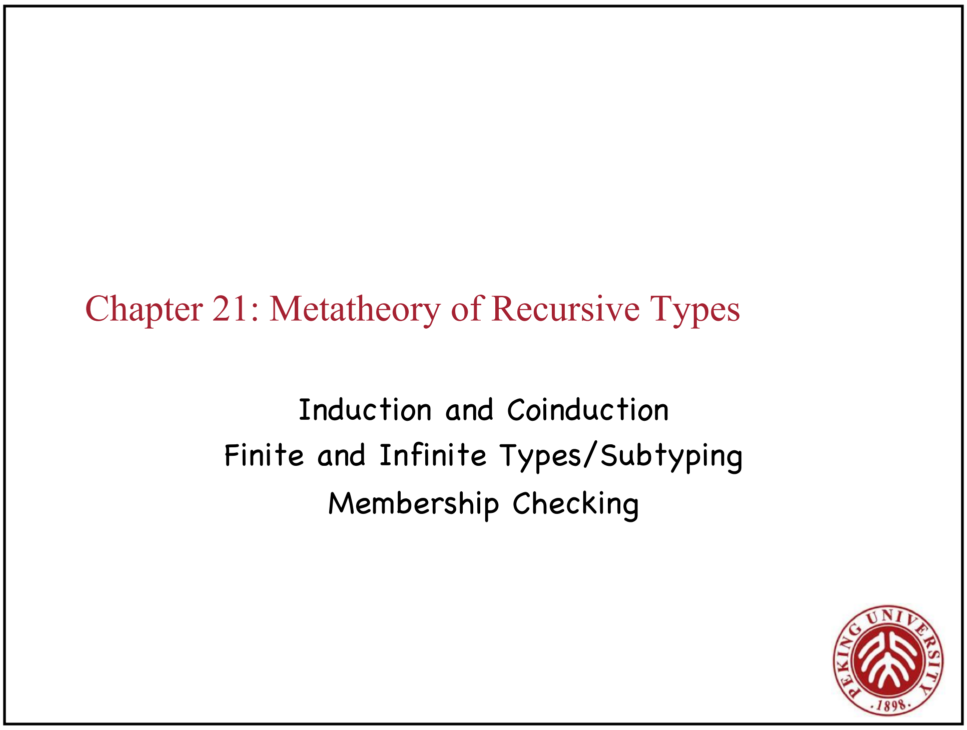
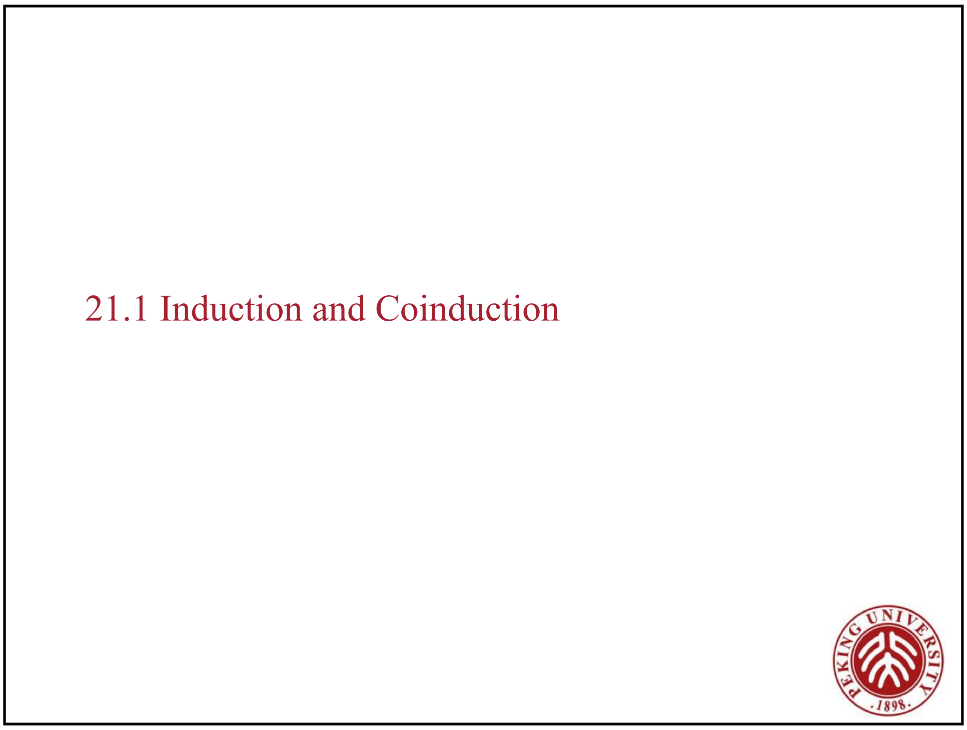


