CS 576 Lecture 5, 1/31/17

J. Meseguer

Recall the definition of the $\to_{R/B}$ relation for $\mathcal{R} = (\Sigma, B, R)$ a rewrite theory as the relation $\to_{R/B} \, = \, =_B ; \to_R ; =_B$.

Recall also the notions of:

1. $\to_{R/B}$ <u>terminating</u> (i.e., no infinite $\to_{R/B}$-sequences)

2. $\to_{R/B}$ <u>confluent</u>:

$$\begin{tikzcd}[column sep=small] & & u \arrow[dl, "*"', "R/B"] \arrow[dr, "*", "R/B"'] & \\ \forall & v \arrow[d, "R/B"] & & v' \arrow[d, "R/B"] \\ \exists & w \arrow[rr, equal, "B"'] & & w' \end{tikzcd}$$

1. The $\to_{R,B}$ Relation

Obviously, the $\to_{R/B}$ relation is conceptually the one we want to reason <u>modulo</u> the equational properties B, since it <u>induces</u> an entirely similar relation of B-equivalence classes $[u], [v] \in T_{\Sigma/B}(X)$ by:

$$[u] \to_{R/B} [v] \overset{\text{def.}}{\Longleftrightarrow} u \to_{R/B} v$$

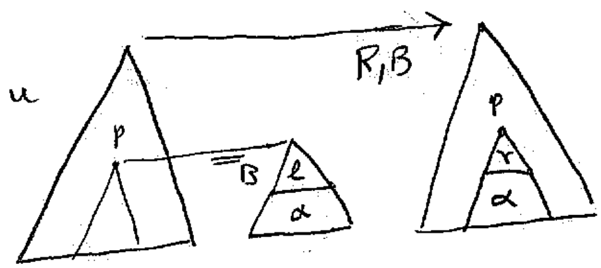
However, <u>computing</u> the $\to_{R/B}$ can be very inefficient, since to <u>decide</u> whether we can rewrite a term u with $\to_{R/B}$ we may need to <u>explore</u> <u>all</u> u' such that $u =_B u'$

to see if any such u' is such that $u' \xrightarrow[R]{} v'$, and there can be an <u>infinite</u> number of u' with $u =_B u'$, or even if $[u]_B$ is a <u>finite</u> set (e.g. for B = assoc, or assoc & comm) it may be very inefficient to search for all u' such that $u' =_B u$.

For this reason, a much more efficient relation $\xrightarrow[R,B]{}$ based on the idea of B-matching is used:

<u>Def</u>. Let $\mathcal{R} = (\Sigma, B, R)$ be a rewrite theory and $u, v \in T_\Sigma(X)$. We define $u \xrightarrow[R,B]{} v$ iff there is a position p, a rule $l \to r \in R$ and a substitution α such that:

$$\begin{cases} 1. & u|_p =_B l\alpha \\ 2. & v = u[r\alpha]_p \end{cases}$$



We then call α a B-<u>matching substitution</u>, and say that $u|_p$ B-<u>matches</u> the lefthand side l, denoted: $l \overset{\alpha}{\underset{B}{\sqsupseteq}} u|_p$.

Of course, for $\to_{R,B}$ to be implementable we need a B-matching algorithm in the following sense:

Def. An equational theory has a B-matchp algorithm iff there is an algorithm such that for each $u, v \in T_\Sigma(X)$,

1. If $\nexists \alpha$ such that $u \overset{\alpha}{\sqsupseteq}_B v$ (i.e., such that $u\alpha =_B v$), then the algorithm stops in finite time with "failure".

2. If $\exists \alpha$ such that $u \overset{\alpha}{\sqsupseteq}_B v$, then the algorithm generates a complete set of B-matches, denoted $\mathrm{Match}_B(u,v)$, i.e., substitutions α such that:

(i) $\forall \alpha \in \mathrm{Match}_B(u,v)$, $u \overset{\alpha}{\sqsupseteq}_B v$

(ii) $\forall \beta$ s.t. $u \overset{\beta}{\sqsupseteq}_B v$ $\exists \alpha \in \mathrm{Match}_B(u,v)$ such that $\beta =_B \alpha$.

The B-matching algorithm is called finitary iff $\mathrm{Match}_B(u,v)$ is always finite and the algorithm terminates.

