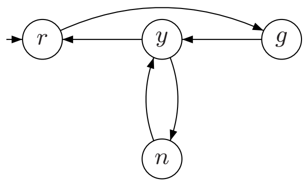
TD - Introduction en logique du temps ramifié (CTL)

C. Dima

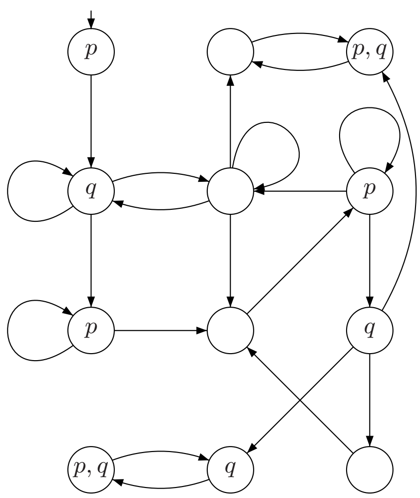
Exercice 1: Prenons l'exemple d'un système de transitions modélisant un feu tricolore (plus un état d'erreur) dans la figure suivante (les étiquettes précisent les variables propositionnelles qui sont vraies dans les états respectifs) :



Parmi la liste suivante de propriétés, préciser lesquelles sont satisfaites et dans quel état :

1. $\forall \bigcirc (r \vee n)$.
2. $\forall \Diamond y, \forall \Box y, \exists \Diamond g$.
3. $\forall \Box \forall \Diamond y, \forall (n \,\mathcal{U}\, \neg n)$.
4. $\forall (g \,\mathcal{U}\, \forall (y \,\mathcal{U}\, r))$.

Exercice 2: Considérons le système de transition de la figure suivante :



Calculer les états dans lesquels les formules suivantes sont satisfaites, selon les différents algorithmes (algorithme de graphes, calcul de point fixe) :

$$\forall\big((\exists \Diamond p)\,\mathcal{U}(\exists \Box q)\big) \qquad \forall\big(\bigcirc q \wedge \exists(\exists \Box p \,\mathcal{U}\, q)\big)$$

Exercice 3: Laquelle des formules suivantes est une tautologie (formule valide dans n'importe quel modèle) :

$$\forall \bigcirc \forall \Diamond \phi \equiv \forall \Diamond \forall \bigcirc \phi$$
$$\forall \bigcirc \forall \Box \phi \equiv \forall \Box \forall \bigcirc \phi$$
$$\exists \Diamond \exists \bigcirc \phi \equiv \exists \bigcirc \exists \Diamond \phi$$
$$\exists \Diamond \exists \Box \phi \equiv \exists \Box \exists \Diamond \phi$$
$$\neg \forall (\phi \,\mathcal{U}\, \psi) \equiv \exists (\phi \,\mathcal{U}\, \neg \psi)$$
$$\exists \big((\phi \wedge \psi) \mathcal{U} (\neg \phi \bigcirc \psi)\big) \equiv \big(\phi \mathcal{U} (\neg \phi \wedge \psi)\big)$$
$$\forall \Box \phi \wedge (\neg \phi \vee \exists \bigcirc \exists \Diamond \neg \phi) \equiv \exists \bigcirc \neg \phi \wedge \forall \bigcirc \phi$$

Exercice 4: Pour chacune des paires de formules qui suit (la première formule étant une formule CTL, la deuxième une formule LTL), indiquer si les deux formules sont équivalentes sur tous les modèles de systèmes de transition ou, sinon, donner un contre-exemple (un système de transition et un état qui satisfont l'une et pas l'autre) :

1. $\forall \Box \forall \bigcirc p$ et $\Box \bigcirc p$.
2. $\forall \Diamond p \vee \forall \Diamond q$ et $\Diamond (p \vee q)$.
3. $\forall \Box (a \to \forall \Diamond b)$ et $\Box (a \to \Diamond b)$.

Exercice 5: (Reprise d'un exercice du module d'*Initiation à la sécurité*) On considère un système dans lequel on a quatre utilisateurs, $U = \{a, b, c, d\}$ et trois fichiers, $F = \{x, y, z\}$. Les actions possibles sont la lecture et l'écriture d'un fichier par un utilisateur, ainsi que la création, et les droits d'accès sont o (possesion), r et w.

On veut imposer une politique de sécurité dans laquelle a pourrait avoir accès aux fichiers z, t seulement s'il n'a pas eu accès à un fichier auquel b aurait fait un accès auparavant. Modéliser cette situation comme système de contrôle d'accès obligatoire, en rajoutant éventuellement des permissions et en modifiant les commandes. Raffiner la spécification avec des propriétés temporelles permettant d'obtenir le système le plus "libéral" possible.