Chapter 21: Metatheory of Recursive Types

Induction and Coinduction

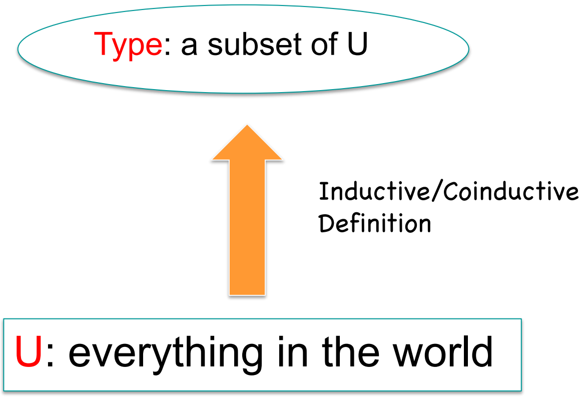
Finite and Infinite Types/Subtyping

Membership Checking



21.1 Induction and Coinduction

Universal Set U



Type: a subset of U

Inductive/Coinductive Definition

U: everything in the world

Generating Function

- Definition: A function F ∈ P(U) → P(U) is monotone if X ⊆ Y implies F(X) ⊆ F(Y).
- Definition: Let F be monotone, and X be a subset of U.
  - X is F-closed if F(X) ⊆ X.
  - X is F-consistent if X ⊆ F(X).
  - X is a fixed point of F if F(X) = X.

Exercise: Consider the following generating function on the three-element universe U={a, b, c}:

E1(∅) = {c}
E1({a}) = {c}
E1({b}) = {c}
E1({c}) = {b, c}
E1({a,b}) = {c}
E1({a, c}) = {b, c}
E1({b, c}) = {a, b, c}
E1({a, b, c}) = {a, b, c}

$$\frac{}{c} \qquad \frac{c}{b} \qquad \frac{b \quad c}{a}$$

Q: Which subset is E1-closed, E1-consistent?

Knaster-Tarski Theorem (1955)

Theorem

- The intersection of all F-closed sets is the least fixed point of F.
- The union of all F-consistent sets is the greatest fixed point of F.

Definition: The least fixed point of F is written μF. The greatest fixed point of F is written νF.

Exercise: Consider the following generating function on the three-element universe U={a, b, c}:

E1(∅) = {c}
E1({a}) = {c}
E1({b}) = {c}
E1({c}) = {b, c}
E1({a,b}) = {c}
E1({a, c}) = {b, c}
E1({b, c}) = {a, b, c}
E1({a, b, c}) = {a, b, c}