Example. B is assoc. and com. of $+$, $u = a + x + y$

$v = (b + d) + (c + a)$. Then $\mathrm{Match}_{AC}(u,v)$ has six

AC-matchp solutions:

$\{x \mapsto b, y \mapsto c+d\}$ $\quad$ $\{x \mapsto c+d, y \mapsto b\}$

$\{x \mapsto c, y \mapsto b+d\}$ $\quad$ $\{x \mapsto b+d, y \mapsto c\}$

$\{x \mapsto d, y \mapsto b+c\}$ $\quad$ $\{x \mapsto b+c, y \mapsto d\}$

Another AC-matchp substitution is, e.g., $\{x \mapsto b, y \mapsto d+c\}$, but then we have $\{x \mapsto b, y \mapsto d+c\} =_{AC} \{x \mapsto b, y \mapsto c+d\}$.

<u>Exercise</u>. Prove that B-matching is a special case of B-unification (sometimes called "one-way B-unification) in the following sense: suppose (Σ, B) has a B-unification algorithm. Then we obtain from it a B-matching algorithm as follows:

$$Match_B(u,v) = \{\alpha \in [X \to T_\Sigma(X)] \mid \overline{\alpha} \in Unif_B(u, \overline{v})\}$$

where $\overline{v}$ is a ground term obtained from v by turning its variables $\{x_1, .., x_n\} = vars(v)$ into fresh new constants $\overline{x}_1, .., \overline{x}_n$, and α is defined by the equivalence:

$$\alpha : x \mapsto w \iff \overline{\alpha} : x \mapsto \overline{w}$$

Note, therefore, that if B has a finitary B-unification algorithm it has <u>a fortiori</u> a finitary B-matching algorithm. However, the situation can be even better (and the B-matching algorithms much more efficient). For example: associative matching is finitary, whereas associative unif^{on} infinitary.

Going back to the $\rightarrow_{R,B}$ relation we obviously have:

<u>Fact</u> $\rightarrow_{R,B} \subseteq \rightarrow_{R/B}$

<u>Proof</u> $u \rightarrow_{R,B} v$ means $u =_B u[l\alpha]_p \rightarrow_R u[r\alpha]_p$ for some $\begin{cases} l \to r \in R \\ \alpha \\ \text{and } p \end{cases}$

The crucial matter is whether $\rightarrow_{R,B}$ can <u>simulate</u> $\rightarrow_{R/B}$ in the following sense:

$$
(SC) \qquad \forall \quad
\begin{tikzcd}
u \arrow[r, "R/B"'] \arrow[d, equal, "B"] & v \arrow[d, equal, dashed, "B"] \\
u' \arrow[r, dashed, "R,B"'] & v'
\end{tikzcd}
\quad \exists
$$

This is always true, for example, for B = commutativity, but it can fail rather badly for other theories such as associativity, or associativity-commutativity

<u>Examples</u> (1) B is AC for $+$, $R = \{a+b \rightarrow c\}$

Have $(b+d)+a \rightarrow_{R/AC} d+c$, but $(b+d)+a$ <u>cannot</u> be rewritten with $\rightarrow_{R,AC}$

(2) B is A (assoc) for $\_\cdot\_$, $R = \{a \cdot b \rightarrow c\}$.

Have $a \cdot (b \cdot d) \rightarrow_{R/A} c \cdot d$, but $a \cdot (b \cdot d)$ <u>cannot</u> be rewritten with $\rightarrow_{R,A}$.

<u>Definition</u> $\mathcal{R} = (\Sigma, B, R)$ is <u>strictly</u> B-<u>coherent</u> iff $\forall\, u, u', v \in T_\Sigma(X)$ such that $u =_B u'$ and $u \rightarrow_{R/B} v$ property (SC) above holds.

See the <u>strict coherence</u> paper in the recommended readings for an algorithm that, provided the axioms B are regular and linear and B-unifiability is decidable, will generate for each $\mathcal{R}=(\Sigma, B, R)$ a strictly B-coherent $\overline{\mathcal{R}}=(\Sigma, B, \overline{R})$ such that:

$$\begin{cases} 1. & \to_{R/B} = \to_{\overline{R}/B} \\ 2. & \to_{R,B} \subseteq \to_{\overline{\mathcal{R}},B} \end{cases}$$

For B any combination of $\left\{\begin{matrix} \text{assoc} \\ \text{comm} \\ \text{id} \end{matrix}\right\}$ axioms, if R is finite, so is $\overline{R}$. Maude automates the generation $R \mapsto \overline{R}$, making it invisible to the user by adding so-called B-extension rules.

