Clôture par congruence et procédures de décision

Damien Rouhling

ENS de Lyon

03 Septembre 2013

Contexte

- Preuve automatique de formules

Contexte

- Preuve automatique de formules
- PSYCHE

Contexte

- Preuve automatique de formules
- PSYCHE
- Raisonnement modulo théories

Contexte

- Preuve automatique de formules
- PSYCHE
- Raisonnement modulo théories
- Théorie de l'égalité

Contexte

- Preuve automatique de formules
- PSYCHE
- Raisonnement modulo théories
- Théorie de l'égalité
  Exemple :

  $f(b) = d \wedge b = d \wedge f(d) = a \Rightarrow a = b$

Plan

Plan

Le problème

Axiomes :

1. $\forall x,\ x = x$ (réflexivité)
2. $\forall x, y, z,\ x = y \wedge y = z \Rightarrow x = z$ (transitivité)
3. $\forall x, y,\ x = y \Rightarrow y = x$ (symétrie)
4. Pour chaque symbole de fonction f d'arité n :

$$\forall x_1, \ldots, x_n, y_1, \ldots, y_n,\ (x_1 = y_1 \wedge \cdots \wedge x_n = y_n)$$

$$\Rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$$

Exemple

$$f(b) = d \wedge b = d \wedge f(d) = a \Rightarrow a = b$$

Exemple

$$f(b) = d \wedge b = d \wedge f(d) = a \Rightarrow a = b$$

$$b = d$$

Exemple

$$f(b) = d \wedge b = d \wedge f(d) = a \Rightarrow a = b$$

$$f(b) = f(d)$$

Exemple

$$f(b) = d \wedge b = d \wedge f(d) = a \Rightarrow a = b$$

$$f(b) = f(d)$$

$$f(b) = a$$

Exemple

$$f(b) = d \wedge b = d \wedge f(d) = a \Rightarrow a = b$$

$$f(b) = f(d)$$

$$f(b) = a$$

$$d = a$$

Exemple

$$f(b) = d \wedge b = d \wedge f(d) = a \Rightarrow a = b$$

$$f(b) = f(d)$$

$$f(b) = a$$

$$d = a$$

$$b = a$$

Plan

Ajout de diségalités

$$\{a = f\left(f\left(f\left(a\right)\right)\right), a = f\left(f\left(f\left(f\left(f\left(a\right)\right)\right)\right)\right), a \neq f\left(a\right)\}$$

Ajout de diségalités

$$\{a = f(f(f(a))), a = f(f(f(f(f(a))))), a \neq f(a)\}$$

$$a = f(f(f(a)))$$

Ajout de diségalités

$$\{a = f\left(f\left(f\left(a\right)\right)\right), a = f\left(f\left(f\left(f\left(f\left(a\right)\right)\right)\right)\right), a \neq f\left(a\right)\}$$

$$f(a) = f(f\left(f\left(f\left(a\right)\right)\right))$$

Ajout de diségalités

$$\{a = f\left(f\left(f\left(a\right)\right)\right), a = f\left(f\left(f\left(f\left(f\left(a\right)\right)\right)\right)\right), a \neq f\left(a\right)\}$$

$$f(f(a)) = f(f(f\left(f\left(f\left(a\right)\right)\right)))$$

Ajout de diségalités

$$\{a = f(f(f(a))), a = f(f(f(f(f(a))))), a \neq f(a)\}$$

$$f(f(a)) = f(f(f(f(f(a)))))$$

$$f(f(a)) = a$$

Ajout de diségalités

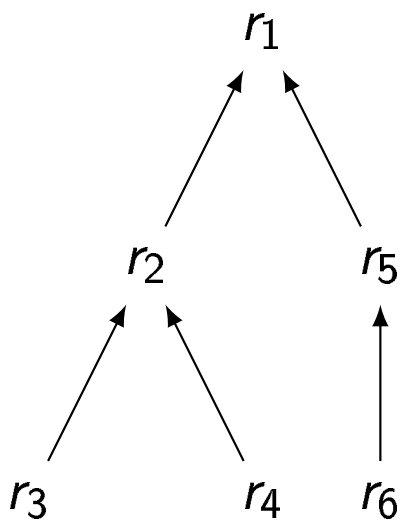
$$\{a = f(f(f(a))), a = f(f(f(f(f(a))))), a \neq f(a)\}$$