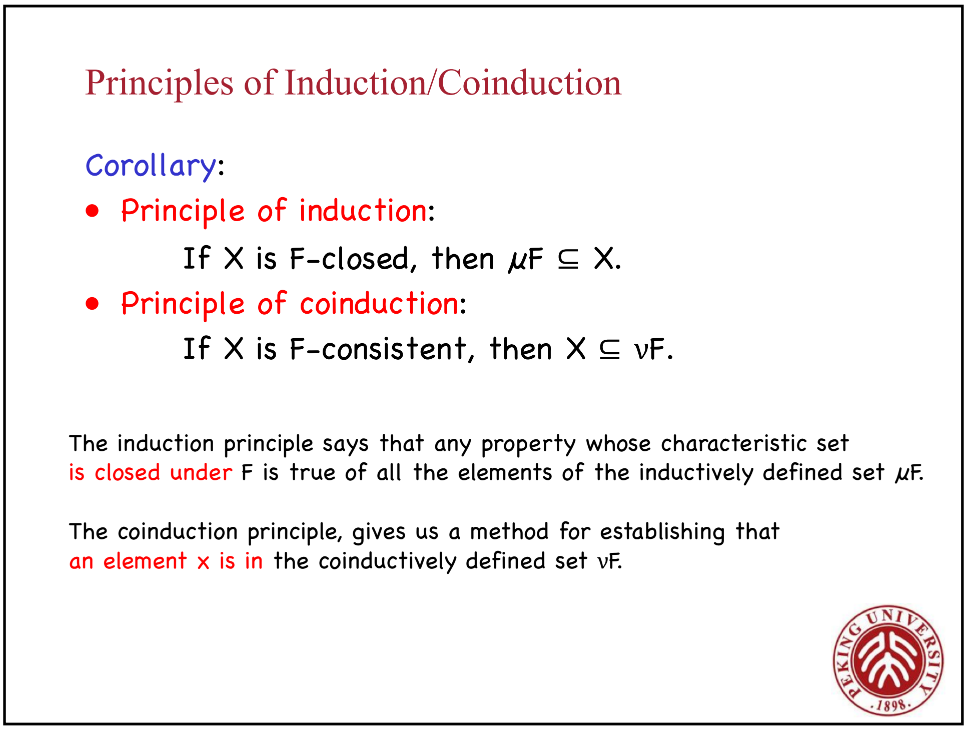
$$\frac{}{c} \qquad \frac{c}{b} \qquad \frac{b \quad c}{a}$$

Q: What are μE1 and νE1?

Exercise: Suppose a generating function E2 on the universe {a, b, c} is defined by the following inference rules:

$$\frac{}{a} \qquad \frac{c}{b} \qquad \frac{a \quad b}{c}$$

Q: Write out the set of pairs in the relation E2 explicitly, as we did for E1 above. List all the E2-closed and E2-consistent sets. What are μE2 and νE2?



Principles of Induction/Coinduction

Corollary:

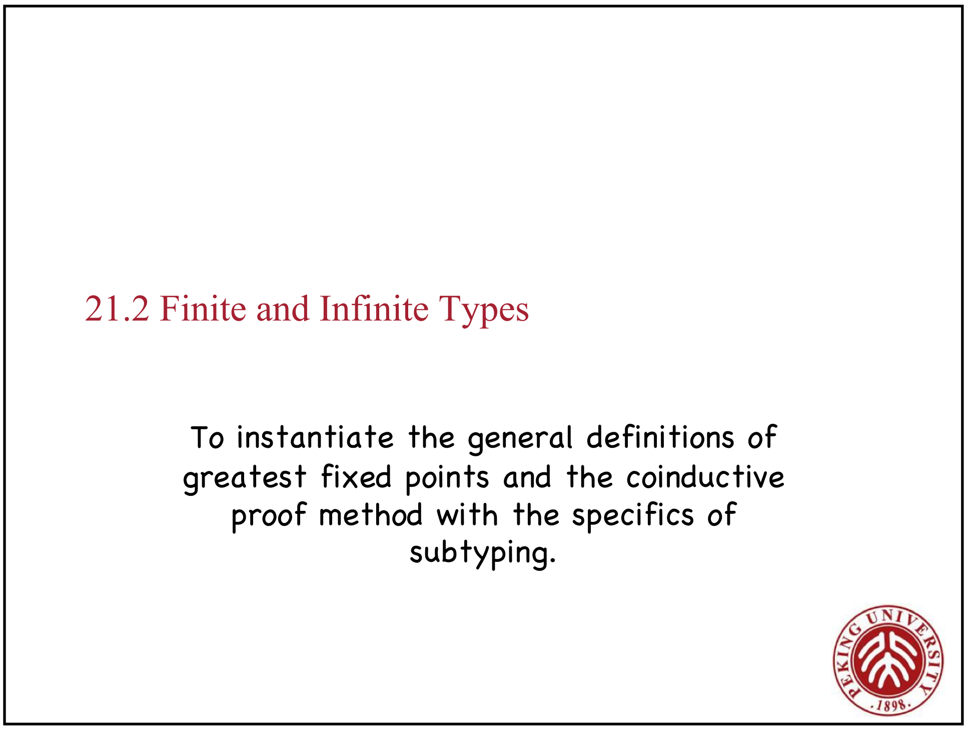
- Principle of induction:

  If X is F-closed, then $\mu F \subseteq X$.
- Principle of coinduction:

  If X is F-consistent, then $X \subseteq \nu F$.

