Abstract

We propose a new method for clustering based on finding maximum margin hyperplanes through data. By reformulating the problem in terms of the implied equivalence relation matrix, we can pose the problem as a convex integer program. Although this still yields a difficult computational problem, the hard-clustering constraints can be relaxed to a soft-clustering formulation which can be feasibly solved with a semidefinite program. Since our clustering technique only depends on the data through the kernel matrix, we can easily achieve nonlinear clusterings in the same manner as spectral clustering. Experimental results show that our maximum margin clustering technique often obtains more accurate results than conventional clustering methods. The real benefit of our approach, however, is that it leads naturally to a semi-supervised training method for support vector machines. By maximizing the margin simultaneously on labeled and unlabeled training data, we achieve state of the art performance by using a single, integrated learning principle.

1 Introduction

Clustering is one of the oldest forms of machine learning. Nevertheless, it has received a significant amount of renewed attention with the advent of nonlinear clustering methods based on kernels. Kernel based clustering methods continue to have a significant impact on recent work in machine learning [14, 13], computer vision [16], and bioinformatics [9].

Although many variations of kernel based clustering has been proposed in the literature, most of these techniques share a common “spectral clustering” framework that follows a generic recipe: one first builds the kernel (“affinity”) matrix, normalizes the kernel, performs dimensionality reduction, and finally clusters (partitions) the data based on the resulting representation [17].

In this paper, our primary focus will be on the final partitioning step where the actual clustering occurs. Once the data has been preprocessed and a kernel matrix has been constructed (and its rank possibly reduced), many variants have been suggested in the literature for determining the final partitioning of the data. The predominant strategies include using k-means clustering [14], minimizing various forms of graph cut cost [13] (relaxations of which amount to clustering based on eigenvectors [17]), and finding strongly connected components in a Markov chain defined by the normalized kernel [4]. Some other recent alternatives are correlation clustering [12] and support vector clustering [1].

What we believe is missing from this previous work however, is a simple connection to...
other types of machine learning, such as semisupervised and supervised learning. In fact, one of our motivations is to seek unifying machine learning principles that can be used to combine different types of learning problems in a common framework. For example, a useful goal for any clustering technique would be to find a way to integrate it seamlessly with a supervised learning technique, to obtain a principled form of semisupervised learning. A good example of this is [18], which proposes a general random field model based on a given kernel matrix. They then find a soft cluster assignment on unlabeled data that minimizes a joint loss with observed labels on supervised training data. Unfortunately, this technique actually requires labeled data to cluster the unlabeled data. Nevertheless, it is a useful approach.

Our goal in this paper is to investigate another standard machine learning principle—maximum margin classification—and modify it for clustering, with the goal of achieving a simple, unified way of solving a variety of problems, including clustering and semisupervised learning.

Although one might be skeptical that clustering based on large margin discriminants can perform well, we will see below that, combined with kernels, this strategy can often be more effective than conventional spectral clustering. Perhaps more significantly, it also immediately suggests a simple semisupervised training technique for support vector machines (SVMs) that appears to improve the state of the art.

The remainder of this paper is organized as follows. After establishing the preliminary ideas and notation in Section 2, we tackle the problem of computing a maximum margin clustering for a given kernel matrix in Section 3. Although it is not obvious that this problem can be solved efficiently, we show that the optimal clustering problem can in fact be formulated as a convex integer program. We then propose a relaxation of this problem which yields a semidefinite program that can be used to efficiently compute a soft clustering. Section 4 gives our experimental results for clustering. Then, in Section 5 we extend our approach to semisupervised learning by incorporating additional labeled training data in a seamless way. We then present experimental results for semisupervised learning in Section 6 and conclude.

2 Preliminaries

Since our main clustering idea is based on finding maximum margin separating hyperplanes, we first need to establish the background ideas from SVMs as well as establish the notation we will use.

