AUTOMATED REASONING

SLIDES 16:

KNUTH BENDIX COMPLETION
Basic steps of Knuth Bendix completion
Aspects of Critical Pair Formation
Knuth Bendix Procedure
Outline of Correctness

KB - AR - 2009

Knuth-Bendix Completion Procedure (Rules 1)

The KB procedure consists of 3 basic steps:
- orient equations to form directed rewrite rules
- form critical pairs and hence new equations
- use the rewrite rules to rewrite terms (and so make them smaller)

These steps can be taken in various combinations.
eg we used all three in our earlier examples of finding new rules in Slides 14.
There are also other steps useful to keep the final rule set streamlined.

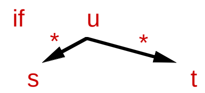
In what follows, R are the rewrite rules and A are equations not yet orientated.

orient equation

A ∪ {s=t} ; R
________________ (Oeq)
A ; R ∪{s =>t}
(or A ; R ∪{t =>s})

find critical pairs

A ; R
________________ (CP)
A ∪ {s=t} ; R



Knuth-Bendix Completion Procedure (Rules 2)

Use of various kinds of Normalisation is implicit in finding critical pairs
(recall that u is rewritten as far as possible into terms s and t)

normalise equation

A ∪ {s = t} ; R
________________ if {t =>* u} (Neq)
A ∪{s = u}; R

normalise rule

A ; R ∪ {s => t}
________________ if {t =>* u} (Nru)
A ; R ∪{s => u}

collapse rule

A ; R ∪ {s => t}
________________ if {s =>* u} (Coll)
A∪{u = t} ; R

remove useless equation

A ∪{s=s} ; R
________________ (Req)
A;R

Examples of using rules (Nru) and (Coll)

normalise rule

A ; R ∪ {s => t}
________________ if {t =>* u} (Nru)
A ; R ∪{s => u}

f(x)=>g(x,x) and g(x,y)=>x yield f(x)=>x by Nru.
(Nru) is similar to transitivity.

collapse rule

A ; R ∪ {s => t}
________________ if {s =>* u} (Coll)
A∪{u = t} ; R

Eg1: (i) f(x) => g(x,x), (ii) f(b)=>c, (iii) b=>a
Since f(b)=>f(a)=>g(a,a), (Coll) gives (iv) g(a,a)=c and removes (ii)
If (iv) orders as g(a,a)=> c, left with (i), (iii), (iv)

Eg2: (i) f(x)=>g(x,x), (ii) f(f(x))=>h(x)
Since f(f(x))=> f(g(x,x)), (Coll) derives f(g(x,x))=h(x) (iii)
If order on (iii) gives f(g(x,x))=>h(x) left with (i) and (iii)

(Coll) is very useful and applies if the critical term is identical to s in rule s=>t

Knuth-Bendix Completion Procedure (Rules 3)

16aiv

remove subsumed equations

$$\frac{A \cup \{s=t,\ u[s\sigma] = u[t\sigma]\}\ ;\ R}{A \cup \{s=t\}\ ;\ R} \quad \text{(Sub)}$$

Example of subsumption: a= b and h(g(a),x) = h(g(b),x)
Of course, equations or rules θ-subsumed by rules can be removed too.
Q: Can equations be used to θ-subsume **rules**?
Hint: consider f(x,y)=f(y,x) and f(b,a)=>f(a,b)

Other kinds of subsumption are possible:
The most useful makes use of (Coll). If the equation that results can be normalised to x=x the original rule will in effect have been eliminated.

eg: Suppose there exist the rules
(1) -0=>0 (2) 0+z=>z (3) -0+z=>z

Apply collapse to (3) using (1): 0+z = z, which then normalises by (Neq) to z=z, which can be removed by (Req)

Knuth Bendix Procedure:

16av

The Knuth Bendix procedure can be presented in several different ways:

(1) As a collection of inference rules that can be applied in any order to a set of equations and rewrite rules;
(2) As an imperative program;
(3) As a corresponding declarative (eg Prolog) program.

