Supplementary Document for paper: Convex Adversarial Collective Classification

MohamadAli Torkamani
Department of Computer and Information Science
University of Oregon, Eugene, OR 97403 USA
ali@cs.uoregon.edu

Daniel Lowd
Department of Computer and Information Science
University of Oregon
Eugene, OR 97403 USA
lowd@cs.uoregon.edu

1 Proofs of Theorems

Lemma 1. *For K=2, any fixed j and $0 \leq x_{ij}, y_i^k \leq 1,\ \hat{y}_i^k \in \{0,1\}$, if $A_j^k = \sum_{i=1}^N \min(x_{ij}, y_i^k) - x_{ij}\hat{y}_i^k$, then $\sum_{k=1}^K A_j^K \geq 0$.*

Proof. $A_j^1 + A_j^2 = \sum_{i=1}^N \min(x_{ij}, y_i^1) - x_{ij}\hat{y}_i^1 + \min(x_{ij}, y_i^2) - x_{ij}\hat{y}_i^2$. Since $y_i^1 + y_i^2 = 1$ and $\hat{y}_i^1 + \hat{y}_i^2 = 1$, we can rewrite it as $\sum_{i=1}^N \min(x_{ij}, y_i^1) - x_{ij}(\hat{y}_i^1 + \hat{y}_i^2) + \min(x_{ij}, 1 - y_i^1) = \sum_{i=1}^N \min(x_{ij}, y_i^1) + \min(x_{ij}, 1 - y_i^1) - x_{ij}$. Now three cases can happen:

(a) If $x_{ij} \geq \max(y_i^1, 1 - y_i^1)$, then $\min(x_{ij}, y_i^1) + \min(x_{ij}, 1 - y_i^1) - x_{ij} = y_i^1 + 1 - y_i^1 - x_{ij} = 1 - x_{ij} \geq 0$.

(b) If $\min(y_i^1, 1 - y_i^1) \leq x_{ij} \leq \max(y_i^1, 1 - y_i^1)$, then $\min(x_{ij}, \min(y_i^1, 1 - y_i^1)) + \min(x_{ij}, \max(y_i^1, 1-y_i^1)) - x_{ij} = \min(x_{ij}, \min(y_i^1, 1-y_i^1)) + x_{ij} - x_{ij} = \min(x_{ij}, y_i^1, 1 - y_i^1) \geq 0$.

(c) If $x_{ij} \leq \min(y_i^1, 1 - y_i^1)$, then $\min(x_{ij}, y_i^1) + \min(x_{ij}, 1 - y_i^1) - x_{ij} = x_{ij} + x_{ij} - x_{ij} = x_{ij} \geq 0$.

Therefore $\min(x_{ij}, y_i^1) + \min(x_{ij}, y_i^2) - x_{ij}$ is always nonnegative and consequently $A_j^1 + A_j^2 = \sum_{i=1}^N \min(x_{ij}, y_i^1) - x_{ij}\hat{y}_i^1 + \min(x_{ij}, y_i^2) - x_{ij}\hat{y}_i^2$ is always nonnegative. □

Lemma 2. *For $K = 2$, in the optimal solution of the final quadratic program , W^* satisfies the following property: $\min(w_j^1, w_j^2) = 0\ \forall j = 1 \ldots m$.*

Proof. Let $\theta_j = \min(w_j^1, w_j^2)$, we define $u_j^1 = w_j^1 - \theta_j$ and $u_j^2 = w_j^2 - \theta_j$, by substitution the objective of the constraint's linear program will be:

$$\sum_{i,j,k}(u_j^k+\theta_j)z_{ij}^k-(u_j^k+\theta_j)x_{ij}\hat{y}_i^k+\underbrace{\sum_{(i,j)\in E,k}w_e^k y_{ij}^k-\sum_{i,k}y_i^k\cdot\hat{y}_i^k+\sum_{i,j}\delta_{ij}(1-2\hat{x}_{ij})x_{ij}}_{B}$$

$$=\sum_j\sum_i u_j^1 z_{ij}^1-u_j^1x_{ij}\hat{y}_i^1+u_j^2z_{ij}^2-u_j^2x_{ij}\hat{y}_i^2+\theta_j(z_{ij}^1-x_{ij}\hat{y}_i^1+z_{ij}^2-x_{ij}\hat{y}_i^2)+B$$

$$=\sum_j\left[\sum_i F_{ij}+\theta_j\underbrace{\sum_i H_ij}_{\geq 0}\right]+B$$