The induction principle says that any property whose characteristic set is closed under F is true of all the elements of the inductively defined set μF.

The coinduction principle, gives us a method for establishing that an element x is in the coinductively defined set νF.



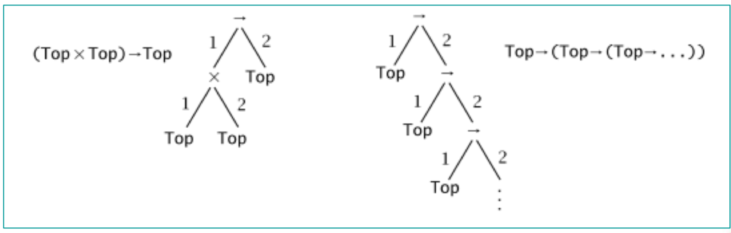
21.2 Finite and Infinite Types

To instantiate the general definitions of greatest fixed points and the coinductive proof method with the specifics of subtyping.

Tree Type

Definition: A tree type (or, simply, a tree) is a partial function $T \in \{1,2\}* \rightharpoonup \{\rightarrow, \times, Top\}$ satisfying the following constraints:

- T(•) is defined;
- if T(π,σ) is defined then T(π) is defined;
- if T(π) =→ or T(π) = × then T(π,1) and T(π,2) are defined;
- if T(π) = Top then T(π,1) and T(π,2) are undefined.



Definition: A tree type T is finite if dom(T) is finite. The set of all tree types is written $\mathcal{T}$; the subset of all finite tree types is written $\mathcal{T}_f$.

Exercise: Give a universe U and a generating function F ∈ P(U) → P(U) such that the set of finite tree types $\mathcal{T}_f$ is the least fixed point of F and the set of all tree types $\mathcal{T}$ is its greatest fixed point.

21.3 Subtyping

Finite Subtyping

Definition: Two finite tree types S and T are in the subtype relation ("S is a subtype of T") if $(S,T) \in \mu S_f$, where the monotone function

$$S_f \in P(\mathcal{T}_f \times \mathcal{T}_f) \to P(\mathcal{T}_f \times \mathcal{T}_f)$$

is defined by

$$\begin{aligned} S_f(R) = {} & \{ (T,Top) \mid T \in \mathcal{T}_f \} \\ & \cup \{ (S1\times S2,\ T1\times T2) \mid (S1,T1),\ (S2,T2) \in R\} \\ & \cup \{ (S1\to S2,\ T1\to T2) \mid (T1,S1),\ (S2,T2) \in R\}. \end{aligned}$$

Inference Rules

$$T <: Top$$

$$\frac{S1 <: T1 \quad S2 <: T2}{S1 \times S2 <: T1 \times T2}$$

$$\frac{T1 <: S1 \quad S2 <: T2}{S1 \to S2 <: T1 \to T2}$$

Infinite Subtyping

Definition: Two (finite or infinite) tree types S and T are in the subtype relation (“S is a subtype of T”) if $(S,T) \in \nu S$, where the monotone function

$$S \in P(\mathcal{T} \times \mathcal{T}) \to P(\mathcal{T} \times \mathcal{T})$$

is defined by

$$\begin{aligned} S(R) = {} & \{(T, Top) \mid T \in \mathcal{T}\} \\ & \cup \{(S1 \times S2, T1 \times T2) \mid (S1,T1), (S2,T2) \in R\} \\ & \cup \{(S1 \to S2, T1 \to T2) \mid (T1,S1), (S2,T2) \in R\}. \end{aligned}$$