In all cases, the procedure takes a set of unorientated equations and, when successful, derives a set of rewrite rules that are confluent. The various steps may be applied in any order, although a fixed sequence of applying the steps of the procedure can be made, as shown on the slides.

There are two unsuccessful outcomes:
(i) the procedure doesn't terminate - always another step can be applied, or
(ii) an equation is derived that cannot be orientated sensibly.
An example of such an equation is x+y = y+x - it is bound to lead to non-termination of a rewriting sequence.

In fact, both undesirable outcomes can still be put to some good use.
In the case of (i), called *divergence*, the rules obtained at a given stage may be adequate to show that the answer to the current problem (is s=*t?) is TRUE; however, an incomplete set of rules cannot be used to show the answer is FALSE.

If an equation E: l=r can't be orientated, then it can be left as an equation and used for rewriting in both directions. The only restriction is this: if an instance lσ=rσ of E is used for rewriting lσ into rσ then lσ > rσ and if used for rewriting rσ into lσ then rσ > lσ.

Knuth Bendix Algorithm (Imperative)

16avi

```
WHILE equations remain in A {
    remove equations that rewrite to x=x
       or are subsumed
    select an equation E
       and remove from A {
          normalise E;              //(Neq)
          orient E;                 //(Oeq)
          normalise RHS. of rules in R
             using and including E;    //(Nru)
          find all critical pairs C of E with R; //(CP)
          add E to R;   add C to A;
          apply (Coll) using E;
       }
  }
```

Often, (Neq), (Nru), (Coll) and (Oeq) are performed on all current equations before finding critical pairs (CP). New equations cause a new sequence of (Neq), (Oeq), (Nru) and (CP). But one at a time may be easier for a person to do.

Outcomes of Knuth Bendix Procedure:

Terminates converges to a confluent set of terminating rewrite rules.

Diverges (and never stops): the confluent set would be infinite.

Fails (and stops): cannot find a termination ordering to orient the rules.

(eg x+y = y+ x causes difficulties.)

Knuth Bendix Algorithm (Declarative)

16avii

Transforms a set of equations X into a confluent set of rewrite rules R.

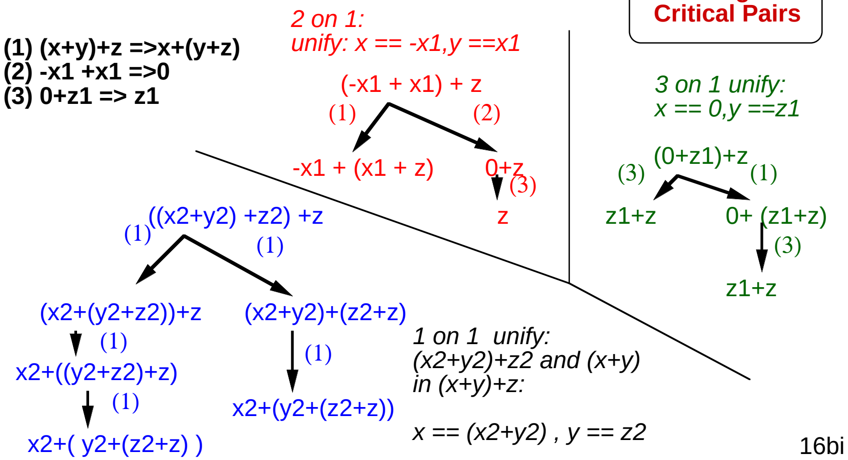
```
kb( [ ],R ).  /*All equations dealt with*/

kb(X,R) :- remove_normalised (X,X1,R), kb(X1,R).

/*remove_normalised succeeds
if an equation in X rewrites to x=x and is removed to leave X1 */

kb(X,R) :- select(A,X,X1), normalise_orient(A,AN,R),
           normalise(AN,R,AN1,R1), superpose(AN1,R1,C),
           app(X1,C,X2),  app(R1,[AN1],R2) ,
           collapse(AN1,R2,R3,X3), app(X3,X2,X4), kb(X4,R3).

/*select finds an axiom A that does not rewrite to x=x and removes it from X
           leaving X1*/
/*normalise_orient uses R to normalise an axiom A and orients A to AN if
possible, else fails  */
/*normalise uses AN to normalise R and itself to R1 and AN1*/
/*superpose finds all critical pairs C from normalised rule AN1 and other
rules R1 if any  */
/*collapse uses AN1 to collapse and removes collapsed rules from R2
leaving R3 and new equations X3*/

/* Initial call is kb( A,[ ] )  */
```