In which F_{ij} and H_{ij} are:

$$\begin{aligned}F_{ij} &= u_j^1z_{ij}^1-u_j^1x_{ij}\hat{y}_i^1+u_j^2z_{ij}^2-u_j^2x_{ij}\hat{y}_i^2\\ H_{ij} &= z_{ij}^1-x_{ij}\hat{y}_i^1+z_{ij}^2-x_{ij}\hat{y}_i^2\end{aligned}$$

According to Lemma 1, $\sum_i(z_{ij}^1-x_{ij}\hat{y}_i^1+z_{ij}^2-x_{ij}\hat{y}_i^2)\geq 0$, therefore the coefficient of each θ_j is non-negative. Since $\theta_j=\min(w_j^1,w_j^1)\geq 0$, thus:

i. If optimization algorithm chooses smaller value for θ_j, the relaxed inequality constraint will not be violated, and also smaller θ_j will not imply larger ξ.

ii. Smaller θ_j will directly reduce the objective value.

Therefore, the optimization algorithm chooses the smallest possible θ_j, which is $\theta_j=0\ \forall j$. So $\min(w_j^1,w_j^2)=0$ or equivalently $w_j^1w_j^2=0\ \forall j=1\dots m$. □

Theorem 1. *Adversary's problem in Eq. (3), has integral solution for both* $\mathbf{X}$ *and* Y.

Proof. According to Lemma 2, we know that $\min(w_j^1,w_j^2)=0$ for all j. So we can rewrite Eq. (3) as:

$$\max_{\mathbf{y}\in\mathcal{Y}',0\leq\mathbf{x}\leq 1}\sum_{i,j}D_{ij}+\sum_{(i,j)\in E,k}w_e^ky_{ij}^k-\sum_{i,k}y_i^k\cdot\hat{y}_i^k+\sum_{i,j}\delta_{ij}(1-2\hat{x}_{ij})x_{ij}\tag{1}$$

Where $D_{ij}=w_j^1z_{ij}^1-w_j^1x_{ij}\hat{y}_i^1+w_j^2z_{ij}^2-w_j^2x_{ij}\hat{y}_i^2$. Here we assume that one the w_j^1 or w_j^2 is not zero because this the interesting case otherwise the proof is trivial, therefore since either w_j^1 or w_j^2 is zero, we have:

$$\begin{aligned}D_{ij} &= w_j^1\min(x_{ij},y_i^1)-w_j^1x_{ij}\hat{y}_i^1+w_j^2\min(x_{ij},y_i^2)-w_j^2x_{ij}\hat{y}_i^2\\ &= I(w_j^1=0)\left[w_j^1\min(1-x_{ij},y_i^1)-w_j^1(1-x_{ij})\hat{y}_i^1+w_j^2\min(x_{ij},y_i^2)-w_j^2x_{ij}\hat{y}_i^2\right]+\\ &\quad I(w_j^2=0)\left[w_j^1\min(x_{ij},y_i^1)-w_j^1x_{ij}\hat{y}_i^1+w_j^2\min(1-x_{ij},y_i^2)-w_j^2(1-x_{ij})\hat{y}_i^2\right]\end{aligned}$$