$$f(f(a)) = f(f(f(f(f(a)))))$$

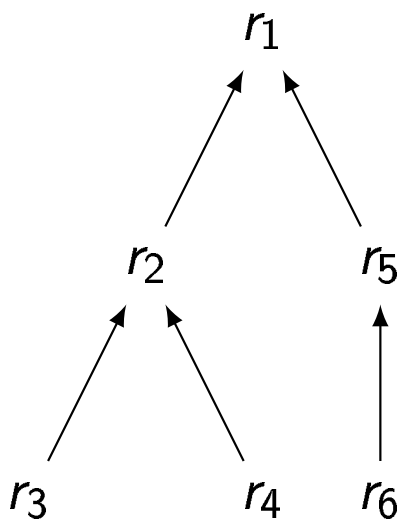
$$f(f(a)) = a$$

$$a = f(a)$$

Classes d'équivalence



Classes d'équivalence



Union-Find

Symboles interprétés

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

Symboles interprétés

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

Termes connus : $\{0, 1, x, y, 0 + x, x + y, y + 1, f(x + y), f(1)\}$

Symboles interprétés

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

Termes connus : $\{0, 1, x, y, 0 + x, x + y, y + 1, f(x + y), f(1)\}$

Valeurs sémantiques associées :

Valeurs	0						
Termes associés	0						

Symboles interprétés

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

Termes connus : $\{0, 1, x, y, 0 + x, x + y, y + 1, f(x + y), f(1)\}$

Valeurs sémantiques associées :

Valeurs	0	1						
Termes associés	0	1						

Symboles interprétés

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

Termes connus : $\{0, 1, x, y, 0 + x, x + y, y + 1, f(x + y), f(1)\}$

Valeurs sémantiques associées :

Valeurs	0	1	X					
Termes associés	0	1	x					

Symboles interprétés

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

Termes connus : $\{0, 1, x, y, 0 + x, x + y, y + 1, f(x + y), f(1)\}$

Valeurs sémantiques associées :

Valeurs	0	1	X	Y				
Termes associés	0	1	x	y				

Symboles interprétés

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

Termes connus : $\{0, 1, x, y, 0 + x, x + y, y + 1, f(x + y), f(1)\}$

Valeurs sémantiques associées :

Valeurs	0	1	X	Y				
Termes associés	0	1	x $0 + x$	y				

Symboles interprétés

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

Termes connus : $\{0, 1, x, y, 0 + x, x + y, y + 1, f(x + y), f(1)\}$

Valeurs sémantiques associées :

Valeurs	0	1	X	Y	$X + Y$			
Termes associés	0	1	x $0 + x$	y	$x + y$			

Symboles interprétés

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

Termes connus : $\{0, 1, x, y, 0 + x, x + y, y + 1, f(x + y), f(1)\}$

Valeurs sémantiques associées :

Valeurs	0	1	X	Y	$X + Y$	$1 + Y$		
Termes associés	0	1	x $0 + x$	y	$x + y$	$y + 1$		

Symboles interprétés

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

Termes connus : $\{0, 1, x, y, 0 + x, x + y, y + 1, f(x + y), f(1)\}$

Valeurs sémantiques associées :

Valeurs	0	1	X	Y	$X + Y$	$1 + Y$	F
Termes associés	0	1	x $0 + x$	y	$x + y$	$y + 1$	$f(x + y)$

Symboles interprétés

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

Termes connus : $\{0, 1, x, y, 0 + x, x + y, y + 1, f(x + y), f(1)\}$

Valeurs sémantiques associées :

Valeurs	0	1	X	Y	$X + Y$	$1 + Y$	F	G
Termes associés	0	1	x $0 + x$	y	$x + y$	$y + 1$	$f(x + y)$	$f(1)$

Plan

La question

Exemple :

$1 + 1 = 2\,?$

La question

Exemple :

$1 + 1 = 2\,?$

$$E = \{a_1 = b_1, a_1 = c_1, f(a_1, a_1) = a, f(b_1, b_1) = b, f(c_1, c_1) = c, a \neq c\}$$

La question

Exemple :

$1 + 1 = 2\,?$

$$E = \{a_1 = b_1, a_1 = c_1, f(a_1, a_1) = a, f(b_1, b_1) = b, f(c_1, c_1) = c, a \neq c\}$$

E

La question

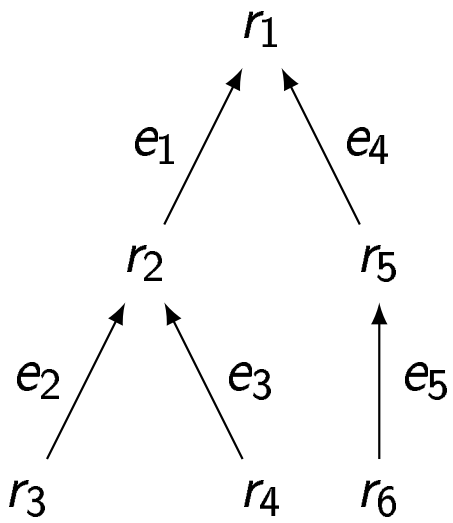
Exemple :

$1 + 1 = 2$?

