EE 382V: Social Computing **Fall 2018**

Homework 4: November 30

Partner1: Javier Palomares *Partner2: Porter Perry*

1.1 Question1

[Textbook Ch.23 Question 1]
In this chapter, we discussed how voting systems based on majority rule are susceptible to strategic agenda-setting. Lets explore how one might do this on some basic examples.

(a) Suppose there are four alternatives, named A, B, C, and D. There are three voters who have the following individual rankings:

$B >_1 C >_1 D >_1 A$
$C >_2 D >_2 A >_2 B$
$D >_3 A >_3 B >_3 C$

You're in charge of designing an agenda for considering the alternatives in pairs and eliminating them using majority vote, via an elimination tournament in the style of the examples shown in Figure 23.3.
You would like alternative A to win. Can you design an agenda (i.e. an elimination tournament) in which A wins? If so, describe how you would structure it; if not, explain why it is not possible.

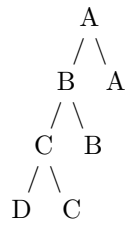
(b) Now, consider the same question, but for a slightly different set of individual rankings in which the last two positions in voter 3's ranking have been swapped. That is, we have:

$B >_1 C >_1 D >_1 A$
$C >_2 D >_2 A >_2 B$
$D >_3 A >_3 C >_3 B$

We now ask the same question: Can you design an agenda in which A wins? If so, describe how you would structure it; if not, explain why it is not possible.

1.1.1 Answer1

(a) Yes. Alternative A would only win by majority rule over alternative B. Alternative B can only win by majority rule over alternative C. Alternative C will win by majority rule over both alternatives A and D. So, structure the elimination tournament by method of introducing new alternatives one at a time. At the first step, have alternative C go against D. The winner of the first step, alternative C, would then go against B. The winner of the second step, which would be alternative B, would then finally go against alternative A. The final winner of alternatives A vs B would be A.



(b) No, it is not possible for alternative A to win an voting elimination tournament by majority rule. Again, alternative A would only win by majority rule over alternative B. However, alternative B will not win by majority rule over any other alternative, so it is not possible to for alternative B to advance to the final step where alternative A could beat it and win the overall tournament.

1.2 Question2

[Textbook Ch.23 Question 2]
The Borda Count is susceptible to strategic misreporting of preferences. Here are some examples to practice how this works.

(a) Suppose you are one of three people voting on a set of four alternatives named A, B, C, and D. The Borda Count will be used as the voting system. The other two voters have the rankings

$D >_1 C >_1 A >_1 B$
$D >_2 B >_2 A >_2 C$

You are voter 3 and would like alternative A to appear first in the group ranking, as determined by the Borda Count. Can you construct an individual ranking for yourself so that this will be the result? If so, explain how you would choose your individual ranking; if not, explain why it is not possible.

(b) Lets consider the same question, but with different rankings for the other two voters, as follows:

$D >_1 A >_1 C >_1 B$
$B >_2 D >_2 A >_2 C$

Again, as voter 3, you would like alternative A to appear first in the group ranking determined by the Borda Count. Can you construct an individual ranking for yourself so that this will be the result? If so, explain how you would choose your individual ranking; if not, explain why it is not possible.

1.2.1 Answer2

(a) No. Using the Borda count system, alternative D already has 6 points from the first two voters, while alternative A has only two. The gap between the two cannot be closed with one additional vote, which would could give alternative A at most 5 points.

(b) Yes. Based on the first two votes, the alternative would have the following Borda count totals:

$A = 3$
$B = 3$
$C = 1$
$D = 5$

A vote with alternative A ranked first, and D ranked last would would cause A to overtake D with a count of 6 to 5. Alternatives B and C would be second and third rank, and it does not matter which. So the possible ranks would be:

$A >_3 C >_3 B >_3 D$
-or-
$A >_3 B >_3 C >_3 D$

1.3 Question3

Compute 5^{97} mod 11.

1.3.1 Answer3

$5^1 \bmod 11 = 5$
$5^2 \bmod 11 = (5 \times 5) \bmod 11) = 25 \bmod 11 = 3$
$5^4 \bmod 11 = (3 \times 3) \bmod 11) = 9 \bmod 11 = 9$
$5^8 \bmod 11 = (9 \times 9) \bmod 11) = 81 \bmod 11 = 4$
$5^{16} \bmod 11 = (4 \times 4) \bmod 11) = 16 \bmod 11 = 5$
$5^{32} \bmod 11 = (5 \times 5) \bmod 11) = 25 \bmod 11 = 3$
$5^{64} \bmod 11 = (3 \times 3) \bmod 11) = 9 \bmod 11 = 9$

$$\begin{aligned} 5^{97} \bmod 11 &= (5^{64} \times 5^{32} \times 5^1) \bmod 11 \\ &= ((5^{64} \bmod 11) \times (5^{32} \bmod 11) \times (5^1 \bmod 11)) \bmod 11 \\ &= (9 \times 3 \times 5) \bmod 11 \\ &= 135 \bmod 11 \\ &= 3 \end{aligned}$$

1.4 Question4

Let two primes p and q for the RSA scheme be 11 and 13. Suppose that you want the public key e of your encryption scheme to be 7. What would be the private key d for this setting? What would be the ciphertext corresponding to the number 71?

1.4.1 Answer4

RSA key pair algorithm for $p = 11$ and $q = 13$:

1. Let $n = pq = 11 \times 13 = 143$.
2. Compute Euler's totient function for n:
   $\phi(143) = (11 - 1) \times (13 - 1) = 120$
3. Choose $e = 7$ as number relatively prime to 143.
4. Find d such that $d \times e \equiv 1 \bmod \phi(n)$:
   $d = 103$ works since $(7 \times 103) \bmod 120 = 721 \bmod 120 = 1$

$71^1 \bmod 143 = 71$
$71^2 \bmod 143 = 5041 \bmod 143 = 36$
$71^4 \bmod 143 = 36 \times 36 \bmod 143 = 9$

The ciphertext corresponding to message number 71 would be:

$$\begin{aligned} C &= M^e \bmod n \\ &= 71^7 \bmod 143 \\ &= (71^4 \times 71^2 \times 71^2) \bmod 143 \\ &= (9 \times 36 \times 71) \bmod 143 \\ &= (23004) \bmod 143 \\ &= 124 \end{aligned}$$