<u>Examples</u>. (1) For $B = AC$ for $+$, $R = \{a+b \to c\}$ we have $\overline{R} = R \cup \{(a+b)+x \to c+x\}$.

(2) For $B = A$ for $\_\cdot\_$, $R = \{a \cdot b \to c\}$ we have $\overline{R} = R \cup \{x \cdot (a \cdot b) \to x \cdot c,\ (a \cdot b) \cdot y \to c \cdot y,$
$(x \cdot (a \cdot b)) \cdot y \to (x \cdot c) \cdot y\}$

<u>Def.</u> $\to_{R,B}$ is <u>confluent</u> iff

$$\forall \quad \begin{tikzcd} & u \arrow[dl, "*"', "{R,B}"] \arrow[dr, "{R,B}", "*"'] & \\ v \arrow[d, dashed, "{R,B}"'] & & v' \arrow[d, dashed, "{R,B}"] \\ w & =_B & w' \end{tikzcd} \quad \exists$$

$\to_{R,B}$ is <u>terminating</u> iff there are no ∞ sequences

$$u_0 \to_{R,B} u_1 \to_{R,B} u_2 \cdots u_n \to_{R,B} u_{n+1} \cdots$$

<u>Lemma</u>. Let $\mathcal{R} = (\Sigma, B, R)$ be strictly B-coherent. Then

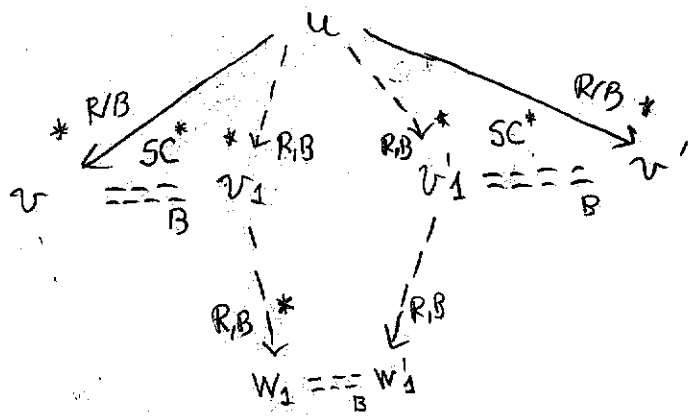
1. $\to_{R,B}$ is confluent iff $\to_{R/B}$ is so
2. $\to_{R,B}$ is terminating iff $\to_{R/B}$ is so

<u>Proof</u>. We will use the following lemma, which has an easy proof by induction on the number n of steps in $\xrightarrow{*}_{R/B}$:

<u>Lemma</u> (SC*) For each $u, u', v \in T_\Sigma(X)$ such that $u =_B u'$ and $u \xrightarrow{*}_{R/B} v$ we have,

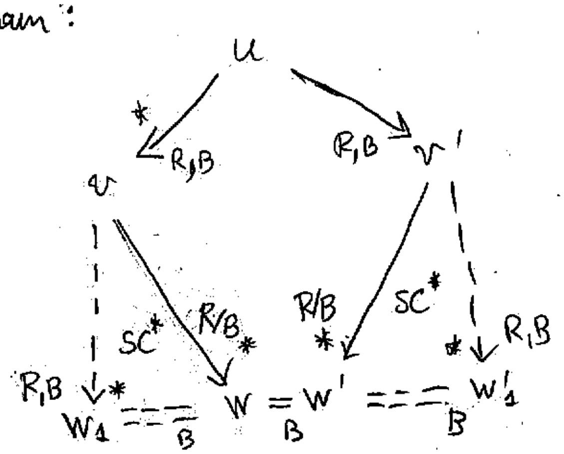
$$(SC^*) \quad \begin{tikzcd} u \arrow[r, "*", "R/B"'] \arrow[d, equal, "B"'] & v \arrow[d, equal, "B"] \\ u' \arrow[r, dashed, "{R,B}"'] & v' \end{tikzcd}$$

To see ($\Rightarrow$) for (1) consider the diagram:



where obviously $v =_B v_1 \xrightarrow[R/B]{*} w_1$ implies $v \xrightarrow[R/B]{*} w_1$, and we likewise have $v' \xrightarrow[R/B]{*} w'_1$, as desired.