$E = \{a_1 = b_1, a_1 = c_1, f(a_1, a_1) = a, f(b_1, b_1) = b, f(c_1, c_1) = c, a \neq c\}$

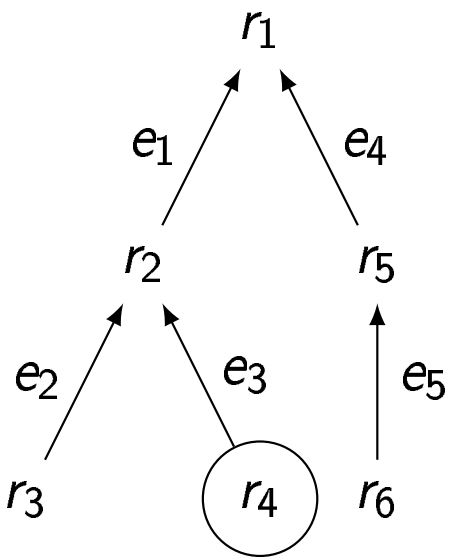
E ou $\{a_1 = c_1, f(a_1, a_1) = a, f(c_1, c_1) = c, a \neq c\}$?

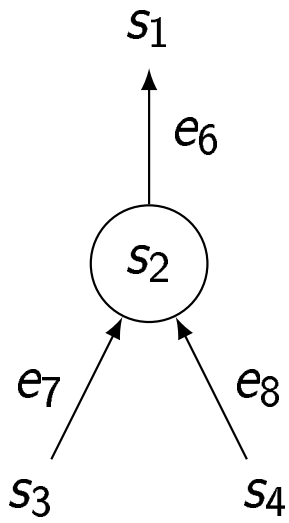
Format des classes d'équivalences



Format des classes d'équivalences

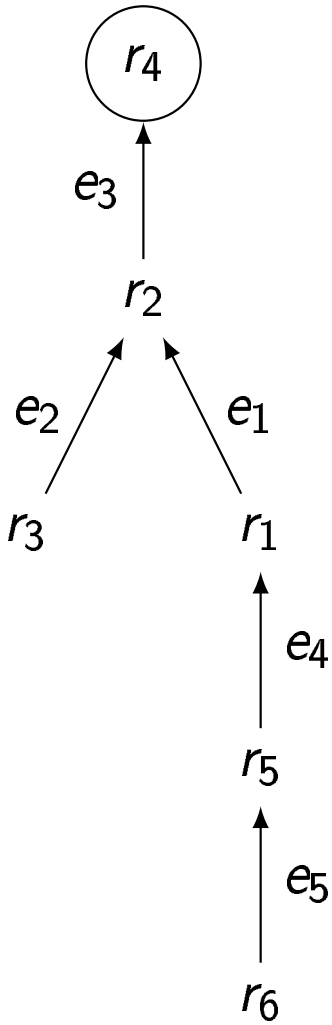
$r_4 \equiv s_2$ via e_9 :

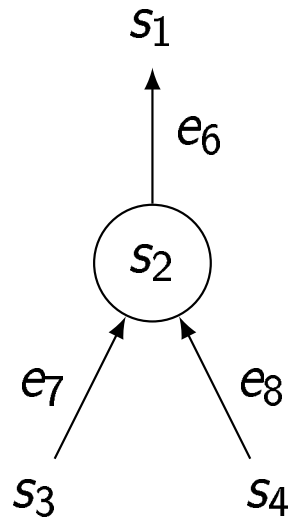




Format des classes d'équivalences

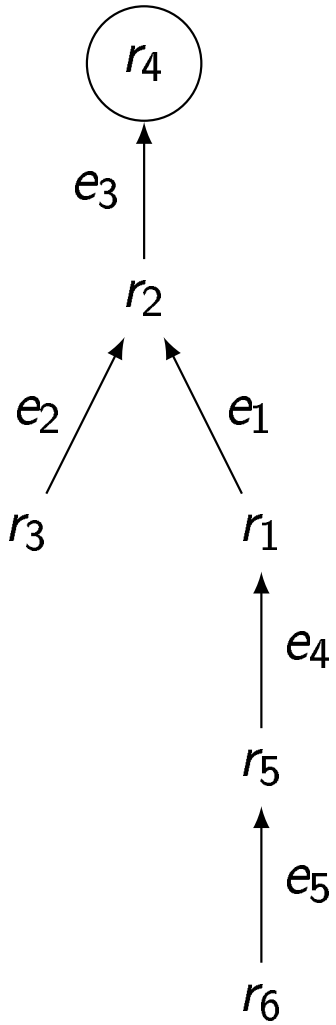
$r_4 \equiv s_2$ via e_9 :

