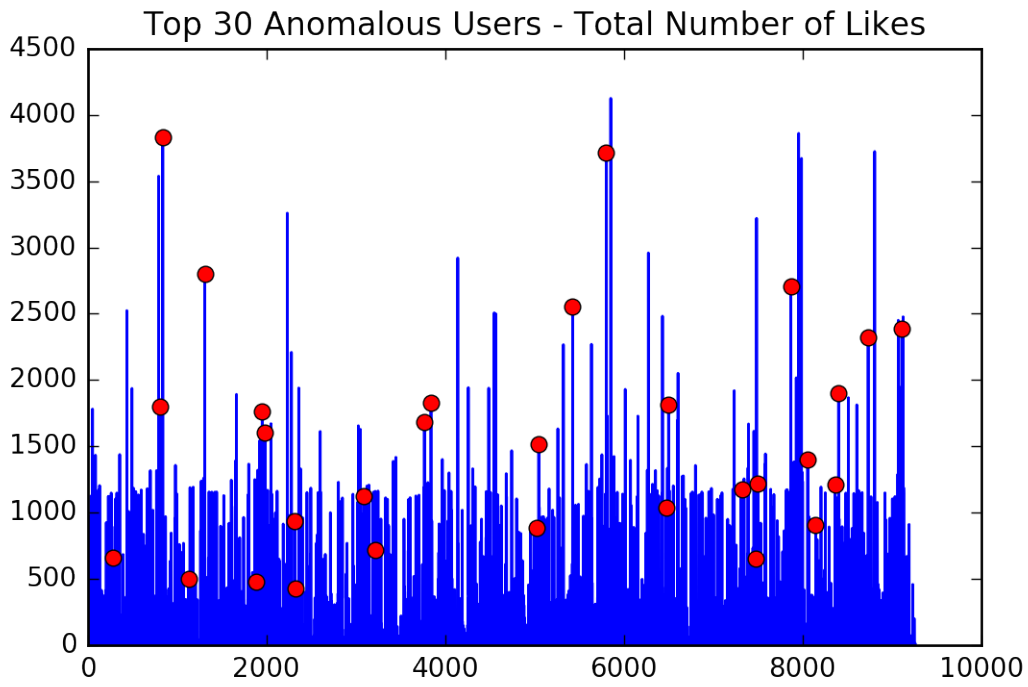
```
In [363]: data = np.loadtxt('data/social/temporal_data.txt')
          FBTemporal = data[:,1:]
```

```
FBTnorm = np.linalg.norm(FBTemporal,axis=1,ord=1)
u,s,vt = np.linalg.svd(FBTemporal,full_matrices=False)
_ = plt.plot(s)
```



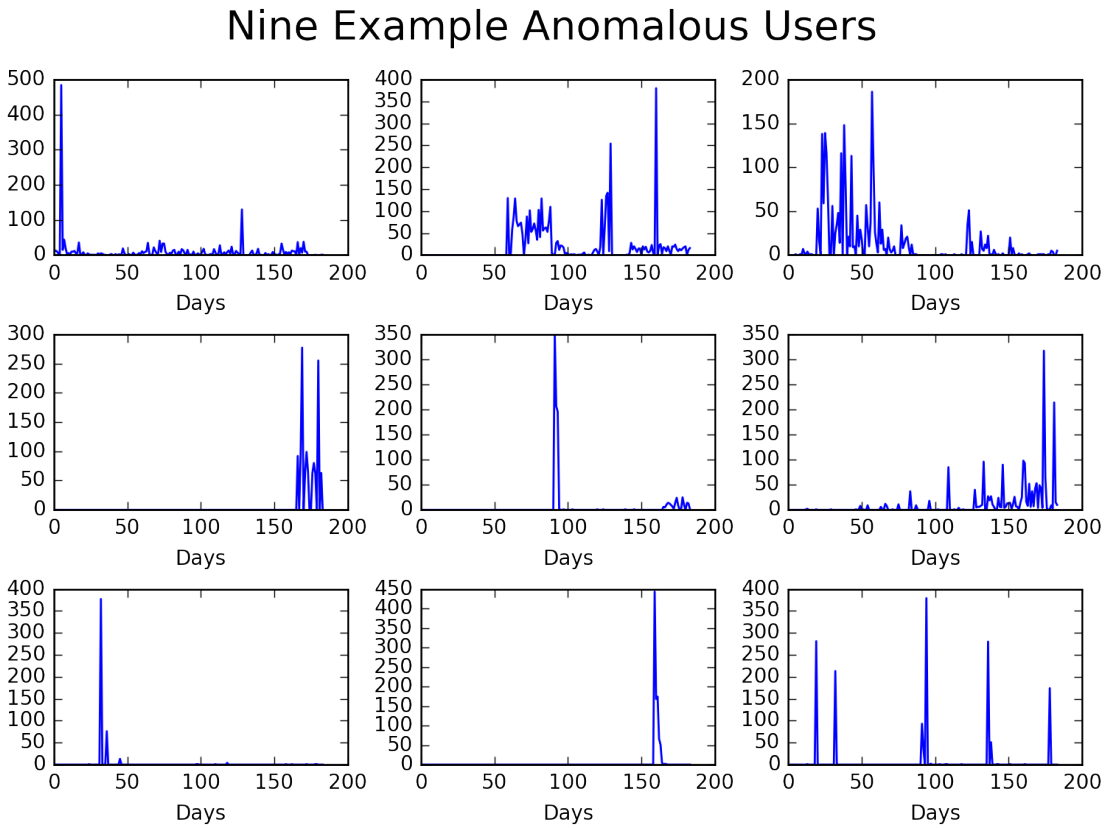
We'll again assume an effective rank of 25.
Next, plot the anomalous users as before.

```
In [355]: # choose the top 25 columns of U for the normal space
          unorm = u[:,0:24]
          P = unorm.dot(unorm.T)
          N = P.dot(FBTemporal)
          O = FBTemporal - N
          Onorm = np.linalg.norm(O,axis=1)
          # get top 30 anomalies
          anomSet = np.argsort(Onorm)[-30:]
          plt.plot(FBTnorm)
          plt.plot(anomSet,FBTnorm[anomSet],'ro')
          _ = plt.title('Top 30 Anomalous Users - Total Number of Likes')
```