Inference Rules

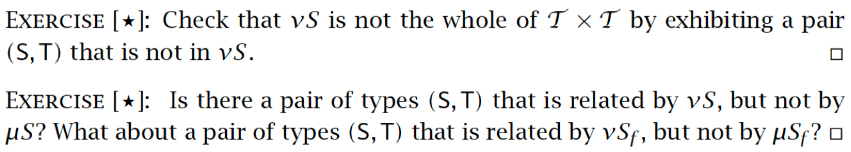
T <: Top

S1 <: T1   S2 <: T2

S1×S2 <: T1×T2

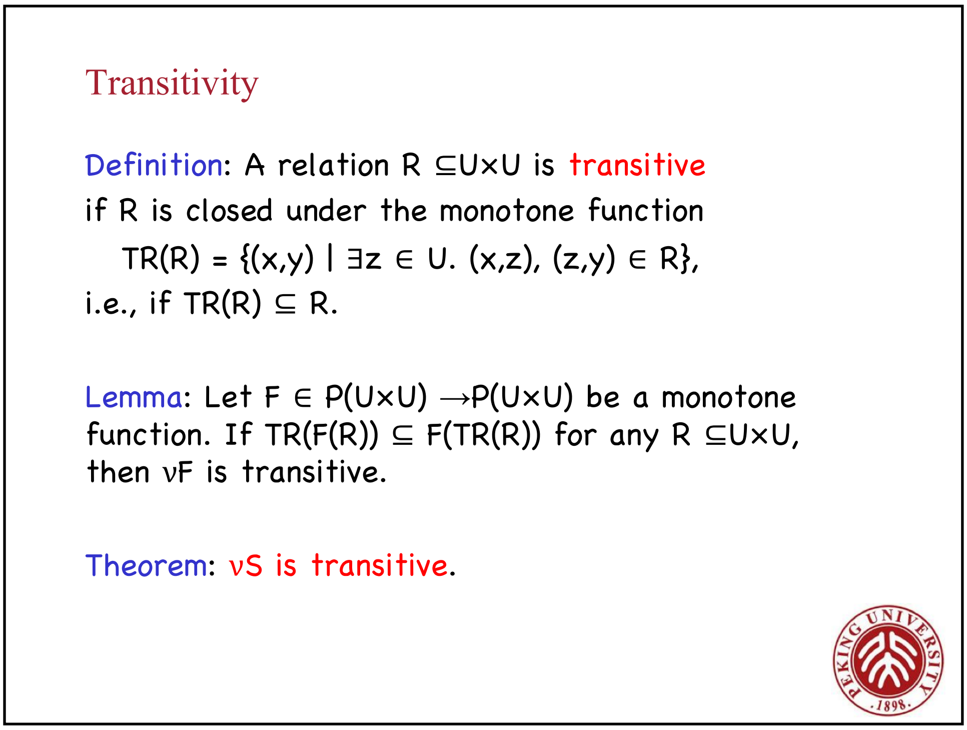
T1 <: S1 S2 <: T2

S1→S2 <: T1→T2



EXERCISE [★]: Check that νS is not the whole of $\mathcal{T} \times \mathcal{T}$ by exhibiting a pair (S, T) that is not in νS. □

EXERCISE [★]: Is there a pair of types (S, T) that is related by νS, but not by μS? What about a pair of types (S, T) that is related by νS_f, but not by μS_f? □