Let $v_{ij}^k=x_{ij}I(w_j^k>0)+(1-x_{ij})I(w_j^k=0)$, where $I(.)$ is the indicator function, then:

$$\begin{aligned}D_{ij} &= I(w_j^1=0)\left[w_j^1\min(v_{ij}^1,y_i^1)-w_j^1v_{ij}^1\hat{y}_i^1+w_j^2\min(v_{ij}^2,y_i^2)-w_j^2v_{ij}^2\hat{y}_i^2\right]+\\ &\quad I(w_j^2=0)\left[w_j^1\min(v_{ij}^1,y_i^1)-w_j^1v_{ij}^1\hat{y}_i^1+w_j^2\min(v_{ij}^2,y_i^2)-w_j^2v_{ij}^2\hat{y}_i^2\right]\\ &= \left(I(w_j^1=0)+I(w_j^2=0)\right)\left[w_j^1\min(v_{ij}^1,y_i^1)-w_j^1v_{ij}^1\hat{y}_i^1+w_j^2\min(v_{ij}^2,y_i^2)-w_j^2v_{ij}^2\hat{y}_i^2\right]\\ &= w_j^1\min(v_{ij}^1,y_i^1)-w_j^1v_{ij}^1\hat{y}_i^1+w_j^2\min(v_{ij}^2,y_i^2)-w_j^2v_{ij}^2\hat{y}_i^2\end{aligned}\tag{2}$$

Clearly, we $v_{ij}^1 + v_{ij}^2 = 1$, because:

$$\begin{aligned} v_{ij}^1 + v_{ij}^2 &= x_{ij} I(w_j^1 > 0) + (1 - x_{ij}) I(w_j^1 = 0) + x_{ij} I(w_j^2 > 0) + (1 - x_{ij}) I(w_j^2 = 0) \\ &= x_{ij} \underbrace{\left[I(w_j^1 > 0) + I(w_j^2 > 0) \right]}_{=1} + (1 - x_{ij}) \underbrace{\left[I(w_j^1 = 0) + I(w_j^2 = 0) \right]}_{=1} \\ &= x_{ij} + 1 - x_{ij} = 1. \end{aligned}$$

Obviously, as a result we will have $z_{ij}^k = \min(v_{ij}^k, y_i^k)$, because otherwise increasing z_{ij}^k can increase the objective, so the solver program will choose the maximum possible value for z_{ij}^k. By lemma 3, and reformulation of suggested D_{ij} in Eq. (2), we conclude that Eq. (1) has integral solution for y_i^k and v_{ij}^k for all i, j and $k = 1, 2$. Since inetgrality of v_{ij}^k implies integrality of x_{ij}, proof is complete. □

Lemma 3. *If K=2, for any $W = [W^1, W^2]$, $W^k = [w_1^k, \ldots, w_m^k]^T$, linear program in Eq. (1), has an integral solution.*

Proof. Here, our argument is similar to the proof of the theorem 3.1 of [1]. We show that for any fractional solution $\mathbf{X}$ (and respectively $\mathbf{V}$) and Y of Eq. (1), we can construct a new feasible integral assignment $\mathbf{X}'$ and Y', that increases the objective or does not change it.

Since all w_e^k's and w_j^k's are positive, therefore, $y_{ij}^k = \min(y_i^k, y_j^k)$ and $z_{ij}^k = \min(y_i^k, x_{ij})$; this means that the slack variables corresponding to $z_{ij}^k \leq y_i^k$,$z_{ij}^k \leq x_{ij}$ and $y_{ij}^k \leq y_i^k$,$y_{ij}^k \leq y_j^k$ are zero, because otherwise by increasing y_{ij}^k or z_{ij}^k, the objective could be increased.

Let $\lambda^k = \min(\min_{i, y_i^k > 0} y_i^k, \min_{ij, v_{ij}^k > 0} v_{ij}^k)$ and $\lambda = \lambda^1$ or $\lambda = -\lambda^2$. We propose a new construction of solution, that either increases the objective or does not change it, and at the same time reduces the number of fractional values in the solution.

$$\begin{aligned} v_{ij}^{'1} &= v_{ij}^1 - \lambda I(0 < v_{ij}^1 < 1),\ v_{ij}^{'2} = v_{ij}^2 + \lambda I(0 < v_{ij}^2 < 1) \\ z_{ij}^{'1} &= z_{ij}^1 - \lambda I(0 < z_{ij}^1 < 1),\ z_{ij}^{'2} = z_{ij}^2 + \lambda I(0 < z_{ij}^2 < 1) \\ y_i^{'1} &= y_i^1 - \lambda I(0 < y_i^1 < 1),\ \ y_i^{'2} = y_i^2 + \lambda I(0 < y_i^2 < 1) \\ y_{ij}^{'1} &= y_{ij}^1 - \lambda I(0 < y_{ij}^1 < 1),\ y_{ij}^{'2} = y_{ij}^2 + \lambda I(< 0 y_{ij}^2 < 1) \end{aligned}$$