For SVM training, we assume we are given labeled training examples \((x^1, y^1), \ldots, (x^N, y^N)\), where each example is assigned to one of two classes \(y^i \in \{-1, +1\}\). The goal of an SVM of course is to find the linear discriminant \(f_{w, b}(x) = w^T \phi(x) + b\) that maximizes the minimum misclassification margin

\[
\gamma^* = \max_{w, b, \gamma} \gamma \quad \text{subject to} \quad y^{i}(w^T \phi(x^i) + b) \geq \gamma, \forall i = 1, \ldots, N, \|w\|_2 = 1
\]  

(1)

Here the Euclidean normalization constraint on \(w\) ensures that the Euclidean distance between the data and the separating hyperplane (in \(\phi(x)\) space) determined by \(w^*, b^*\) is maximized. It is easy to show that this same \(w^*, b^*\) is a solution to the quadratic program

\[
\gamma^{*-2} = \min_{w, b} \|w\|^2 \quad \text{subject to} \quad y^{i}(w^T \phi(x^i) + b) \geq 1, \forall i = 1, \ldots, N
\]  

(2)

Importantly, the minimum value of this quadratic program, \(\gamma^{*-2}\), is just the inverse square of the optimal solution value \(\gamma^*\) to (1) [10].

To cope with potentially inseparable data, one normally introduces slack variables to reduce the dependence on noisy examples. This leads to the so called soft margin SVM (and its
dual) which is controlled by a tradeoff parameter $C$

$$\gamma^* = \min_{w, \epsilon, c} \|w\|^2 + C \epsilon \mathbf{e} \quad \text{subject to} \quad y^i (w^T \phi(x^i) + b) \geq 1 - \epsilon_i, \forall i = 1, \ldots, N, \quad \epsilon \geq 0$$

$$\gamma^* = \max_{\lambda} 2 \lambda^T \mathbf{e} - \langle K \circ \lambda \lambda^T, yy^T \rangle \quad \text{subject to} \quad 0 \leq \lambda \leq C, \lambda^T y = 0 \quad (3)$$

The notation we use in this dual formulation requires some explanation, since we will use it below: Here $K$ denotes the $N \times N$ kernel matrix formed from the inner products of feature vectors $\Phi = [\phi(x^1), \ldots, \phi(x^N)]$ such that $K = \Phi^T \Phi$. Thus $k_{ij} = \phi(x^i)^T \phi(x^j)$. The vector $\mathbf{e}$ denotes the vector of all 1 entries. We let $A \circ B$ denote componentwise matrix multiplication, and let $\langle A, B \rangle = \sum_{ij} a_{ij} b_{ij}$. Note that (3) is derived from the standard dual SVM by using the fact that $\lambda^T (K \circ yy^T) \lambda = \langle K \circ yy^T, \lambda \lambda^T \rangle = \langle K \circ \lambda \lambda^T, yy^T \rangle$.

To summarize: for supervised maximum margin training, one takes a given set of labeled training data $(x^1, y^1), \ldots, (x^N, y^N)$, forms the kernel matrix $K$ on data inputs, forms the kernel matrix $yy^T$ on target outputs, sets the slack parameter $C$, and solves the quadratic program (3) to obtain the dual solution $\lambda^*$ and the inverse square maximum margin value $\gamma^{*-2}$. Once these are obtained, one can then recover a classifier directly from $\lambda^*$ [15].

Of course, our main interest initially is not to find a large margin classifier given labels on the data, but instead to find a labeling that results in a large margin classifier.

3 Maximum margin clustering

The clustering principle we investigate is to find a labeling so that if one were to subsequently run an SVM, the margin obtained would be maximal over all possible labelings. That is, given data $x^1, \ldots, x^N$, we wish to assign the data points to two classes $y^i \in \{-1, +1\}$ so that the separation between the two classes is as wide as possible.