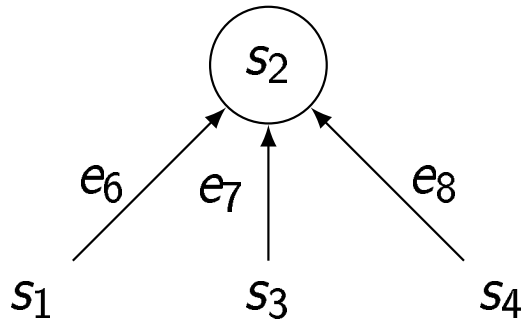




Format des classes d'équivalences

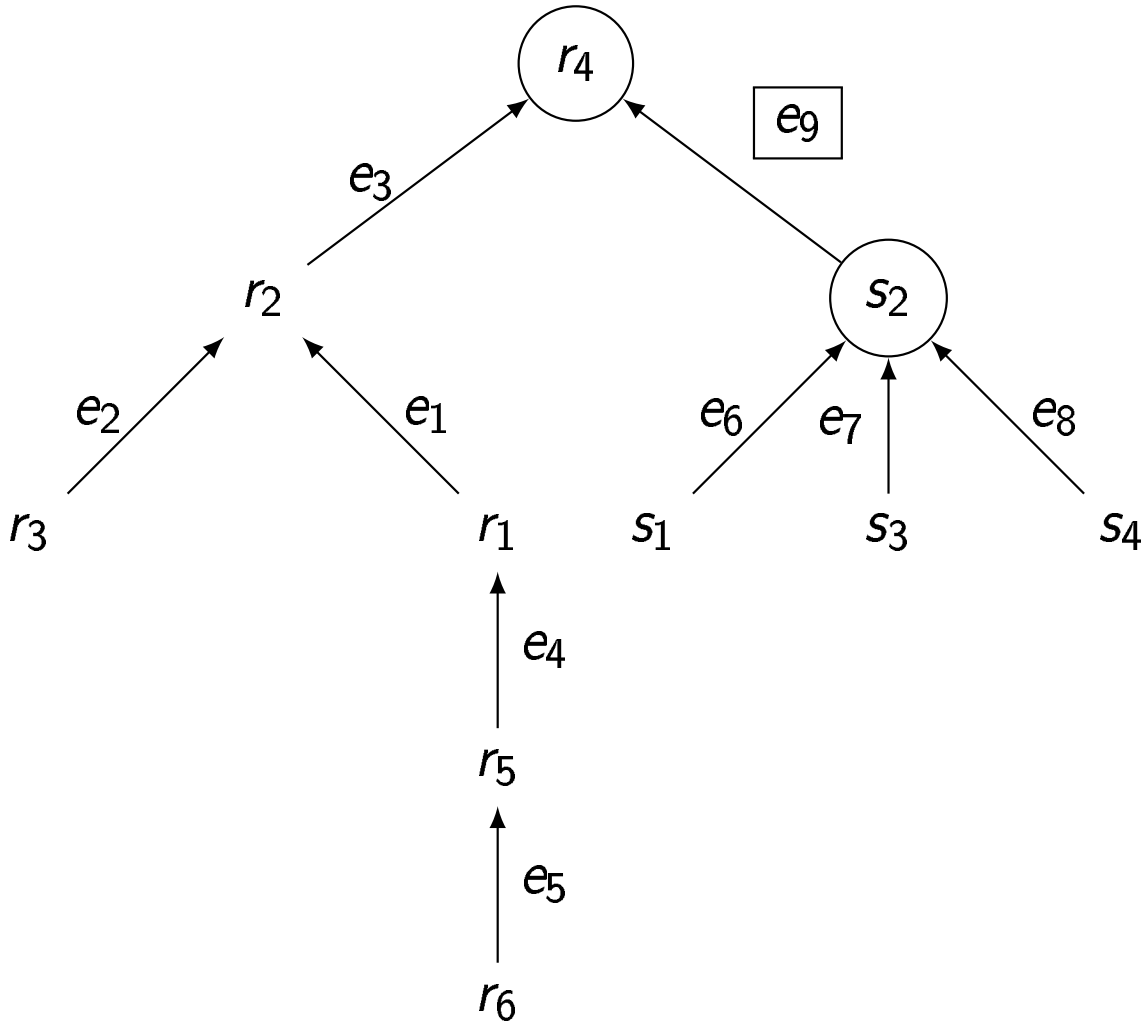
$r_4 \equiv s_2$ via e_9 :