It is obvious that by this update, at least two of the fractional values become integral. First, we show that in this new construction, values remain feasible. So we need to show that $v_{ij}^{'1} + v_{ij}^{'2} = 1$,$y_i^{'1} + y_i^{'2} = 1$, $v_{ij}^{'k} \geq 0$, $y_i^{'k} \geq 0$, $y_{ij}^{'k} = \min(y_i^{'k}, y_j^{'k})$ and $z_{ij}^{'k} = \min(v_{ij}^{'k}, y_i^{'k})$. In the following we show that all of the feasibility requirements are satisfied.

$$v_{ij}^{'1} + v_{ij}^{'2} = v_{ij}^1 - \lambda I(0 < v_{ij}^1 < 1) + v_{ij}^2 + \lambda I(0 < v_{ij}^2 < 1 = v_{ij}^1 + v_{ij}^2 = 1.$$

$$y_i^{'1} + y_i^{'2} = y_i^1 - \lambda I(0 < y_i^1 < 1) + y_i^2 + \lambda I(0 < y_i^2 < 1) = y_i^1 + y_i^2 = 1.$$

Above we used the fact that if v_{ij}^1 is fractional then v_{ij}^2 will also be fractional, and similarly if y_i^1 is fractional then y_i^2 will also be fractional, since $v_{ij}^1 + v_{ij}^2 = 1$ and $y_i^1 + y_i^2 = 1$. To show $v_{ij}^{'k} \geq 0$ and $y_i^{'k} \geq 0$, we prove that $\min_{ij}\ v_{ij}^{'k} \geq 0$ and $\min_i\ y_i^{'k} \geq 0$.

$$\begin{aligned}
\min_{ij}\ v_{ij}^{'k} &= \min_{ij}(v_{ij}^k - (\min(\min_{i,y_i^k>0} y_i^k, \min_{ij,v_{ij}^k>0} v_{ij}^k))I(0<v_{ij}^k<1)) \\
&= \min\left(\min_{ij}\ v_{ij}^k, \min_{ij}\left[v_{ij}^k - (\min(\min_{i,y_i^k>0} y_i^k, \min_{ij,v_{ij}^k>0} v_{ij}^k))\right]\right) \\
&\geq \min\left(\min_{ij}\ v_{ij}^k, \min_{ij}\left[v_{ij}^k - (\min_{ij,v_{ij}^k>0} v_{ij}^k)\right]\right) \\
&\geq \min_{ij}\left[v_{ij}^k - (\min_{ij,v_{ij}^k>0} v_{ij}^k)\right] = 0.
\end{aligned}$$

$$\begin{aligned}
\min_{i}\ y_{i}^{'k} &= \min_{i}(y_i^k - (\min(\min_{i,y_i^k>0} y_i^k, \min_{ij,v_{ij}^k>0} v_{ij}^k))I(0<y_i^k<1)) \\
&= \min\left(\min_{i}\ y_i^k, \min_{i}\left[y_i^k - (\min(\min_{i,y_i^k>0} y_i^k, \min_{ij,v_{ij}^k>0} v_{ij}^k))\right]\right) \\
&\geq \min\left(\min_{i}\ y_i^k, \min_{i}\left[y_i^k - (\min_{i,y_i^k>0} y_i^k)\right]\right) \\
&\geq \min_{i}\left[y_i^k - (\min_{i,y_i^k>0} y_i^k)\right] = 0.
\end{aligned}$$

The last step in showing that the proposed construction is feasible is showing that $y_{ij}^{'k} = \min(y_i^{'k}, y_j^{'k})$ and $z_{ij}^{'k} = \min(v_{ij}^{'k}, y_i^{'k})$.