Unsurprisingly, this is a hard computational problem. However, with some reformulation we can express it as a convex integer program, which suggests that there might be some hope of obtaining practical solutions. However, more usefully, we can relax the integer constraint to obtain a semidefinite program that yields soft cluster assignments which approximately maximize the margin. Therefore, one can obtain soft clusterings efficiently using widely available software. However, before proceeding with the main development, there are some preliminary issues we need to address.

First, we clearly need to impose some sort of constraint on the class balance, since otherwise one could simply assign all the data points to the same class and obtain an unbounded margin. A related issue is that we would also like to avoid the problem of separating a single outlier (or very small group of outliers) from the rest of the data. Thus, to mitigate these effects we will impose a constraint that the difference in class sizes be bounded. This will turn out to be a natural constraint for semisupervised learning and is very easy to enforce. Second, we would like the clustering to behave gracefully on noisy data where the classes may in fact overlap, so we adopt the soft margin formulation of the maximum margin criterion. Third, although it is indeed possible to extend our approach to the multiclass case [5], the extension is not simple and for ease of presentation we focus on simple two class clustering in this paper. Finally, there is a small technical complication that arises with one of the SVM parameters: It turns out that an unfortunate nonconvexity problem arises when we include the use of the offset $b$ in the underlying large margin classifier. We currently do not have a way to avoid this nonconvexity, and therefore we currently set $b = 0$ and therefore only consider homogeneous linear classifiers. The consequence of this restriction is that the constraint $\lambda^T y = 0$ is removed from the dual SVM quadratic program (3). Although it would seem like this is a harsh restriction, the negative effects are mitigated by centering the data at the origin, which can always be imposed. Nevertheless, dropping this
restriction remains an important question for future research. With these caveats in mind, we proceed to the main development.

We wish to solve for a labeling \( y \in \{-1,+1\}^N \) that leads to a maximum (soft) margin. Straightforwardly, one could attempt to tackle this optimization problem by directly formulating

\[
\min_{y \in \{-1,+1\}^N} \gamma^{*2}(y) \quad \text{subject to} \quad -\ell \leq e^T y \leq \ell \quad \text{where}
\]

\[
\gamma^{*2}(y) = \max_{\lambda} 2\lambda^T e - \langle K \circ \lambda \lambda^T, yy^T \rangle \quad \text{subject to} \quad 0 \leq \lambda \leq C
\]

Unfortunately, \( \gamma^{*2}(y) \) is not a convex function of \( y \), and this formulation does not lead to an effective algorithmic approach. In fact, to obtain an efficient technique for solving this problem we need two key insights.

The first key step is to re-express this optimization, not directly in terms of the cluster labels \( y \), but instead in terms of the label kernel matrix \( M = yy^T \). The main advantage of doing so is that the inverse soft margin \( \gamma^{*-2} \) is in fact a convex function of \( M \)

\[
\gamma^{*-2}(M) = \max_{\lambda} 2\lambda^T e - \langle K \circ \lambda \lambda^T, M \rangle \quad \text{subject to} \quad 0 \leq \lambda \leq C \quad (4)
\]

The convexity of \( \gamma^{*-2} \) with respect to \( M \) is easy to establish since this quantity is just a maximum over linear functions of \( M \) [3]. This observation parallels one of the key insights of [10], here applied to \( M \) instead of \( K \).

Unfortunately, even though we can posit a convex objective, it does not allow us to immediately solve our problem because we still have to relate \( M \) to \( y \), and \( M = yy^T \) is not a convex constraint. Thus, the main challenge is to find a way to constrain \( M \) to ensure \( M = yy^T \) while respecting the class balance constraints \(-\ell \leq e^T y \leq \ell \). One obvious way to enforce \( M = yy^T \) would be to impose the constraint that \( \text{rank}(M) = 1 \), since combined with \( M \in \{-1,+1\}^{N \times N} \) this forces \( M \) to have a decomposition \( yy^T \) for some \( y \in \{-1,+1\}^N \). Unfortunately, \( \text{rank}(M) = 1 \) is not a convex constraint on \( M \) [7].