Basic Steps of Knuth Bendix Procedure (Revision)

Finding critical pairs enables new rewrite rules to be formed, which will contribute towards confluence.

Examples of Forming Critical Pairs

(1) (x+y)+z =>x+(y+z)
(2) -x1 +x1 =>0
(3) 0+z1 => z1



Applying the Knuth Bendix Procedure

(1) (x+y)+z => x+(y+z)
(2) -x1 +x1 => 0
(3) 0+z1 => z1
(4) -x1 + (x1+z) => z

There are various options next, but the useful ones are (2) on (4) and (3) on (4) giving (5) and (6).

I leave the rest for you to work out their derivations

(5) --x1+0 => x1
(6) -0+z => z

(7) --0+z => z
(8) -0 => 0

(6) and (7) can be removed using (8) by (Coll)

(9) --x1 + z => x1 + z
(10) x + 0 => x
(11) --x => x

(9) and (5) can be removed using (11) by (Coll)

I think (1), (2), (3), (4), (8), (10), (11) is the final confluent set.

<u>**About forming Critical Pairs:**</u>

A critical pair may occur when a term (the *critical term*) rewrites in two different ways. If the two resulting terms are different and cannot be further rewritten to the same term, the eventually resulting different terms are called the *critical pair*. On Slide 16bi there are 3 examples. The first yields the critical pair (z , -x1+(x1+z)) and the second and third examples do not yield a critical pair. Critical terms arise because the LHSs of two rewrite rules apply to a term ***s*** in two different ways. (It may be just one rule involved in different places.) This can happen in essentially three ways.

(a) One way is when the parts of ***s*** being rewritten do not overlap. This way will not yield a critical pair (see 16bv, case 1): if a term ***s*** can be rewritten in two ways, but by rewriting two non-overlapping terms, then this will not be because the LHSs of the rules overlap. The two steps can be applied separately. If θ is the substitution applied to rule 1 and σ the substitution applied to rule 2, then ***s*** can be written as s[LHS1θ, LHS2σ], which rewrites into s[RHS1θ, LHS2σ] or s[LHS1θ, RHS2σ] and then into s[RHS1θ, RHS2σ].

(b) Otherwise, the LHSs themselves must "overlap" or can be superposed. That is, either LHS1 and LHS2 unify, or LHS1 unifies with a subterm of LHS2 (or vice versa). There are two different ways in which this can occur, only one of which is useful. If the LHSs of the two rules overlap on a variable subterm ***x*** – ie LHS1 unifies with a variable x in LHS2 with substitution θ, then the critical term is the instance LHS2θ of LHS2; although LHS2θ rewrites to 2 different terms, these can always be rewritten to a common term: LHS2θ, rewrites into RHS2θ (by rule 2) and also into LHS2θ' by rule 1, where θ' is the substitution x==RHS1. Both of these rewrite into RHS2θ', the first by rule 1 and the second by rule 2. You should draw a diagram to convince yourself that this is so. Case 2 on 16bv illustrates this. Note that if ***x*** does not occur in RHS2 then RHS2θ is the same as RHS2θ'.

