

# Mathematics for Computer Science: Homework 8

Instructed by *Andrew C. Yao & Wang Yuexuan*

Due on April 29, 2010

**Zhang Kunwei** J92 2009011269

## Special Problem 1

Let  $n > k > 0$ . In class it was shown that the Byzantine Generals Problem has a solution for  $k = 1$ ,  $n = 4$ . Now, prove that the Byzantine Generals Problem has a solution for  $k = 2$ ,  $n = 7$ .

### Answer:

Here's an algorithm for  $n$  people and  $k$  traitors when  $m = k$ .

```
func OM(n,m,C[1],C[],message) return A[]
  for i in [2,n]
    T[i]=C[i] ask message from C[1]
  if n=0 return with A=T
  for i in [2,n]
    Tx[i]=OM(n-1,m-1,C[i],C-C[i],T[i])
  for i in [2,n]
    A[i]=majority(Tx[2..n][i])
    // if equal, majority should return retreat.
```

**Lemma.1** This algorithm works when  $n > 2k + m$  and the commander is loyal.

**Proof** Induction on  $m$ . First of all, OM(0) works.  $n > 2k+m$  leads to  $(n-1) > 2k+(m-1)$ , so with OM( $n-1$ ) working, a loyal general will give correct message to others.  $k \leq -k + 2k + (m-1) < -k + n - 1$ , majority will be the message from the loyal. Thus each general get the correct answer.

Now let  $m = k$ , and consider the case when the commander is a traitor. Induction on  $k$ . Given OM( $k-1$ ) returns the same value, i.e.  $Tx[i]=Tx[j]$  for any loyal  $C[i],C[j]$ , we have  $A[i] = \text{majority}(Tx[2..n][i]) = \text{majority}(Tx[2..n][j]) = A[j]$ . Thus OM( $k$ ) returns the same value.

## Special Problem 2

Let  $G = (V, E)$  where  $V = \{0, 1, 2, 3, 4\}$  and  $E$  is the set of edges  $\{0, 1\}, \{0, 2\}, \{0, 3\}, \{1, 2\}, \{2, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\}$ . Give a solution for the  $(G, 5, 1)$ -Byzantine Generals Problem. Give a rigorous proof that your algorithm achieves the Byzantine Generals requirements.

### Answer:

**Algorithm** Add a virtual channel  $\{1,3\}$ , meaning  $1 \rightarrow 4 \rightarrow 3$  or  $3 \rightarrow 4 \rightarrow 1$ . Use BGP(4,1) to sync  $\{0,1,2,3\}$  (with the virtual channel added). Then,  $\{1,2,3\}$  tell 4 the answer, in which the majority is used for 4's output.

**Proof** If 4 is loyal, BGP(4,1) will succeed. Because at least two in  $\{1,2,3\}$  is loyal, 4 will get the same answer with loyal guys, too. If 4 is a traitor,  $\{0,1,2,3\}$  are all loyal.  $0 \rightarrow 1$  and  $0 \rightarrow 2 \rightarrow 1$  lead 1 to the correct answer.  $0 \rightarrow 2$  and  $0 \rightarrow 1 \rightarrow 2$  for 2.  $0 \rightarrow 3$  and  $0 \rightarrow 2 \rightarrow 3$  for 3.

**Acknowledgement:** Answers here are all original, with some help from *The Byzantine Generals Problem*, L. , R. , and M. Pease, 1982.