Harvard CS 182: Artificial Intelligence	October 20, 2022

Section 7: Stackelberg Security Games and Social Choice Solutions

Lecturer: Ariel Procaccia *Authors: Lauren Cooke and Sanjana Singh*

Stackelberg Security Games

Problem 1 *Consider the following game:*

$(3,1)$	$(5,0)$
$(2,0)$	$(4,2)$

Table 1: Problem 1 Game

Find the nash equilibrium for this game and find the strategy that the leader can play to maximize their utility in a stackelberg game where the row player is the leader.

1. We first find the nash equilibrium for this game. For our row player, we see that the top row is a dominant strategy, meaning that regardless of what the column player will do, the row player will always be betterr off by choosing the top row. Given this information, our column player can maximize his utility by choosing the column who's top row value is greater. $1 > 0$, meaning that the column player will choose the left column. Therefore, our nash equilibrium exists at $(3,1)$.

Now, we want to find the strategy that the leader can play to maximize their utility in a stackelberg game. Looking at our game space, we know that we can maximize the payoff for the leader if we can convince the column player to play the right column as often as possible while still allowing the (5,0) option to be a possibility. If the leader plays the strategy $\left(\frac{2}{3}, \frac{1}{3}\right)$, our column player will respond by choosing the right column every time because we break ties in favor of the leader, as the expected payoff for the follower will be $1 * \frac{2}{3}$ for the left column and $2 * \frac{1}{3}$ for the right column. Given this setup, the leader will earn a utility of 5 $\frac{2}{3}$ of the time and a utility of 4 $\frac{1}{3}$ of the time, giving the leader an expected utility of $\frac{10}{3} + \frac{4}{3} = 4.67$. Therefore, the leader can maximize their utility in a stackelberg game with strategy $\left(\frac{2}{3}, \frac{1}{3}\right)$.

Social Choice

Problem 2 *Americans typically revile third-party presidential candidates like Ralph Nader as "spoilers," candidates that distort an election, but many countries have (reasonably) well-functioning governments with multiple parties. Concept check: Why does America's "winner-take-all" majority voting rule function poorly for three, but well for two, parties?*

2. A winner-take-all policy uses the plurality voting rule. With two parties, the winner is preferred by the majority of voters. However with three parties, the winner A may be preferred by 34 percent of voters by the bottom choice for the remaining voters, who split their vote 33 percent and 33 percent between very similar candidates B and C.

Problem 3 *The year is 2019, and you and your housemates are having some friends over for a party. You're tasked with planning food. To ensure that your guests are as happy as can be, you send out a survey asking them to rank their favorite cheeses: gouda, brie, or edam. Their results come in, and the responses are:*

- *4 votes: 1. edam 2. gouda 3. brie*
- *3 votes: 1. brie 2. gouda 3. edam*
- *2 votes: 1. gouda 2. brie 3. edam*

Unfortunately, there is no clear winner and you can only select one cheese. To be the best possible host, how should you decide?

Fortunately, you've just had a lecture on computational social choice, so you decide to put some voting rules into practice. What would your decision be if you used each of the following voting rules?

Plurality, Borda, STV, Plurality with runoff.

How do the pairwise elections between the following alternatives turn out?

- *Edam vs. Brie*
- *Edam vs. Gouda*
- *Gouda vs. Brie*

Looking at these pairwise results, are any alternatives a Condorcet winner?

What is the Dodgson score of each alternative?

3.

What would your decision be if you used each of the following voting rules?

Plurality:

Edam is favored by 4 voters, versus 3 for brie and 2 for gouda. So you'd choose edam.

Borda:

Edam: $2 \times 4 = 8$. Brie: $3 \times 2 + 2 \times 1 = 8$. Gouda: $4 \times 1 + 3 \times 1 + 2 \times 2 = 11$. So you'd choose gouda.

STV:

We first eliminate gouda. Then brie is preferred by $3 + 2 = 5$ voters vs. 4 for edam, so you'd choose brie.

Plurality with runoff:

Same as STV when we have 3 alternatives.

How do the pairwise elections between the following alternatives turn out?

Edam vs. brie: Edam wins 4; brie wins 5

Edam vs. gouda: Edam wins 4; gouda wins 5

Gouda vs. brie: Gouda wins 6; brie wins 3

Looking at these pairwise results, are any alternatives a Condorcet winner?

Gouda wins pairwise majority comparisons against both competitors edam and brie, thus is the Condorcet winner.

What is the Dodgson score of each alternative?

Gouda, as the Condorcet winner, has distance 0 to become so. Brie could become the Condorcet winner by having both voters of the third column change their ranking, thus has distance 2. Edam could become the Condorcet winner by convincing one voter in the second column to prefer it over gouda, and also one voter in the third column to prefer it over brie. So it has Dodgson score of 2.

Problem 4 *Consider the STV voting rule. Suppose that Arrow Academy, a high school with very democratic-minded students, is holding an election for class president. Suppose the students running comprise the set of alternatives is $A = \{$Frances Allen, Daniel Bernoulli, Mary Cartwright$\}$ and we have the preference profile:*

- *27 votes: 1. Allen 2. Bernoulli 3. Cartwright*
- *42 votes: 1. Cartwright 2. Allen 3. Bernoulli*
- *24 votes: 1. Bernoulli 2. Cartwright 3. Allen*

a) Cartwright puts forth a very rousing campaign to extend the lunch period by 10 minutes, and four votes switch from [Allen $\succ$ Bernoulli $\succ$ Cartwright] to [Cartwright $\succ$ Allen $\succ$ Bernoulli]. How does this change the result?

b) What would happen if, in a parallel world, Cartwright instead enacted a voter suppression campaign, causing four voters with preference [Allen Bernoulli Cartwright] to not vote?

4. The original winner, before Cartwright's campaign, would have been: Cartwright. The first round would eliminate Bernoulli, and then Cartwright would become the winner with $42+24 = 66$ top votes compared to Allen's 27. However, after the campaign when four voters switch their preferences up, we now have 23, 46, 24 voters with each preference ranking. The first round now eliminates Allen, so Bernoulli bumps up among the first group. Now, Bernoulli wins with a small margin, earning $23 + 24 = 47$ votes above Cartwright's 46.

We would have 23, 42, 24. First round would eliminate Allen, bringing up Bernoulli. Now, we have Bernoulli earning $23 + 24 = 47$ votes to Cartwright's 42, making Bernoulli the winner. Cartwright's efforts again block her position.