$$\begin{aligned}
y_{ij}^{'1} &= y_{ij}^1 - \lambda I(0<y_{ij}^1<1) \\
&= \min(y_i^1, y_j^1) - \lambda I(0<\min(y_i^1, y_j^1)<1) \\
&= \min(y_i^1 - \lambda I(0<y_i^1<1), y_j^1 - \lambda I(0<y_j^1<1)) \\
&= \min(y_i^{'1}, y_j^{'1}).
\end{aligned}$$

$$\begin{aligned}
y_{ij}^{'2} &= y_{ij}^2 + \lambda I(0<y_{ij}^2<1) \\
&= \min(y_i^2, y_j^2) + \lambda I(0<\min(y_i^2, y_j^2)<1) \\
&= \min(y_i^2 + \lambda I(0<y_i^2<1), y_j^2 + \lambda I(0<y_j^2<1)) \\
&= \min(y_i^{'2}, y_j^{'2}).
\end{aligned}$$

$$\begin{aligned}
z_{ij}^{'1} &= z_{ij}^1 - \lambda I(0<z_{ij}^1<1) \\
&= \min(v_{ij}^1, y_i^1) - \lambda I(0<\min(v_{ij}^1, y_i^1)<1) \\
&= \min(v_{ij}^1 - \lambda I(0<v_{ij}^1<1), y_i^1 - \lambda I(0<y_i^1<1)) \\
&= \min(v_{ij}^{'1}, y_i^{'1}).
\end{aligned}$$

$$\begin{aligned}
z_{ij}^{'2} &= z_{ij}^2 + \lambda I(0<z_{ij}^2<1) \\
&= \min(v_{ij}^2, y_i^2) + \lambda I(0<\min(v_{ij}^2, y_i^2)<1) \\
&= \min(v_{ij}^2 + \lambda I(0<v_{ij}^2<1), y_i^2 + \lambda I(0<y_i^2<1)) \\
&= \min(v_{ij}^{'2}, y_i^{'2}).
\end{aligned}$$

So far we have shown that the new variable construction is feasible, and it remains to show that we can increase the objective. We substitute the newly constructed feasible values in Eq. (1) and subtract the objective with unchanged values from it. Then we show that with proper choice of $\lambda = \lambda^1$ or of $\lambda = -\lambda^2$, we can improve the objective.

$$
\begin{aligned}
V_{old} &= \sum_{i,j} D_{ij} + \sum_{(i,j)\in E,k} w_e^k y_{ij}^k - \sum_{i,k} y_i^k \cdot \hat{y}_i^k + \sum_{i,j} \delta_{ij}(1-2\hat{x}_{ij})x_{ij} \\
&= \sum_{i,j} w_j^1 z_{ij}^1 - w_j^1 v_{ij}^1 \hat{y}_i^1 + w_j^2 z_{ij}^2 - w_j^2 v_{ij}^2 \hat{y}_i^2 \\
&\quad + \sum_{(i,j)\in E,k} w_e^k y_{ij}^k - \sum_{i,k} y_i^k \cdot \hat{y}_i^k + \sum_{i,j} \delta_{ij}(1-2\hat{x}_{ij})x_{ij} \\
&= \sum_{i,j} w_j^1 z_{ij}^1 - w_j^1 v_{ij}^1 \hat{y}_i^1 + w_j^2 z_{ij}^2 - w_j^2 v_{ij}^2 \hat{y}_i^2 \\
&\quad + \sum_{(i,j)\in E,k} w_e^k y_{ij}^k - \sum_{i,k} y_i^k \cdot \hat{y}_i^k \\
&\quad + \sum_{i,j} \delta_{ij}(1-2\hat{x}_{ij}) \left[\left(I(w_j^1 > 0) - I(w_j^1 = 0) \right) v_{ij}^1 + I(w_j^1 = 0) \right] \\
&= \sum_{i,j} w_j^1 z_{ij}^1 - w_j^1 v_{ij}^1 \hat{y}_i^1 + w_j^2 z_{ij}^2 - w_j^2 v_{ij}^2 \hat{y}_i^2 \\
&\quad + \sum_{(i,j)\in E,k} w_e^k y_{ij}^k - \sum_{i,k} y_i^k \cdot \hat{y}_i^k \\
&\quad + \sum_{i,j} \left[\delta_{ij}(1-2\hat{x}_{ij}) \left(I(w_j^1 > 0) - I(w_j^1 = 0) \right) \right] v_{ij}^1 + C.
\end{aligned}
$$