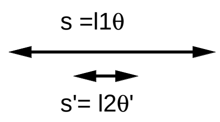
(Continued on Slide 16biv.)

(c) ***s*** rewrites in 2 different ways by rules that overlap on a non-variable sub-term of ***s***. In case the LHS of the two rules also overlap on a non-variable sub-term (see below). (This is illustrated in Case 3 on 16bv).

s matches l1
s' in s[s'] matches l2

(l1 => r1)
(l2 => r2)

i.e. l2 and a subterm of l1 have a common instance.
Hence ∃σ: l2σ is a subterm of l1σ.



s=l1θ, s' = l2θ'
and s' is not in a variable position in l1θ

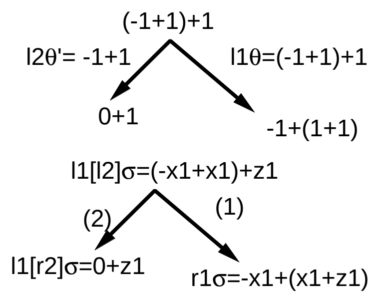
So l1[l2σ]σ rewrites (by 1) to r1σ and (by 2) to l1[r2σ]σ

<u>**Exercise**</u>: identify θ,θ',σ in the following:

Use (x+y)+z => x+(y+z) (1)
and -x1+x1 =>0 (2)

s=(-1+1)+1 matches with l1 and s' = (-1+1)
s rewrites to 0+1 (by 2)
and to -1+(1+1) (by 1)

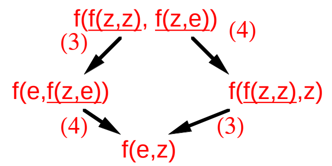
θ' is {x1==1}, θ is{x==-1, y==1, z==1}
and σ is {x==-x1, y==x1}



Formation of critical pairs - possibilities for non-confluence 16bv

Case 1: non-overlapping occurrences: can rewrite occurrences in turn and can write to a common term.

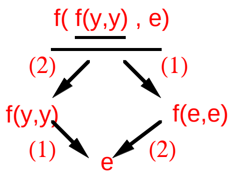
3. f(y,y) => e   4. f(x,e) => x



s = f(f(z,z), f(z,e))
can be rewritten by 3 and 4:
θ (for 3) = {y==z}; σ (for 4) = {x==z}
s = f(LHS3θ, LHS4σ)
=> (by 3) f(RHS3θ, LHS4σ)
or (by 4) f(LHS3θ, RHS4σ)
=> f(RHS3θ, RHS4σ) (by 4, or by 3)

Case 2: Rules apply such that they *overlap on a variable subterm* - can also rewrite to a common term.

1. f(y,y) => e
2. f(x,e) => x



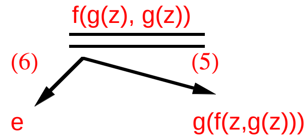
s = f(f(y,y), e)
can be rewritten by 1 and 2
(they overlap on variable x in f(x,e))
θ (for 2) = {x==f(y,y)}
s = LHS2θ => (by 2) RHS2θ
or (by 1) LHS2θ' (θ' = {x==e})
=> RHS2θ' (by 1, or by 2)

Formation of critical pairs - possibilities for non-confluence

Case 3: rules apply such that they overlap on a **non-variable** subterm

- **Only need to check occurrences of Case 3 for possible non-confluence.**
- **All necssary critical pairs can be found by unifying the LHS of rules with *non-variable* subterms of other LHS and rewriting as far as possible (first using overlapping rules, then maybe other rules)**

5. f(g(x),y1) =>g(f(x,y1))
6. f(y2,y2) => e



(Note: g(f(z,g(z))) does *not* rewrite by 5, since to do so would require *narrowing* z to g(x1))