Format des classes d'équivalences

$r_4 \equiv s_2$ via e_9 :



Exemple

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

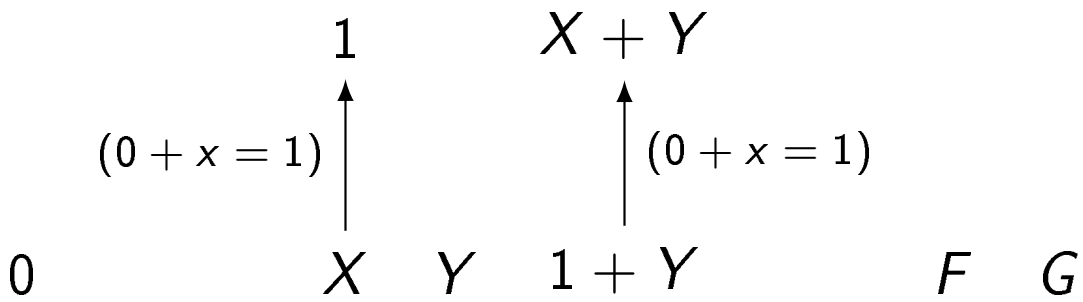
Termes connus : $\{0, 1, x, y, 0 + x, x + y, y + 1, f(x + y), f(1)\}$

$$0 \quad 1 \quad X \quad Y \quad X + Y \quad 1 + Y \quad F \quad G$$

Exemple

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

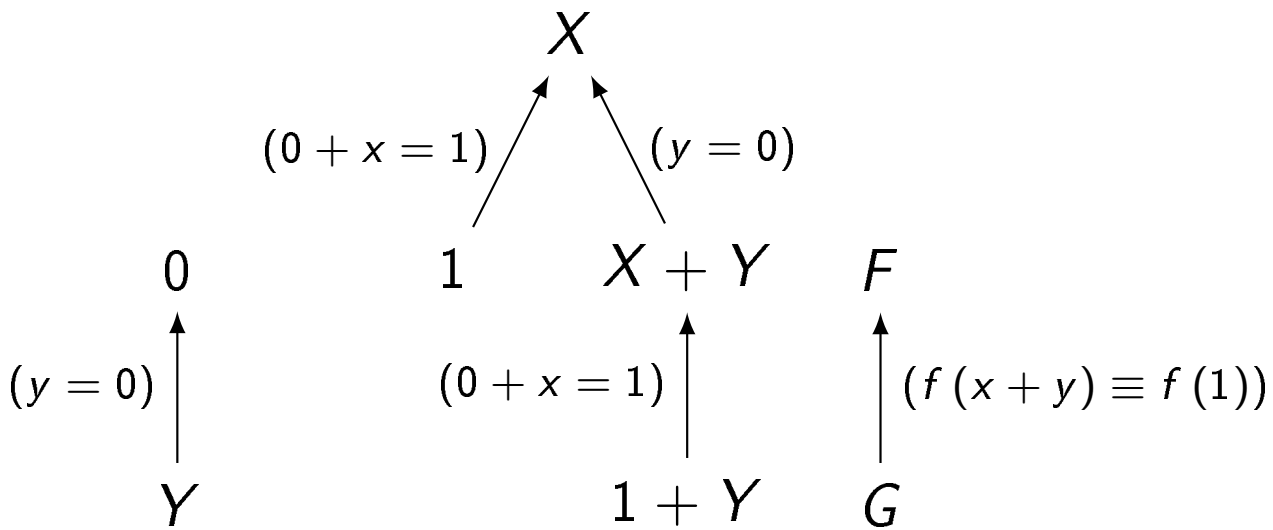
Termes connus : $\{0, 1, x, y, 0 + x, x + y, y + 1, f(x + y), f(1)\}$