Above we have used the fact that $x_{ij} = I(w_j^{'k} > 0)v_{ij}^{'k} + I(w_j^{'k} = 0)(1 - v_{ij}^{'k}) = I(w_j^{'1} > 0)v_{ij}^{'1} + I(w_j^{'1} = 0)(1 - v_{ij}^{'1}) = \left(I(w_j^{'1} > 0) - I(w_j^{'1} = 0) \right) v_{ij}^{'1} + I(w_j^{'1} = 0)$.

$$
\begin{aligned}
V_{new} &= \sum_{i,j} w_j^1 z_{ij}^{'1} - w_j^1 v_{ij}^{'1} \hat{y}_i^1 + w_j^2 z_{ij}^{'2} - w_j^2 v_{ij}^{'2} \hat{y}_i^2 \\
&\quad + \sum_{(i,j)\in E,k} w_e^k y_{ij}^{'k} - \sum_{i,k} y_i^{'k} \cdot \hat{y}_i^k \\
&\quad + \sum_{i,j} \left[\delta_{ij}(1-2\hat{x}_{ij})\left(I(w_j^1>0) - I(w_j^1=0)\right)\right] v_{ij}^{'1} + C \\
&= \sum_{i,j} [w_j^1(z_{ij}^1 - \lambda I(0<z_{ij}^1<1)) - w_j^1 \hat{y}_i^1 (v_{ij}^1 - \lambda I(0<v_{ij}^1<1)) \\
&\quad + w_j^2(z_{ij}^2 + \lambda I(0<z_{ij}^2<1)) - w_j^2 \hat{y}_i^2 (v_{ij}^2 + \lambda I(0<v_{ij}^2<1))] \\
&\quad + \sum_{(i,j)\in E} \left[w_e^1(y_{ij}^1 - \lambda I(0<y_{ij}^1<1)) + w_e^2(y_{ij}^2 + \lambda I(0<y_{ij}^2<1))\right] \\
&\quad - \sum_i \hat{y}_i^1 \cdot (y_i^1 - \lambda I(0<y_i^1<1)) + \hat{y}_i^2 \cdot (y_i^2 + \lambda I(0<y_i^2<1)) \\
&\quad + \sum_{i,j} \left[\delta_{ij}(1-2\hat{x}_{ij})\left(I(w_j^1>0) - I(w_j^1=0)\right)\right](v_{ij}^1 - \lambda I(0<v_{ij}^1<1)) + C \\
&= V_{old} + \sum_{i,j} [w_j^1(-\lambda I(0<z_{ij}^1<1)) - w_j^1 \hat{y}_i^1 (-\lambda I(0<v_{ij}^1<1)) \\
&\quad + w_j^2(\lambda I(0<z_{ij}^2<1)) - w_j^2 \hat{y}_i^2 (\lambda I(0<v_{ij}^2<1))] \\
&\quad + \sum_{(i,j)\in E} \left[w_e^1(-\lambda I(0<y_{ij}^1<1)) + w_e^2(\lambda I(0<y_{ij}^2<1))\right] \\
&\quad - \sum_i \hat{y}_i^1 \cdot (-\lambda I(0<y_i^1<1)) + \hat{y}_i^2 \cdot (+\lambda I(0<y_i^2<1)) \\
&\quad + \sum_{i,j} \left[\delta_{ij}(1-2\hat{x}_{ij})\left(I(w_j^1>0) - I(w_j^1=0)\right)\right](-\lambda I(0<v_{ij}^1<1)).
\end{aligned}
$$

Therefore, we can write $V_{new} - V_{old}$ as:

