TD6 : Correction

A Pannes byzantines

A.1 Cet Algorithme termine-t-il ?

Correction : Cet algorithme termine car il fait appel uniquement à $p(m-1)$ sans faire de boucle et le $p(0)$ termine.

A.2 Montrer que pour tout m et k, si $n > 2k + m$ avec k byzantins, l'algorithme $P(m)$ satisfait la condition IC2.

Correction : Nous allons procéder par récurrence de m (nombre de byzantin).

- $P(0)$ Le général n'est pas un Byzantin et il n'y a pas de messages non délivrés. Donc vérifié.
- $P(m)$ Admettons que $P(m-1)$ satisfait la propriété IC2.
  A l'étape 1 : le général l_0 envoie la valeur $< v >$ à chacun de ses lieutenants.
  A l'étape 2 : chaque lieutenants loyal l_i exécute de nouveau $P(m-1)$ à l'étape 2(b)ii (devenant général). On sait que $m > 0$, on a aussi $n - 1 > 2k + (m-1)$ ce qui nous permet d'utiliser l'hypothèse de récurrence. Chaque lieutenant loyal l_i obtient $v_j = v$ de chaque lieutenant loyal l_j. Sa liste $(v_0, ..., v_{n-1})$ contient $n - k$ éléments ayant la valeur v.
  Comme $n > 2k+m$ on a $n > 2k+m > 2k$ ce qui donne $n-2k > 0 \Rightarrow 2n-2k > n \Rightarrow n-k > \frac{n}{2}$
  On en déduit que dans le liste $(v_0, ..., v_{n-1})$ les messages venant de lieutenant loyaux $n - k$ restent majoritaire.
  CQFD.

A.3 Montrer que si il y a n lieutenants avec m byzantins ($n > 3m$), l'algorithme $P(m)$ satisfait les deux IC1 et IC2

Correction : Nous allons procéder par récurrence de m (nombre de byzantin) avec toujours n le nombre de participant.

- $P(0)$ Le général n'est pas un Byzantin et il n'y a pas de messages non délivrés. Donc IC1 et IC2.
- $P(m)$ Admettons que $P(m-1)$ satisfait les propriétés IC1 et IC2.
  Si le général n'est pas byzantin d'après la question précédente, $P(m)$ satisfait la condition IC2. Comme IC2 implique IC1, alors P(m) satisfait IC2 et IC1.

  Si le général est byzantin : Il y a $m-1$ lieutenants byzantins. Regardons le comportement de l'algorithme :
  Au début, le général l_0 exécute l'étape 1 de façon aléatoire. Ensuite ses lieutenants vont passer à l'étape 2 : Chaque lieutenant exécute $P(m-1)$ comme si il était le général avec $n-2$ lieutenants.
  On a que : $n > 3m \Rightarrow n-2 > 3m-2 > 3(m-1)$. Ce qui nous permet d'appliquer l'hypothèse de récurrence sur $P(m-1)$.
  Considérons v_j après l'exécution de $p(m-1)$. Il y a deux possibilités :

  1. Si j est un byzantin, alors pour toutes les valeurs v_j des lieutenant loyaux sont identiques (par IC1).
  2. Si j n'est pas un byzantin, alors pour toutes les valeurs v_j des lieutenant loyaux sont identiques (par IC2).

  Donc tous les lieutenants loyaux possèdent la même liste $(v_0, ..., v_{n-1})$ (dans un ordre différent)
  Comme ils appliquent la même fonction majorité, ils obtiennent le même résultat. Ce qui vérife la condition IC2