(Using notation of 16biii)

l1[l2σ]σ = f(g(z) , g(z))
l2σ = f(g(z) , g(z))
σ = {x==z, y1==g(z), y2==g(z)}

l1[l2σ]σ rewrites (by 5) to
r1σ = g(f(z,g(z)))

and (by 6) to l1[r2σ]σ = l1[e] = e
since the context of l1 in which l2 is embedded is {}

16bvi

Correctness of Knuth Bendix Rules (Bachmair) 16ci

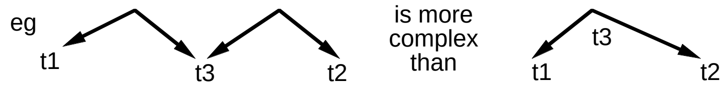
- The inference rule approach allows logic and control to be separated
- Invariant properties can be found that imply confluence on termination.

- A derivation using the inference rules has the form: (A0,R0) , (A1,R1) , ….
- Because of subsumption and Collapse some rules may not remain forever.
- A *persistent rule* is one that occurs in Ri and remains in Rj, $\forall$j$\geq$i.
- R∞ = {persistent rules}   [formally = $\cup$(i$\geq$0) ($\cap$(j$\geq$i)Rj)]
- Aim is for R∞ to be canonical -
  any equation valid in (A0,R0) = (A0,{}) has a rewrite proof in R∞.

- We define $\Leftrightarrow$A$\cup$R by (u,v) $\in$ $\Leftrightarrow$A$\cup$R iff (A,R) |= u=v
  $\Leftrightarrow$A$\cup$R is obtained by using A and R together and treating R as equations.
  $\Leftrightarrow$A$\cup$R is an equivalence relation on terms;
  (Exercise: Show $\Leftrightarrow$A$\cup$R is an equivalence relation)

- Invariant of procedure: For each i, (Ai, Ri) and (Ai+1, Ri+1) are related:
  $\Leftrightarrow$Ai$\cup$Ri = $\Leftrightarrow$Ai+1 $\cup$ Ri+1
- Ensures that (A0,{}) |= u=v iff ({}, R∞) |= u=v
  i.e. no proofs (possibly with peaks) have been lost or gained.

- **Idea of the proof**: to show R∞ is confluent must show that rewrite proofs using derivation (Aj ,Rj) are “less complex” than those using (Ai,Ri), i<j



- A *non-rewrite-only* proof uses equations as well as rewrite rules
- Turning an equation into a rewrite rule may mean it is used 'backwards' in a proof
- Generating critical pairs allows for new rewrite rules to be added which will smooth out a proof (ie remove a peak or two)
- *Fairness* is required so that equations cannot be ignored for ever
- All critical pairs will eventually be formed
- Any proof eventually becomes a rewrite proof as proofs decrease in complexity as rewrite rules are formed from equations.

Problems:

- The KB algorithm can fail because a selected equation cannot be oriented or because R∞ is not finite.
- It may be possible to try a different ordering, or may still be able to use rewrites generated so far to show s=t .

16cii

Summary of Slides 16

1. The Knuth Bendix procedure can be described using an imperative or declarative program, or by a set of inference rules. The main operations are orient, find critical pairs and normalise.

2. It is only necessary to search for overlapping of the LHS of rules in order to find all possible terms that could lead to a critical pair. Overlapping onto a variable is not necessary.

3. Normalising is the operation that applies rewrite rules to other rules or equations. It can be applied to rewrite rules (the RHS), or to equations (either side).

4. The operation of removing useless equations (they rewrite to s=s), or subsumed equations (they are implied by other equations or rules) is helpful.

5. The Knuth Bendix procudeure can terminate, diverge (non-terminating), or fail (an equation can't be oriented – eg x+y=y+x).

6. The Knuth Bendix procedure is correct - when it terminates the final set of rules is confluent and terminating. The proof method shows that the procedure does not remove any proofs, but each proof becomes more like a rewrite proof as each new rewrite rule is generated.