Privacy in Statistics and Machine Learning — Spring 2021
Lecture 17 & 18: Equilibrium in Zero-Sum Games

Adam Smith and Jonathan Ullman

As promised in Lecture 15, we're going to see how many algorithms from query release fit into a larger framework based on computing equilibrium in two-player zero-sum games. To start we'll focus on the mathematical background before we get back to query-release.

1 Two-Player Zero-Sum Games and the Minmax Theorem

You've all likely played a two-player zero-sum game before: *Rock, Paper, Scissors*. In case you aren't familiar, two players each get to choose an action from the set { rock, paper, scissors } and the game is decided according to the rules rock-beats-scissors, scissors-beats-paper, paper-beats-rock, and the game is a tie if the players each use the same action. What makes this game *zero-sum* is that one player's loss is the other player's gain, and vice versa. Either the two players tie. Exactly one player wins and the other loses.

In this lecture we'll study the key concept of *equilibrium* in two-player zero-sum games, and then discuss applications to query release. Mathematically, we can model a two-player, zero-sum game using the following notation:

- There are two *players*, which we will name Rowena and Colin.
- Rowena has a set of *actions* $\mathcal{R}$ and Colin has a set of actions C.
- There is a *payoff matrix* $M \in \mathbb{R}^{|\mathcal{R}| \times |C|}$ where $M_{i,j}$ represents the *reward* that Rowena gets from Colin if she plays action $i \in \mathcal{R}$ and Colin plays action $j \in C$. Thus, $-M_{i,j}$ is the reward for Colin given the same pair of actions.

What makes the game zero-sum is that Rowena "wins" $M_{i,j}$ and Colin "wins" $-M_{i,j}$, so the amount the two players win is always $M_{i,j} - M_{i,j} = 0$. Thus, the two players' goals are directly opposed, Rowena wants to maximize her reward and Colin wants to minimize her reward.

In this model, we can represent Rock, Paper, Scissors as a game where $\mathcal{R} = C = \{1, 2, 3\}$ with $\{1, 2, 3\}$ representing rock, paper, and scissors, respectively. The payoff matrix is

$$\begin{bmatrix} 0 & -1 & +1 \\ +1 & 0 & -1 \\ -1 & +1 & 0 \end{bmatrix} \tag{1}$$

where we assume that Rowena gets 1 from Colin if she wins the game and vice versa, and both players get 0 in the event of a tie.

Even if you're intuitively familiar with rock, paper, scissors, we'll see the tools needed to understand strategic behavior in games where the solution is less obvious, such as the simple game described by a payoff matrix like this one.

$$\begin{bmatrix} +2 & -1 \\ -2 & +3 \end{bmatrix} \tag{2}$$

1.1 Who Goes First?

If you've played Rock, Paper, Scissors recently, you probably remember that both players typically play *simultaneously*, and the game gets pretty uninteresting if one player has to pick an action first. In general, suppose I require that Rowena goes first and let's think about how she would choose her action. Whatever action $i \in \mathcal{R}$ she takes, Colin will play the action $j \in C$ that maximizes his rewards, or equivalently that minimizes Rowena's reward. Thus, if Rowena plays i, then Colin will choose the action $\arg\min_j M_{i,j}$ and Rowena will get $\min_j M_{i,j}$. This is known as a *best response* for Colin. Thus, Rowena should play i to maximize the amount she will get, knowing how Colin will respond to her action. In particular, she should play $\arg\max_i \min_j M_{i,j}$ and her reward will be $\max_i \min_j M_{i,j}$. For Rock, Paper, Scissors we all know that whatever Rowena plays, Colin has a way to win the game, so Rowena will always lose if she has to go first. In other words,

$$\max_i \min_j M_{i,j} = -1 \tag{3}$$

Now, what if Colin goes first? By a completely symmetric argument, we know that whatever action j that Colin plays, Rowena will chose the action i to maximize her reward, thus Colin should play to minimize Rowena's reward knowing how she will respond. Thus, Rowena's reward when Colin plays first is going to be $\min_j \max_i M_{i,j}$. For Rock, Paper, Scissors, if Colin goes first, then Rowena will always win, or, in other words,

$$\min_j \max_i M_{i,j} = 1 \tag{4}$$

One simple fact is that for any two-player zero-sum game, you would prefer to be the player who chooses their action second rather than the player who chooses their action first. In our notation, this comes out as the following inequality.

$$\max_i \min_j M_{i,j} \leq \min_j \max_i M_{i,j} \tag{5}$$

Exercise 1.1. Prove (5).

1.2 Randomized Strategies

As we've seen, the game Rock, Paper, Scissors is pretty boring if require one of the players to go first. What if we add *randomization* to the mix? That is, suppose Rowena still has to act first, but now Rowena doesn't have to pick a specific action i. Instead, she has to pick a *probability distribution* $\mathbf{r}$ over actions, which we can represent as a column vector $\mathbf{r} \in \Delta(\mathcal{R})$. Given this probability distribution over actions, Colin will then get to choose a probability distribution $\mathbf{c}$ over actions, represented as a column vector $\mathbf{c} \in \Delta(C)$. We will sometimes call these distributions *(randomized) strategies*. One these two strategies are chosen, the players sit back and watch while an action i is chosen according to $\mathbf{r}$ and an action j is chosen *independently* according to $\mathbf{c}$ and Rowena wins $M_{i,j}$.