Our second key idea is to realize that one can indirectly enforce the desired relationship \( M = yy^T \) by imposing a different set of linear constraints on \( M \). To do so, notice that any such \( M \) must encode an equivalence relation over the training points. That is, if \( M = yy^T \) for some \( y \in \{-1,+1\}^N \) then we must have

\[
m_{ij} = \begin{cases} 
1 & \text{if } y_i = y_j \\
-1 & \text{if } y_i \neq y_j 
\end{cases}
\]

Therefore, to enforce the constraint \( M = yy^T \) for \( y \in \{-1,+1\}^N \) it suffices to impose the set of constraints: (1) \( M \) encodes an equivalence relation, namely that it is transitive, reflexive and symmetric; (2) \( M \) has at most two equivalence classes; and (3) \( M \) has at least two equivalence classes. Fortunately we can enforce each of these requirements by imposing a set of linear constraints on \( M \in \{-1,+1\}^{N \times N} \) respectively:

\[
\mathcal{L}_1: \quad m_{ii} = 1; \quad m_{ij} = m_{ji}; \quad m_{ik} \geq m_{ij} + m_{jk} - 1; \quad \forall i,j,k
\]

\[
\mathcal{L}_2: \quad m_{jk} \geq -m_{ij} - m_{ik} - 1; \quad \forall i,j,k
\]

\[
\mathcal{L}_3: \quad \sum_i m_{ij} \leq N - 2; \quad \forall j
\]

The result is that with only linear constraints on \( M \) we can enforce the condition \( M = yy^T \). Finally, we can enforce the class balance constraint \(-\ell \leq e^T y \leq \ell \) by imposing the additional set of linear constraints:

\[
\text{Interestingly, for } M \in \{-1,+1\}^{N \times N} \text{ the first two sets of linear constraints can be replaced by the compact set of convex constraints } \text{diag}(M) = e, M \succeq 0 \text{ [7, 11]. However, when we relax the integer constraint below, this equivalence is no longer true and we realize some benefit in keeping the linear equivalence relation constraints.}
\]
\[ L_4: -\ell \leq \sum_i m_{ij} \leq \ell; \ \forall j \]

which obviates \( L_3 \).

The combination of these two steps leads to our first main result: One can solve for a hard clustering \( y \) that maximizes the soft margin by solving a convex integer program. To accomplish this, one first solves for the equivalence relation matrix \( M \) in

\[
\min_{M \in \{-1,+1\}^{N \times N}} \max_{\lambda} 2\lambda^T e - \langle K \circ \lambda \lambda^T, M \rangle \text{ subject to } 0 \leq \lambda \leq C, L_1, L_2, L_4
\]

(5)

Then, from the solution \( M^* \) recover the optimal cluster assignment \( y^* \) simply by setting \( y^* \) to any column vector in \( M^* \).

Unfortunately, the formulation (5) is still not practical because convex integer programming is still a hard computational problem. Therefore, we are compelled to take one further step and relax the integer constraint on \( M \) to obtain a convex optimization problem over a continuous parameter space

\[
\min_{M \in [-1,+1]^{N \times N}} \max_{\lambda} 2\lambda^T e - \langle K \circ \lambda \lambda^T, M \rangle \text{ subject to } 0 \leq \lambda \leq C, L_1, L_2, L_4, M \geq 0
\]

(6)

This can be turned into an equivalent semidefinite program using essentially the same derivation as in [10], yielding

\[
\min_{M, \delta, \mu, \nu} \delta \text{ subject to } L_1, L_2, L_4, \mu \geq 0, \nu \geq 0, M \geq 0
\]

\[
\begin{bmatrix}
M \circ K & e + \mu - \nu \\
(e + \mu - \nu)^T & \delta - 2C \nu^T e
\end{bmatrix} \succeq 0
\]

(7)

This gives us our second main result: To solve for a soft clustering \( y \) that approximately maximizes the soft margin, first solve the semidefinite program (7), and then from the solution matrix \( M^* \) recover the soft cluster assignment \( y \) by setting \( y = \sqrt{\lambda_1} v_1 \), where \( \lambda_1, v_1 \) are the maximum eigenvalue and corresponding eigenvector of \( M^* \).