Exemple

Problème initial : $0 + x = 1, y = 0, f(x + y) \neq f(1)$

Termes connus : $\{0, 1, x, y, 0 + x, x + y, y + 1, f(x + y), f(1)\}$



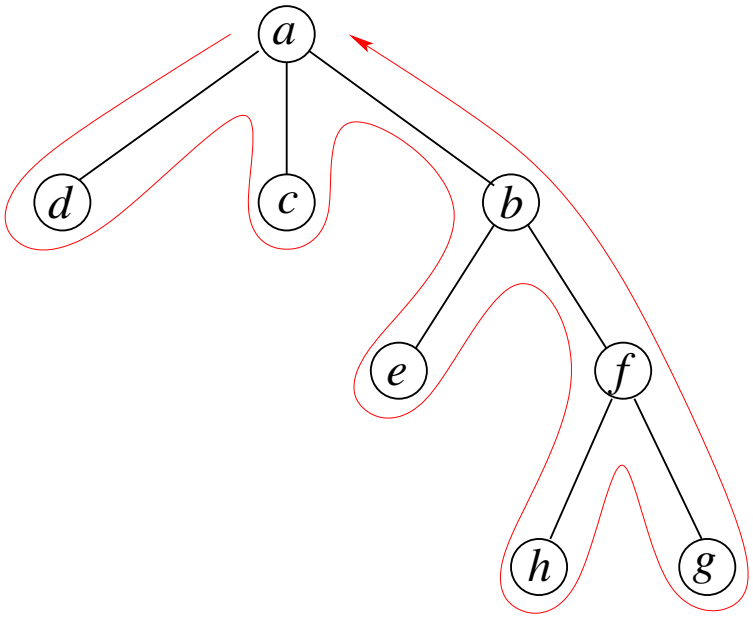
Plan

L'algorithme

PAC (Premier Ancêtre Commun) est lié à
IMIN (Indice de la valeur MINimale entre deux indices dans un tableau).

L'algorithme

PAC (Premier Ancêtre Commun) est lié à
IMIN (Indice de la valeur MINimale entre deux indices dans un tableau).

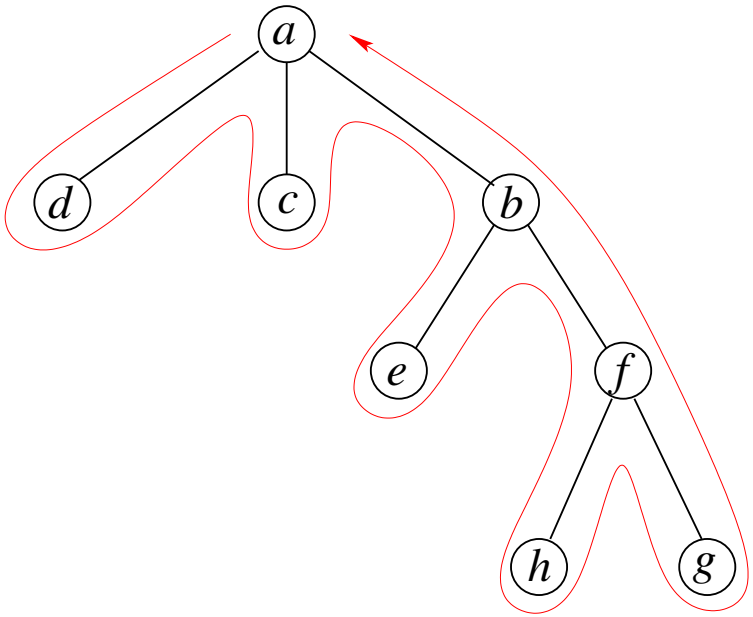


Un Tour Eulerien avec les profondeurs

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Noeud	*a*	*d*	*a*	*c*	*a*	*b*	*e*	*b*	*f*	*h*	*f*	*g*	*f*	*b*	*a*
Profondeur	*0*	*1*	*0*	*1*	*0*	*1*	*2*	*1*	*2*	*3*	*2*	*3*	*2*	*1*	*0*

L'algorithme

PAC (Premier Ancêtre Commun) est lié à
IMIN (Indice de la valeur MINimale entre deux indices dans un tableau).



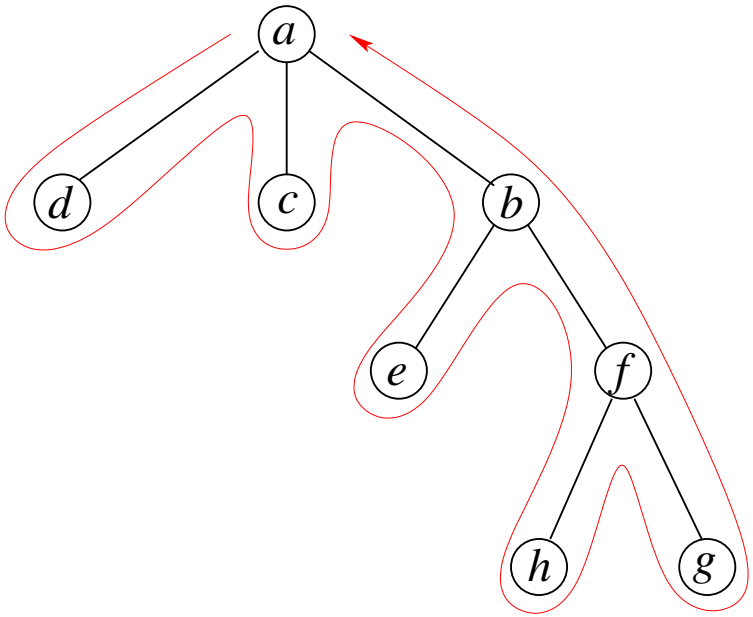
Un Tour Eulerien avec les profondeurs

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Noeud	*a*	*d*	*a*	*c*	*a*	*b*	*e*	*b*	*f*	*h*	*f*	*g*	*f*	*b*	*a*
Profondeur	*0*	*1*	*0*	*1*	*0*	*1*	*2*	*1*	*2*	*3*	*2*	*3*	*2*	*1*	*0*

