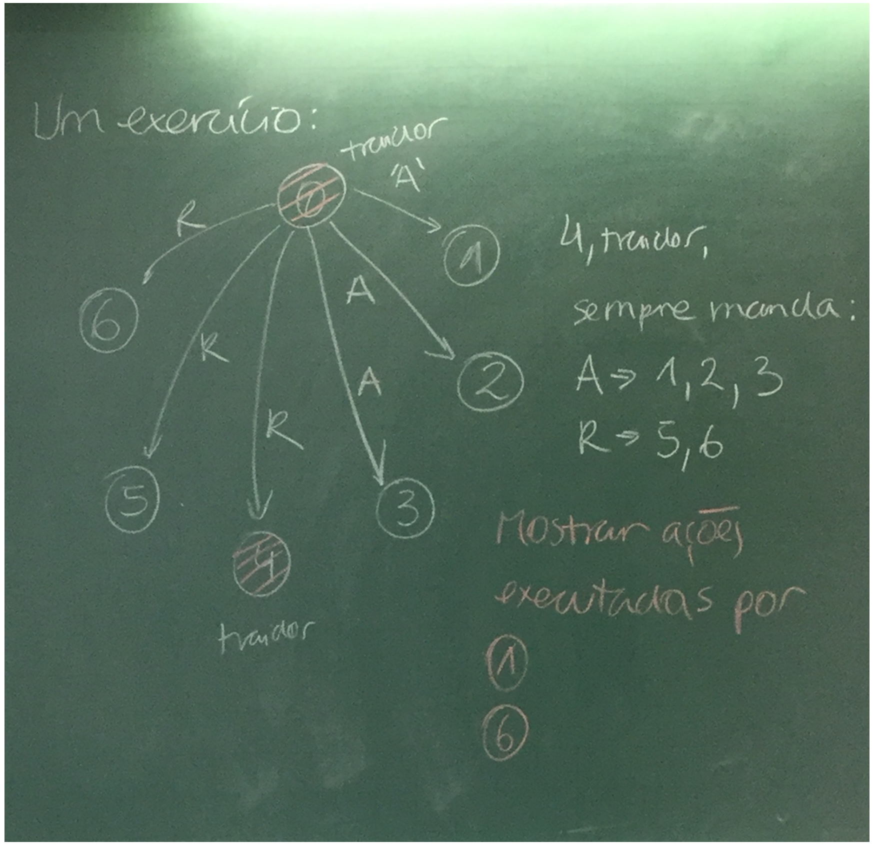
Aula 20 - Generais Bizantinos (cont.)

Monday, May 23, 2016 13:54



Nodo 1:

Passo	Valoresssssssssss	Valoresssssssssss	Valoresssssssssss	Valoresssssssssss	Valoresssssssssss
GP(2)	$n = 4$				

GB(2)	$v_0 = A$				
GB(1)	$v_{2,0} = A$	$v_{3,0} = A$	$v_{4,0} = A$	$v_{5,0} = R$	$v_{6,0} = R$
GB(0)	$v_{3,2,0} = A$ $v_{4,2,0} = A$ $v_{5,2,0} = A$ $v_{6,2,0} = A$	$v_{2,3,0} = A$ $v_{4,3,0} = A$ $v_{5,3,0} = A$ $v_{6,3,0} = A$	$v_{2,4,0} = A$ $v_{3,4,0} = A$ $v_{5,4,0} = R$ $v_{6,4,0} = R$	$v_{2,5,0} = R$ $v_{3,5,0} = R$ $v_{4,5,0} = A$ $v_{6,5,0} = R$	$v_{2,6,0} = R$ $v_{3,6,0} = R$ $v_{4,6,0} = A$ $v_{5,6,0} = R$
MOST	$v_2 = A$	$v_3 = A$	$v_4 = A$	$v_5 = R$	$v_6 = R$

Nodo 1 executa A

Nodo 6:

Passo	Valoressssssssss	Valoressssssssss	Valoressssssssss	Valoressssssssss	Valoressssssssss
GB(2)	$v_0 = R$				
GB(1)	$v_{1,0} = A$	$v_{2,0} = A$	$v_{3,0} = A$	$v_{4,0} = R$	$v_{5,0} = R$
GB(0)	$v_{2,1,0} = A$ $v_{3,1,0} = A$ $v_{4,1,0} = R$ $v_{5,1,0} = A$	$v_{1,2,0} = A$ $v_{3,2,0} = A$ $v_{4,2,0} = R$ $v_{5,2,0} = A$	$v_{1,3,0} = A$ $v_{2,3,0} = A$ $v_{4,3,0} = R$ $v_{5,3,0} = A$	$v_{1,4,0} = A$ $v_{2,4,0} = A$ $v_{3,4,0} = A$ $v_{5,4,0} = R$	$v_{1,5,0} = R$ $v_{2,5,0} = R$ $v_{3,5,0} = R$ $v_{4,5,0} = R$
MOST	$v_1 = A$	$v_2 = A$	$v_3 = A$	$v_4 = A$	$v_5 = R$

Nodo 6 executa A

Prova de corretude

Lema 1

Para quaisquer valores de m e k, o algoritmo genbiz(m) satisfaz IC2 se o número total de ge nerais $n >$ 2*$k + m$ dos quais no máximo k são traidores.

Ou seja, quando o comandante é leal, a margem para número de traidores é muito maior!

Prova

Por indução em m

Base: Se m=0 e o comandante é leal, então todo comandado leal recebe e executa a mesma ordem do comandante.

Hipótese: Assuma que o algoritmo funciona corretamente para (m-1), sendo m>0.
Estamos dizendo que genbiz(m-1) funciona corretamente, satisfaz IC2
Passo: No algoritmo, o comandante executa genbiz(m) enviando a ordem para (n-1) comandados. Cada um se transforma em comandante e executa genbiz(m-1).

Como, por hipótese, $n > 2k + m$, então $(n-1) > 2K + (m-1)$
Um comandado leal recebe o valor "verdadeiro, correto" de todo outro comandado leal
$(n-1) > 2k + (m-1) \geq 2k$
E, no máximo k generais são traidores.
$(n-1) > 2k$
k traidores; $(n-1)$ é mais do que o dobro do número de traidores
(os generais estão executando genbiz($n-1$))

Conclusão: Para um comandado/comandante leal i, todo comandado leal executa a ação correta v_i.
Como a maioria é leal $(n-1) > 2k$), todos executam a mesma ação.

Este lema permite uma compreensão maior dos limites do algoritmo quando o comandante é leal: $n > 2k + m$

Genbiz(3), $n = 18$
$18 > 2k + 3$; $15 > 2k$; até $k = 7$ traidores!

Genbiz(5), $n = 18$
$18 > 2k + 5$; $13 > 2k$; até $k = 6$ traidores.

Genbiz(18), $n = 18$
$18 > 2k + 18$; $0 > 2k$; até $k = 0$ traidores.