4 Experimental results

We implemented the maximum margin clustering algorithm based on the semidefinite programming formulation (7), using the SeDuMi library, and tested it on various data sets.

In these experiments we compared the performance of our maximum margin clustering technique to the spectral clustering method of [14] as well as straightforward k-means clustering. Both maximum margin clustering and spectral clustering were run with the same radial basis function kernel and matching width parameters. In fact, in each case, we chose the best width parameter for spectral clustering by searching over a small set of five widths related to the scale of the problem. In addition, the slack parameter for maximum margin clustering was simply set to an arbitrary value.

To assess clustering performance we first took a set of labeled data, removed the labels, ran the clustering algorithms, labeled each of the resulting clusters with the majority class according to the original training labels, and finally measured the number of misclassifications made by each clustering.

Our first experiments were conducted on the synthetic data sets depicted in Figure 1. Table 1 shows that for the first three sets of data (Gaussians, Circles, A1) maximum margin and spectral clustering obtained identical small error rates, which were in turn significantly

---

2One could also employ randomized rounding to choose a hard class assignment \( y \).

3It turns out that the slack parameter \( C \) did not have a significant effect on any of our preliminary investigations, so we just set it to \( C = 100 \) for all of the experiments reported here.
smaller than those obtained by k-means. However, maximum margin clustering demonstrates a substantial advantage on the fourth data set (Joined Circles) over both spectral and k-means clustering.

We also conducted clustering experiments on the real data sets, two of which are depicted in Figures 2 and 3: a database of images of handwritten digits of twos and threes (Figure 2), and a database of face images of two people (Figure 3). The last two columns of Table 1 show that maximum margin clustering obtains a slight advantage on the handwritten digits data, and a significant advantage on the faces data.

5 Semi-supervised learning

Although the clustering results are reasonable, we have an additional goal of adapting the maximum margin approach to semisupervised learning. In this case, we assume we are given a labeled training set \((x^1, y^1), \ldots, (x^n, y^n)\) as well as an unlabeled training set \(x^{n+1}, \ldots, x^N\), and the goal is to combine the information in these two data sets to produce a more accurate classifier.

In the context of large margin classifiers, many techniques have been proposed for incorporating unlabeled data in an SVM, most of which are intuitively based on ensuring that large margins are also preserved on the unlabeled training data [8, 2], just as in our case. However, none of these previous proposals have formulated a convex optimization procedure that was guaranteed to directly maximize the margin, as we propose in Section 3.

For our procedure, extending the maximum margin clustering approach of Section 3 to semisupervised training is easy: We simply add constraints on the matrix \(M\) to force it to respect the observed equivalence relations among the labeled training data. In addition, we impose the constraint that each unlabeled example belongs to the same class as at least one labeled training example. These conditions can be enforced with the simple set of additional linear constraints

\[ S_1: \quad m_{ij} = y_i y_j \quad \text{for labeled examples } i, j \in \{1, \ldots, n\} \]

\[ S_2: \quad \sum_{i=1}^n m_{ij} \geq 2 - n \quad \text{for unlabeled examples } j \in \{n + 1, \ldots, N\} \]

Note that the observed training labels \(y_i\) for \(i \in \{1, \ldots, n\}\) are constants, and therefore the new constraints are still linear in the parameters of \(M\) that are being optimized.

The resulting training procedure is similar to that of [6], with the addition of the constraints \(L_1-L_4, S_2\) which enforce two classes and facilitate the ability to perform clustering on the unlabeled examples.