a	b	c	d	e	f	g	h
1	6	4	2	7	9	12	10

L'algorithme

PAC (Premier Ancêtre Commun) est lié à
IMIN (Indice de la valeur MINimale entre deux indices dans un tableau).



Un Tour Eulerien avec les profondeurs

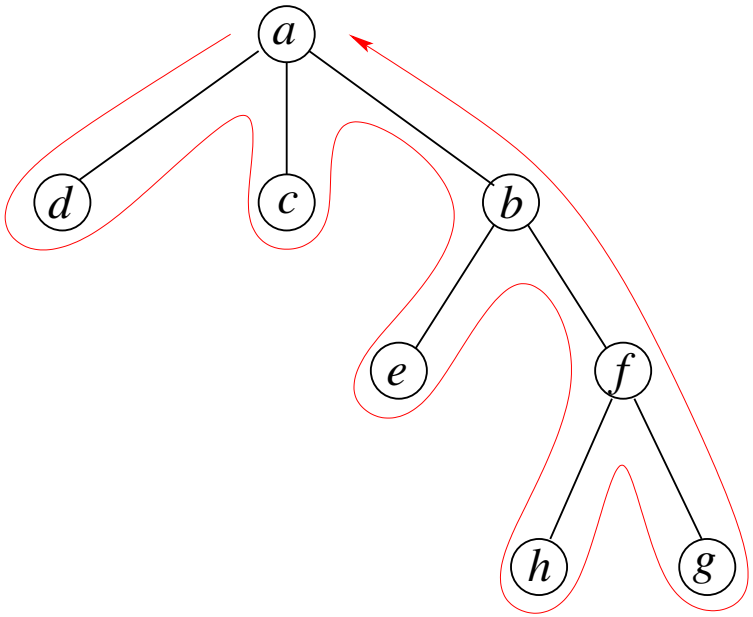
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Noeud	*a*	*d*	*a*	*c*	*a*	*b*	*e*	*b*	*f*	*h*	*f*	*g*	*f*	*b*	*a*
Profondeur	*0*	*1*	*0*	*1*	*0*	*1*	*2*	*1*	*2*	*3*	*2*	*3*	*2*	*1*	*0*

a	b	c	d	e	f	g	h
1	6	4	2	7	9	12	10

PAC(e,g) ?

L'algorithme

PAC (Premier Ancêtre Commun) est lié à
IMIN (Indice de la valeur MINimale entre deux indices dans un tableau).



Un Tour Eulerien avec les profondeurs

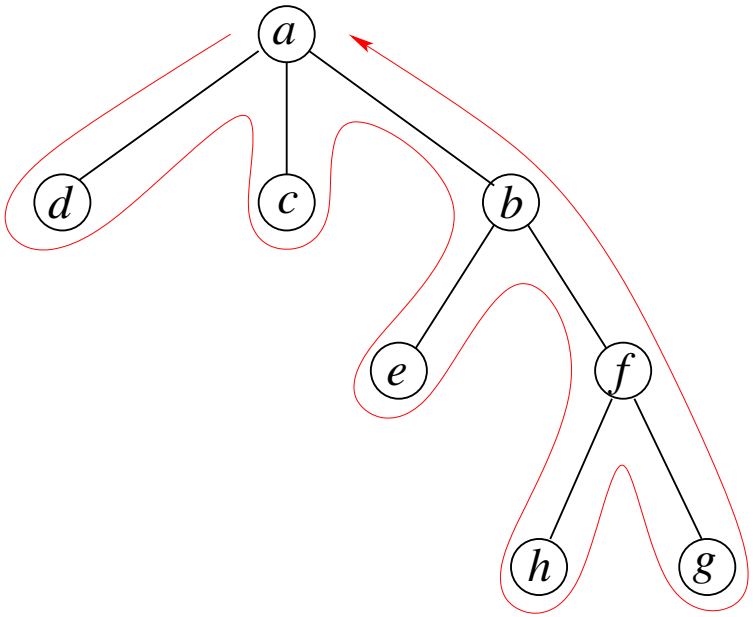
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Noeud	*a*	*d*	*a*	*c*	*a*	*b*	*e*	*b*	*f*	*h*	*f*	*g*	*f*	*b*	*a*
Profondeur	*0*	*1*	*0*	*1*	*0*	*1*	*2*	*1*	*2*	*3*	*2*	*3*	*2*	*1*	*0*

a	b	c	d	e	f	g	h
1	6	4	2	7	9	12	10

PAC(e,g) ? $\Rightarrow$ T(IMIN(7,12))

L'algorithme

PAC (Premier Ancêtre Commun) est lié à
IMIN (Indice de la valeur MINimale entre deux indices dans un tableau).