Given a pair of strategies $\mathbf{r}, \mathbf{c}$, the expected payoff to Rowena is

$$\mathop{\mathbb{E}}_{\substack{i\sim\mathbf{r}\\ j\sim\mathbf{c}}} \left(M_{i,j}\right) = \sum_{\substack{i\in\mathcal{R}\\ j\in C}} \mathbf{r}_i \mathbf{c}_j M_{i,j} = \mathbf{r}^\top M \mathbf{c} \tag{6}$$

where we will often use the matrix expression as a compact way of representing the expected payoff for the pair of strategies (but won't need any fancy linear algebra).

Using the same logic as before, if Rowena has to choose her strategy first, then she will choose $\mathbf{r}$ to maximize her expected reward knowing that Colin will play a best-response, and she will get a payoff of

$$\max_{\mathbf{r}} \min_{\mathbf{c}} \mathbf{r}^\top M \mathbf{c} \tag{7}$$

and similarly if Colin has to choose her strategy first, then he will choose $\mathbf{c}$ to minimize Rowena's expected reward, knowing that she will play a best-response, and then Rowena will get a payoff of

$$\min_{\mathbf{c}} \max_{\mathbf{r}} \mathbf{r}^\top M \mathbf{c} \tag{8}$$

Let's see what will happen in Rock, Paper, Scissors when Rowena goes first and chooses some distribution $\mathbf{r}$. Remember that $\mathbf{r}_1$ is the probability of playing rock, $\mathbf{r}_2$ is the probability of paper, and $\mathbf{r}_3$ is the probability of scissors. You all probably intuitively see that the best thing for Rowena to do is to play the uniform distribution $\mathbf{r} = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$. In this case, no matter what strategy Colin plays, Rowena's expected reward is 0. Thus, for this game,

$$\max_{\mathbf{r}} \min_{\mathbf{c}} \mathbf{r}^\top M \mathbf{c} \geq 0 \tag{9}$$

It's also not too hard to check that if Rowena plays any strategy other than the uniform distribution, Colin has a response that makes Rowena's expected reward strictly negative. Thus we have

$$\max_{\mathbf{r}} \min_{\mathbf{c}} \mathbf{r}^\top M \mathbf{c} = 0 \tag{10}$$

Exercise 1.2. Prove that if Rowena plays any strategy other than $\mathbf{r} = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ then Colin has a strategy $\mathbf{c}$ such that $\mathbf{r}^\top M \mathbf{c} < 0$.

What happens if Colin plays first? By symmetry of the game, Colin also must play the uniform distribution $\mathbf{c}$ or else Rowena will receive a strictly positive reward. Thus

$$\min_{\mathbf{c}} \max_{\mathbf{r}} \mathbf{r}^\top M \mathbf{c} = 0 \tag{11}$$

So, at least for Rock, Paper, Scissors, as long as the players get to choose randomized strategies, it doens't matter who has to pick their strategy first! It turns out that this isn't specific to Rock, Paper, Scissors, and is actually true for *any* two-player, zero-sum game. This fact is what's known as the celebrated *minmax theorem*, due to John von Neumann.

Theorem 1.3 (Minmax Theorem [Neu28])**.** *For any two-player zero-sum game with payoff matrix M,*

$$\max_{\mathbf{r}} \min_{\mathbf{c}} \mathbf{r}^\top M \mathbf{c} = \min_{\mathbf{c}} \max_{\mathbf{r}} \mathbf{r}^\top M \mathbf{c} = \mathrm{val}(M) \tag{12}$$

where the quantity $\mathrm{val}(M)$ *is called the* value *of the game.*

In particular, a pair of strategies $(\mathbf{r}, \mathbf{c})$ such that $\mathbf{r}^\top M \mathbf{c} = \mathrm{val}(M)$ are called an *equilibrium* of the game in the sense that neither player can improve their payoff by changing their strategy. A strategy $\mathbf{r}$ such that $\min_{\mathbf{c}} \mathbf{r}^\top M \mathbf{c} = \mathrm{val}(M)$ is sometimes called a *minmax strategy* and, unsurprisingly, a strategy $\mathbf{c}$ such that $\max_{\mathbf{r}} \mathbf{r}^\top M \mathbf{c}$ is sometimes called a *maxmin strategy*.

The relatively easy part of the minmax theorem is showing that Rowena does *at least* as well if she chooses her strategy second as she does if she chooses it first.

Exercise 1.4. Prove the "easy" direction of the minmax theorem,

$$\max_{\mathbf{r}} \min_{\mathbf{c}} \mathbf{r}^\top M \mathbf{c} \leq \min_{\mathbf{c}} \max_{\mathbf{r}} \mathbf{r}^\top M \mathbf{c} \tag{13}$$

In the next lecture we'll prove the much harder part of the minimax theorem, which says that Rowena can do just as well if she goes first. While there are lots of ways to prove this theorem, we will show a cool proof that deduces the minimax theorem as a consequence of the existence of no-regret online learning algorithms! In addition to being very simple (now that we've done all the hard work of proving that no-regret learning is possible), this proof will also give us some nice, computationally efficient algorithms for computing $\text{val}(M)$ and finding equilibrium strategies.

Exercise 1.5. Suppose players take turns playing a best response to one another's strategy (which is sometimes called *best-response dynamics*). Rowena chooses some action r_1, then Colin best-responds with $c_1 = \arg\min_c r_1^\top M c$, then Rowena best-responds with $r_2 = \arg\max_r r^\top M c_1$, and so on. Specifically,

$$c_t = \arg\min_c r_t^\top M c \text{ and } r_t = \arg\max_r r^\top M c_{t-1}$$

What will happen in this process as $t \to \infty$? Will r_t, c_t converge to an equilibrium of the game?

Additional Reading and Watching

- ...

References

[Neu28] J v Neumann. Zur theorie der gesellschaftsspiele. *Mathematische annalen*, 100(1):295–320, 1928.