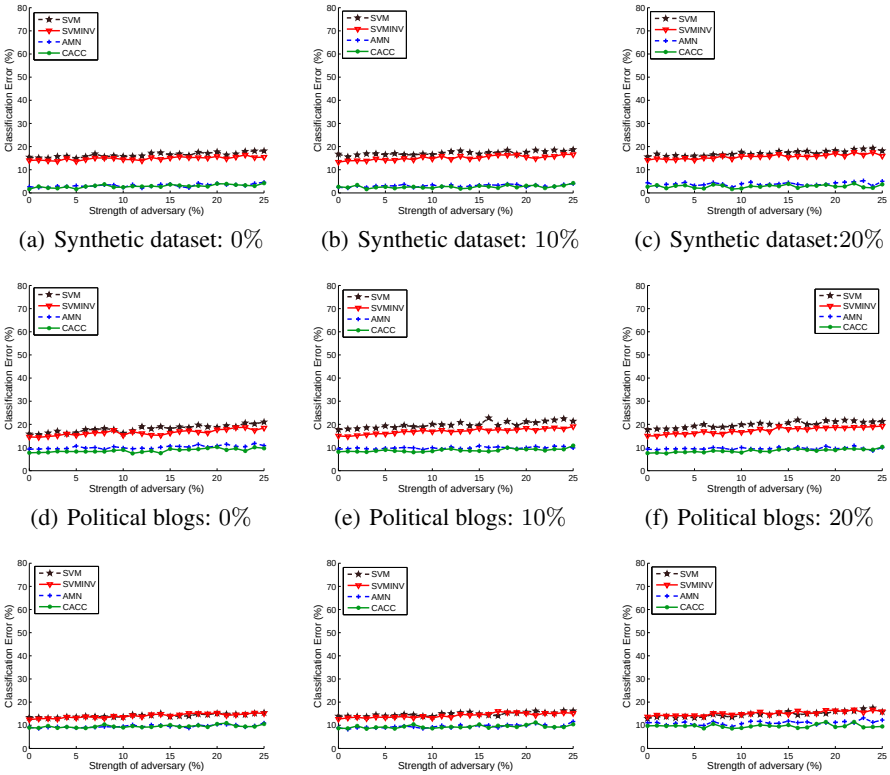
$$
\begin{aligned}
V_{new} - V_{old} &= \lambda[\sum_{i,j} [-w_j^1 I(0<z_{ij}^1<1) + w_j^1 \hat{y}_i^1 I(0<v_{ij}^1<1) \\
&\quad + w_j^2 I(0<z_{ij}^2<1) - w_j^2 \hat{y}_i^2 I(0<v_{ij}^2<1)] \\
&\quad + \sum_{(i,j)\in E} \left[-w_e^1 I(0<y_{ij}^1<1) + w_e^2 I(0<y_{ij}^2<1)\right] \\
&\quad - \sum_i \hat{y}_i^1 \cdot (-I(0<y_i^1<1)) + \hat{y}_i^2 \cdot (+I(0<y_i^2<1)) \\
&\quad + \sum_{i,j} -\delta_{ij}(1-2\hat{x}_{ij})\left(I(w_j^1>0) - I(w_j^1=0)\right) I(0<v_{ij}^1<1)] \\
&= \lambda D.
\end{aligned}
$$

The change in objective is λD, and since D is constant with respect to λ, by choosing $\lambda = -\lambda^2$ for negative D, or $\lambda = \lambda^1$ for positive D, we can always have positive or zero λD.It means that the integral solution will increase the objective or will not change it, while leaving fewer fractional values.

□

2 Random attack results

This section contains the results of the experiments where instead of a worst-case adversary, some naive adversary has randomly changed the features. All other settings are as in the paper.



(a) Synthetic dataset: 0% (b) Synthetic dataset: 10% (c) Synthetic dataset:20%

(d) Political blogs: 0% (e) Political blogs: 10% (f) Political blogs: 20%

(g) Reuters: 0% (h) Reuters: 10% (i) Reuters: 20%

Figure 1

References

[1] B. Taskar, V. Chatalbashev, and D. Koller, "Learning associative Markov networks," in *Proceedings of the twenty-first international conference on machine learning*, ACM Press, 2004.