To see ($\Leftarrow$) for (1) note that $\rightarrow_{R,B} \subseteq \rightarrow_{R/B}$, then consider the diagram:



To see (2), note that, since $\rightarrow_{R,B} \subseteq \rightarrow_{R/B}$, ($\Leftarrow$) for (2) is trivial. To see ($\Rightarrow$) for (2) assume $\rightarrow_{R,B}$ terminating and $\rightarrow_{R/B}$ non-terminating. Then we get the contradiction:

$$\begin{tikzcd}
u_0 \arrow[r, "R/B"'] \arrow[d, equal, "B"'] \arrow[dr, phantom, "SC"] & u_1 \arrow[r, "R/B"'] \arrow[d, dashed, equal, "B"] & u_2 \arrow[r, "R/B"'] \arrow[d, dashed, equal, "B"] & u_3 \cdots \arrow[d, dashed, equal, "B"] & u_n \arrow[r, "R/B"'] \arrow[d, dashed, equal, "B"] & u_{n+1} \cdots \arrow[d, dashed, equal, "B"] \\
u_0 \arrow[r, dashed, "R,B"'] & u'_1 \arrow[r, dashed, "R,B"'] & u'_2 \arrow[r, dashed, "R,B"'] & u'_3 & u'_n \arrow[r, dashed, "R,B"'] & u'_{n+1} \cdots
\end{tikzcd}$$

and this finishes the proof. □

We will be particularly interested in equational theories $(\Sigma, E \cup B)$ such that provable $E \cup B$-equality becomes decidable by $\vec{E}_{/B}$ rewriting.

Definition (1) A rewrite theory $\mathcal{R} = (\Sigma, B, R)$ is convergent iff (i) it is strictly B-coherent, (ii) $\to_{R,B}$ is confluent, and (iii) $\to_{R,B}$ is terminating.

Notation. For $t \in T_\Sigma(X)$, $t!_{R,B}$ denotes a term (i) it is R,B-irreducible (i.e., $\nexists u$ s.t. $t!_{R,B} \to_{R,B} u$), and (ii) $t \xrightarrow[R,B]{*} t!_{R,B}$. Note that, by confluence, $t!_{R,B}$ is unique up to B-equality.

(2) a rewrite theory $\mathcal{R} = (\Sigma, B, \vec{E})$ with B regular and linear is a decomposition of the equational theory $(\Sigma, E \cup B)$ iff $\mathcal{R}$ is convergent.

The main theorem, making $E \cup B$-equality decidable is:

<u>Church-Rosser Theorem</u>. Let $\mathcal{R} = (\Sigma, B, R)$ be a decomposition of $(\Sigma, E \cup B)$. Then the following are equivalent for $t, t' \in T_\Sigma(X)$

1. $t =_{E \cup B} t'$

2. $t \downarrow_{\vec{E},B} t'$ $\quad$ (i.e., $\exists\, w, w'.\ t \xrightarrow[R,B]{*} w =_B w' \xleftarrow[R,B]{*} t'$)

3. $t!_{\vec{E},B} =_B t'!_{\vec{E},B}$

<u>Proof</u> (1) $\Rightarrow$ (2) follows by induction on n realizing that $=_{E \cup B}$ in the rewrite relation $\xrightarrow[(\vec{E} \cup \overleftarrow{E} \cup \vec{B} \cup \overleftarrow{B})]{*}$, consider the following cases for the $n+1$ step:

(a)

$$\begin{tikzcd}
t \arrow[r, "*", "\vec{E}\cup\overleftarrow{E}\cup\vec{B}\cup\overleftarrow{B}"'] \arrow[d, dashed, "\vec{E},B"', "*"] \arrow[dr, phantom, "\mathrm{I.H.}"] & u \arrow[r, "\overleftarrow{B} \text{ or } \vec{B}"] \arrow[d, dashed, "\vec{E},B"', "*"] \arrow[dr, phantom, "SC^*"] & t' \arrow[d, dashed, "*"', "\vec{E},B"] \\
w \arrow[r, phantom, "=_B"] & w_0 \arrow[r, phantom, "=_B"] & w'
\end{tikzcd}$$