6 Experimental results

We tested our approach to semisupervised learning on various two class data sets from the UCI repository. We compared the performance of our technique to the semisupervised SVM technique of [8]. In each case, we evaluated the techniques transductively. That is, we split the data into a labeled and unlabeled part, held out the labels of the unlabeled portion, trained the semisupervised techniques, reclassified the unlabeled examples using the learned results, and measured the misclassification error on the held out labels.

Here we see that the maximum margin approach based on semidefinite programming can often outperform the approach of [8]. Table 2 shows that our maximum margin method is effective at exploiting unlabeled data to improve the prediction of held out labels. In every case, it significantly reduces the error of plain SVM, and obtains the best overall performance of the semisupervised learning techniques we have investigated.
Figure 1: Four artificial data sets used in the clustering experiments. Each data set consists of eighty two-dimensional points. The points and stars show the two classes discovered by maximum margin clustering.

Figure 2: A sampling of the handwritten digits (twos and threes). Each row shows a random sampling of images from a cluster discovered by maximum margin clustering. Maximum margin made very few misclassifications on this data set, as shown in Table 1.

Figure 3: A sampling of the face data (two people). Each row shows a random sampling of images from a cluster discovered by maximum margin clustering. Maximum margin made no misclassifications on this data set, as shown in Table 1.

<table>
<thead>
<tr>
<th></th>
<th>Gaussians</th>
<th>Circles</th>
<th>A I</th>
<th>Joined Circles</th>
<th>Digits</th>
<th>Faces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Margin</td>
<td>1.25</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Spectral Clustering</td>
<td>1.25</td>
<td>0</td>
<td>0</td>
<td>24</td>
<td>6</td>
<td>16.7</td>
</tr>
<tr>
<td>K-means</td>
<td>5</td>
<td>50</td>
<td>38.5</td>
<td>50</td>
<td>7</td>
<td>24.4</td>
</tr>
</tbody>
</table>

Table 1: Percentage misclassification errors of the various clustering algorithms on the various data sets.

<table>
<thead>
<tr>
<th></th>
<th>HWD 1-7</th>
<th>HWD 2-3</th>
<th>UCI Austra.</th>
<th>UCI Flare</th>
<th>UCI Vote</th>
<th>UCI Diabet.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Marg</td>
<td>3.3</td>
<td>4.7</td>
<td>32</td>
<td>34</td>
<td>14</td>
<td>35.55</td>
</tr>
<tr>
<td>Spec Clust</td>
<td>4.2</td>
<td>6.4</td>
<td>48.7</td>
<td>40.7</td>
<td>13.8</td>
<td>44.67</td>
</tr>
<tr>
<td>TSVM</td>
<td>4.6</td>
<td>5.4</td>
<td>38.7</td>
<td>33.3</td>
<td>17.5</td>
<td>35.89</td>
</tr>
<tr>
<td>SVM</td>
<td>4.5</td>
<td>10.9</td>
<td>37.5</td>
<td>37</td>
<td>20.4</td>
<td>39.44</td>
</tr>
</tbody>
</table>

Table 2: Percentage misclassification errors of the various semisupervised learning algorithms on the various data sets. SVM uses no unlabeled data. TSVM is due to [8].
7 Conclusion

We have proposed a simple, unified principle for clustering and semisupervised learning based on the maximum margin principle popularized by supervised SVMs. Interestingly, this criterion can be approximately optimized using an efficient semidefinite programming formulation. The results on both clustering and semisupervised learning are competitive with, and sometimes exceed the state of the art. Overall, margin maximization appears to be an effective way to achieve a unified approach to these different learning problems.

For future work we plan to address the restrictions of the current method, including the omission of an offset $b$ and the restriction to two class problems. We note that a multiclass extension to our approach is possible, but it is complicated by the fact that it cannot be conveniently based on the standard multiclass SVM formulation of [5].

Acknowledgements

Research supported by the Alberta Ingenuity Centre for Machine Learning, NSERC, MITACS, IRIS and the Canada Research Chairs program.

References