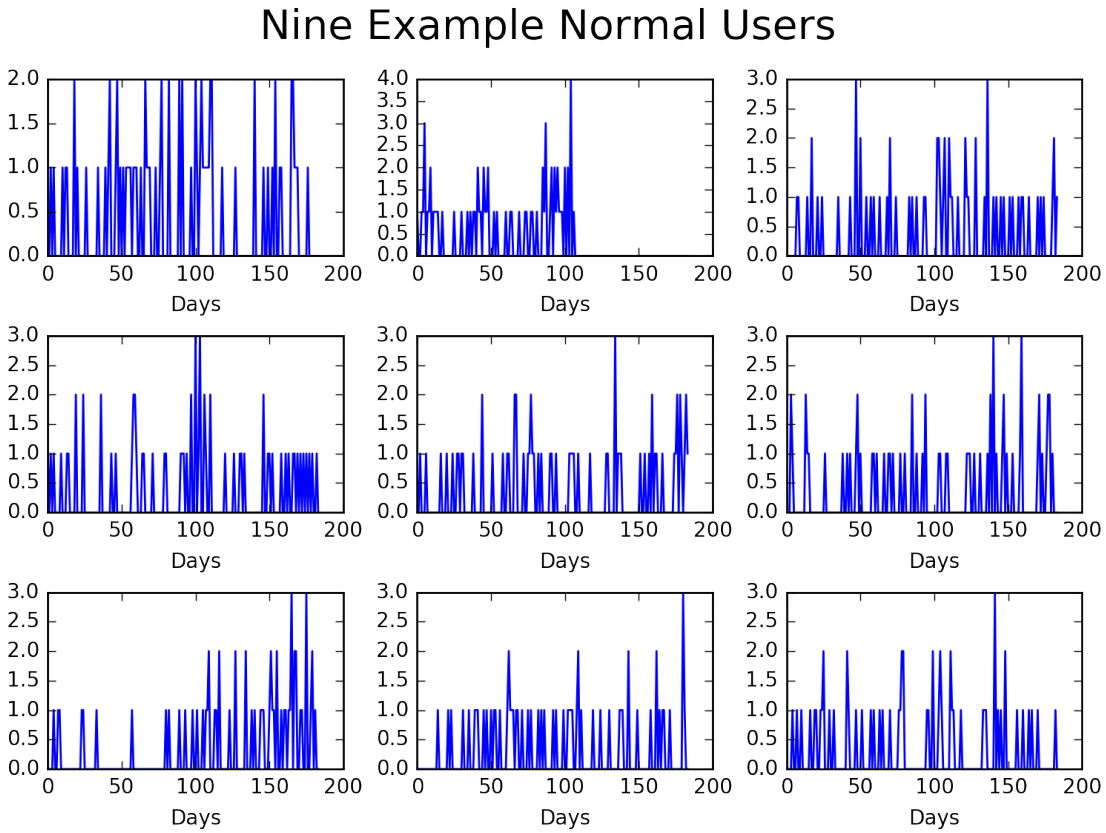


Now let's look at sample anomalous and normal users.

```
In [356]: plt.figure(figsize=(9,6))
          for i in range(1,10):
              ax = plt.subplot(3,3,i)
              plt.plot(FBTemporal[anomSet[i-1],:])
              plt.xlabel('Days')
          plt.subplots_adjust(wspace=0.25,hspace=0.45)
          _ = plt.suptitle('Nine Example Anomalous Users',size=20)
```




```
In [357]: # choose non-anomalous users
          set = np.argsort(Onorm)[0:7000]
          # that have high overall volume
          max = np.argsort(FBTnorm[set])[::-1]
          plt.figure(figsize=(9,6))
          for i in range(1,10):
              ax = plt.subplot(3,3,i)
              plt.plot(FBTemporal[set[max[i-1]],:])
              plt.xlabel('Days')
          plt.subplots_adjust(wspace=0.25,hspace=0.45)
          _ = plt.suptitle('Nine Example Normal Users',size=20)
```



Interestingly, what makes a user anomalous seems to have reversed from the case of the spatial data.