(b)

$$\begin{tikzcd}
t \arrow[r, "*", "\vec{E}\cup\overleftarrow{E}\cup\vec{B}\cup\overleftarrow{B}"'] \arrow[d, dashed, "\vec{E},B *"'] \arrow[dr, phantom, "\mathrm{I.H.}"] & u & t' \arrow[l, "\overleftarrow{E}"'] \\
w \arrow[r, phantom, "=_B"] & w' \arrow[from=u, dashed, "\vec{E},B"', "*"]
\end{tikzcd}$$

since $\to_{\vec{E}} \subseteq \to_{\vec{E},B}$

(c)

$$\begin{tikzcd}
t \arrow[rr, "*", "\vec{E}\cup\overleftarrow{E}\cup\vec{B}\cup\overleftarrow{B}"'] \arrow[d, dashed, "\vec{E},B\,*"'] \arrow[drr, phantom, "\mathrm{I.H.}"] & & u \arrow[rr, "\vec{E}"] \arrow[d, dashed, "\vec{E},B\,*"] \arrow[drr, phantom, "\mathrm{CONF.}"] & & t' \arrow[dd, dashed] \\
v \arrow[rr, equal, dashed, "B"'] \arrow[d, dashed] \arrow[drr, phantom, "SC^*"] & & v_0 \arrow[d, dashed] & & \\
w \arrow[rr, equal, dashed, "B"'] & & w_0 \arrow[rr, equal, dashed, "B"'] & & w'
\end{tikzcd}$$

(2) ⇒ (3)

$$\begin{tikzcd}
t \arrow[d, "\vec{E},B\,*"'] & & & & t' \arrow[d, "*\,\vec{E},B"] \\
w \arrow[rrrr, equal, "B"'] \arrow[d, "\vec{E},B\,*"'] \arrow[drr, phantom, "SC^*"] & & & & w' \arrow[dll, dashed, "\vec{E},B\,*"'] \arrow[d, "*"] \arrow[dl, phantom, "\mathrm{CONF.}"] \\
t!_{\vec{E},B} \arrow[rr, equal, dashed, "B"'] & & u \arrow[rr, equal, dashed, "B"'] & & t'!_{\vec{E},B}
\end{tikzcd}$$

Note that by SC, since $t!_{\vec{E},B}$ is $\vec{E},B$-irred., we have u $\vec{E},B$-irred., forcing $u = t'!_{\vec{E},B}$ by confluence.

(3) ⇒ (1) trivial, since

$$t \xrightarrow[\vec{E},B]{*} t!_{\vec{E},B} =_B t'!_{\vec{E},B} \xleftarrow[\vec{E},B]{*} t'$$

implies $t =_{E\cup B} t'$. □

2. More on B-Unifiers

Certain precisions and hygiene conditions will make it easier to reason about B-unifiers. To begin with, unifiers are irrelevant outside the variables of a system of equations, so we may as well define:

Def. Given (Σ, B) an equational theory, and $\varphi = \bigwedge_{j \in J} u_i = v_j$ a system of Σ-equations, a B-unifier for φ is a substitution $\theta \in [X \to T_\Sigma(X)]$ such that:

(i) $dom(\theta) \subseteq vars(\varphi)$

(ii) $\forall\, j \in J,\quad u_j\theta =_B v_j\theta$

Second, up to renaming of variables a B-unifier θ can always be assumed to be idempotent, in the sense that $dom(\theta) \cap ran(\theta) = \emptyset$, which easily implies the idempotence equation $\theta\theta = \theta$.

Recall the $\sqsupseteq_B$ relation between B-unifiers:

$$\alpha \sqsupseteq_B \beta \quad \text{iff} \quad \exists \rho \ \text{s.t.} \quad \alpha\rho =_B \beta.$$

<u>Lemma</u>. Let θ be a B-unifier of φ. Then there is an idempotent B-unifier γ of φ such that $\theta \sqsupseteq_B \gamma$ and $\gamma \sqsupseteq_B \theta$.

<u>Proof</u> Let $Y = vars(\varphi)$. Let $Y_0 \subseteq Y$ be $Y_0 = dom(\theta)$, $Y_1 = Y - Y_0$, and $Z_0 = ran(\theta)$. Then,

$vars(\varphi\theta) = Y_1 \cup Z_0$. Let $Z = Y_1 \cup Z_0$.