Un Tour Eulerien avec les profondeurs

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Noeud	*a*	*d*	*a*	*c*	*a*	*b*	*e*	*b*	*f*	*h*	*f*	*g*	*f*	*b*	*a*
Profondeur	*0*	*1*	*0*	*1*	*0*	*1*	*2*	*1*	*2*	*3*	*2*	*3*	*2*	*1*	*0*

a	b	c	d	e	f	g	h
1	6	4	2	7	9	12	10

PAC(e,g) ? $\Rightarrow$ T(IMIN(7,12)) $\Rightarrow$ b

Indice de la valeur minimale entre deux indices

Prétraitement $\mathcal{O}(n \log(n))$ **:**
$A(i,k) = \text{IMIN}\left(i, i + 2^k - 1\right)$

$$
\begin{array}{c} \\ i \\ \vdots \\ i + 2^{k-1} \end{array}
\begin{array}{c}
\begin{array}{ccccc} & & k-1 & & k \end{array} \\
\begin{pmatrix}
 & & \vdots & & \vdots \\
\cdots & \cdots & X & \longleftarrow & ? \\
 & & \vdots & \swarrow & \\
\cdots & \cdots & X & &
\end{pmatrix}
\end{array}
$$

Indice de la valeur minimale entre deux indices

Prétraitement $\mathcal{O}(n \log(n))$:
$A(i,k) = \text{IMIN}\left(i, i + 2^k - 1\right)$

$$
\begin{array}{c} \\ i \\ \vdots \\ i + 2^{k-1} \end{array}
\begin{array}{c}
\begin{array}{ccccc} & & k-1 & & k \end{array} \\
\left(\begin{array}{ccccc}
 & & \vdots & & \vdots \\
 & & \vdots & & \vdots \\
\cdots & \cdots & X & \longleftarrow & ? \\
 & & \vdots & \swarrow & \\
\cdots & \cdots & X & &
\end{array}\right)
\end{array}
$$

Résolution d'une instance $\mathcal{O}(1)$:
(i,j)

Indice de la valeur minimale entre deux indices

Prétraitement $\mathcal{O}(n \log(n))$:
$A(i,k) = \text{IMIN}\left(i, i + 2^k - 1\right)$

$$
\begin{array}{c} \\ i \\ \vdots \\ i + 2^{k-1} \end{array}
\begin{array}{c}
\begin{array}{ccccc} & & k-1 & & k \end{array} \\
\begin{pmatrix}
 & & \vdots & & \vdots \\
\cdots & \cdots & X & \longleftarrow & ? \\
 & & \vdots & \swarrow & \\
\cdots & \cdots & X & &
\end{pmatrix}
\end{array}
$$

Résolution d'une instance $\mathcal{O}(1)$:
$(i,j) \Rightarrow p = \lfloor \log_2(j - i + 1) \rfloor$

Indice de la valeur minimale entre deux indices

Prétraitement $\mathcal{O}(n \log(n))$:
$A(i,k) = \text{IMIN}\left(i, i + 2^k - 1\right)$

$$
\begin{array}{c} \\ i \\ \vdots \\ i + 2^{k-1} \end{array}
\begin{array}{c}
\begin{array}{ccccc} & & k-1 & & k \end{array} \\
\begin{pmatrix}
 & & \vdots & & \vdots \\
\cdots & \cdots & X & \longleftarrow & ? \\
 & & \vdots & \swarrow & \\
\cdots & \cdots & X & &
\end{pmatrix}
\end{array}
$$

Résolution d'une instance $\mathcal{O}(1)$:
$(i,j) \Rightarrow p = \lfloor \log_2(j - i + 1) \rfloor \Rightarrow A(i,p)$ ou $A(j - 2^p + 1, p)$?

Conclusion

- Programmation

Conclusion

- Programmation
- Tests et performances

Conclusion

- Programmation
- Tests et performances
- Aspects pratiques

Conclusion

- Programmation
- Tests et performances
- Aspects pratiques
- Premier ordre