Since we assume an infinite set X of variables we can always choose a set of <u>fresh</u> variables Z' disjoint from $Y \cup Z_0$, and therefore from Z such that there is a <u>bijective renaming of variables</u> $\alpha : Z \xrightarrow{\cong} Z'$. Define $\gamma = \theta\alpha$. Then we have, $dom(\gamma) = Y$, and $ran(\gamma) = Z'$, so $Y \cap Z' = \emptyset$ and γ is idempotent. Furthermore, since $\gamma = \theta\alpha$, γ is a B-unifier, and $\theta \sqsupseteq_B \gamma$. But note that $\gamma\alpha^{-1} = \theta$, so we also have $\gamma \sqsupseteq_B \theta$. $\square$

The above lemma in particular means that without loss of generality we can always assume that all B-unifiers in $\mathrm{Unif}_B(\varphi)$ are idempotent. Also, note that if $\gamma \in \mathrm{Unif}_B(\varphi)$ is idempotent, then $\mathrm{dom}(\gamma) = \mathrm{vars}(\varphi)$.

The following lemma is also useful.

<u>Lemma</u>. Let γ be an idempotent B-unifier of φ, and let θ be a B-unifier of B such that $\gamma \sqsupseteq_B \theta$. Then we can always choose the substitution δ such that $\gamma\delta =_B \theta$ so that $\mathrm{dom}(\delta) \subseteq \mathrm{ran}(\gamma)$.

<u>Proof</u>. In any case we have δ_0 such that $\gamma\delta_0 =_B \theta$. Let $Y = \mathrm{vars}(\varphi) = \mathrm{dom}(\gamma)$, $Z = \mathrm{ran}(\gamma)$. If $\mathrm{dom}(\delta_0) = W$ is such that $W \not\subseteq Z$, let $\delta = \delta_0|_Z$. For each $x \in Y$ we must have $\theta(x) =_B \delta_0(\gamma(x)) = \delta(\gamma(x))$, and for $x \notin Y$, either $x \in \mathrm{dom}(\delta)$, and then $\theta(x) = x =_B \delta_0(\gamma(x)) = \delta_0(x) = \delta(x) = \delta(\gamma(x))$, or $x \in W - \mathrm{dom}(\delta)$, and then

$$\theta(x) = x =_B \delta_0(\gamma(x)) = \delta_0(x) =_B x = \delta(x) = \delta(\gamma(x)),$$

or $x \notin W$ and then $\theta(x) = x = \delta_0(\gamma(x)) = \delta_0(x) = x = \delta(x)$ $= \delta(\gamma(x))$, so that we have $\theta =_B \gamma\delta$, as desired. $\square$

Here is another useful lemma.

<u>Lemma</u>. Let B be regular and linear, and $\mathcal{R} = (\Sigma, B, R)$ strictly coherent and such that $\forall x \in X$, x is R,B-irred (irred. variables). Let θ be an R,B-irreducible substitution (i.e., $\forall x \in X$, $\theta(x)$ is R,B-irreducible). Suppose that there exist γ and δ such that:

1. $\theta =_B \gamma\delta$
2. $dom(\delta) \subseteq ran(\gamma)$

Then both γ and δ are R,B-irreducible.

<u>Proof</u> (i) Suppose there exists $x \in X$ with $\gamma(x) \xrightarrow[R,B]{} u$. Then, by definition of $\xrightarrow[R,B]{}$ it follows that

$$\theta(x) =_B x\gamma\delta \xrightarrow[R,B]{} u\delta$$

, so that, by strict coherence, θ is not R,B-irred.

(ii) Suppose δ is R,B-reducible. By the R,B-irred variables assumption, we must have $x \in dom(\delta)$ such that $\delta(x) \xrightarrow[R,B]{} v$. But by $dom(\delta) \subseteq ran(\gamma)$ there exists $y \in X$ such that $x \in vars(\gamma(y))$, so that $\delta(x)$ is a subterm of $y\gamma\delta$

and therefore $y\gamma\delta$ is R,B-reducible. But, by strong coherence, and $\theta(x) =_B y\gamma\delta$ we then have $\theta(x)$ R,B-reducible, contradicting θ R,B-irred. $\square$