Transitivity

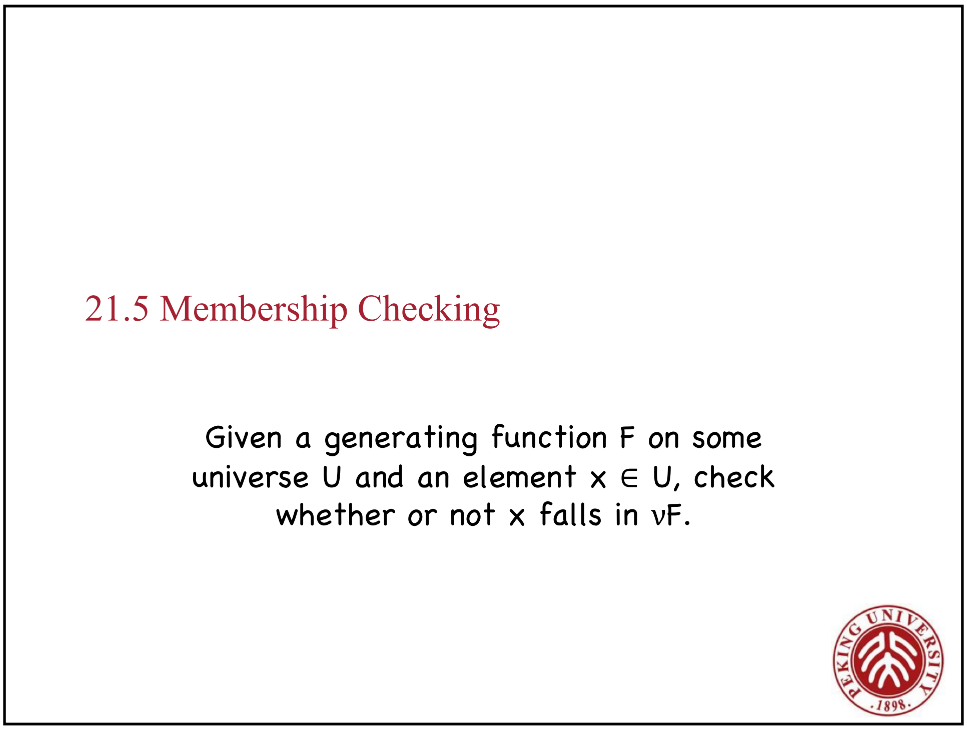
Definition: A relation $R \subseteq U\times U$ is transitive if R is closed under the monotone function

$TR(R) = \{(x,y) \mid \exists z \in U.\ (x,z), (z,y) \in R\}$,

i.e., if $TR(R) \subseteq R$.

Lemma: Let $F \in P(U\times U) \to P(U\times U)$ be a monotone function. If $TR(F(R)) \subseteq F(TR(R))$ for any $R \subseteq U\times U$, then νF is transitive.

Theorem: νS is transitive.



21.5 Membership Checking

Given a generating function F on some universe U and an element $x \in U$, check whether or not x falls in νF.

Invertible Generating Function

Definition: A generating function F is said to be invertible if, for all x ∈ U, the collection of sets

$$G_x = \{X \subseteq U \mid x \in F(X)\}$$

either is empty or contains a unique member that is a subset of all the others.

We will consider invertible generating function in the rest of this chapter.

F-Supported/F-Ground

When F is invertible, we define:

$$support_F(x) = \begin{cases} X & \text{if } X \in G_x \text{ and } \forall X' \in G_x.\ X \subseteq X' \\ \uparrow & \text{if } G_x = \varnothing \end{cases}$$

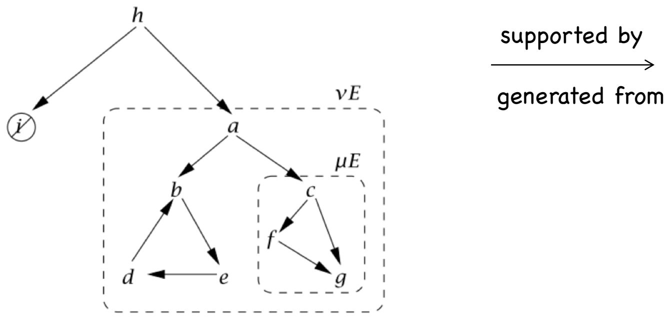
$$support_F(X) = \begin{cases} \bigcup_{x \in X} support_F(x) & \text{if } \forall x \in X.\ support_F(x)\downarrow \\ \uparrow & \text{otherwise} \end{cases}$$

Definition: An element x is F-supported if $support_F(x)\downarrow$; otherwise, x is F- unsupported. An F-supported element is called F-ground if $support_F(x) = \emptyset$.

Exercise: What is $support_S(x)$?

Support Graph

- An Example of the support graph of E function on {a,b,c,d,e,f,g,h,i}



x is in the greatest fixed point iff no unsupported element is reachable from x in the support graph.

Greatest Fixed Point

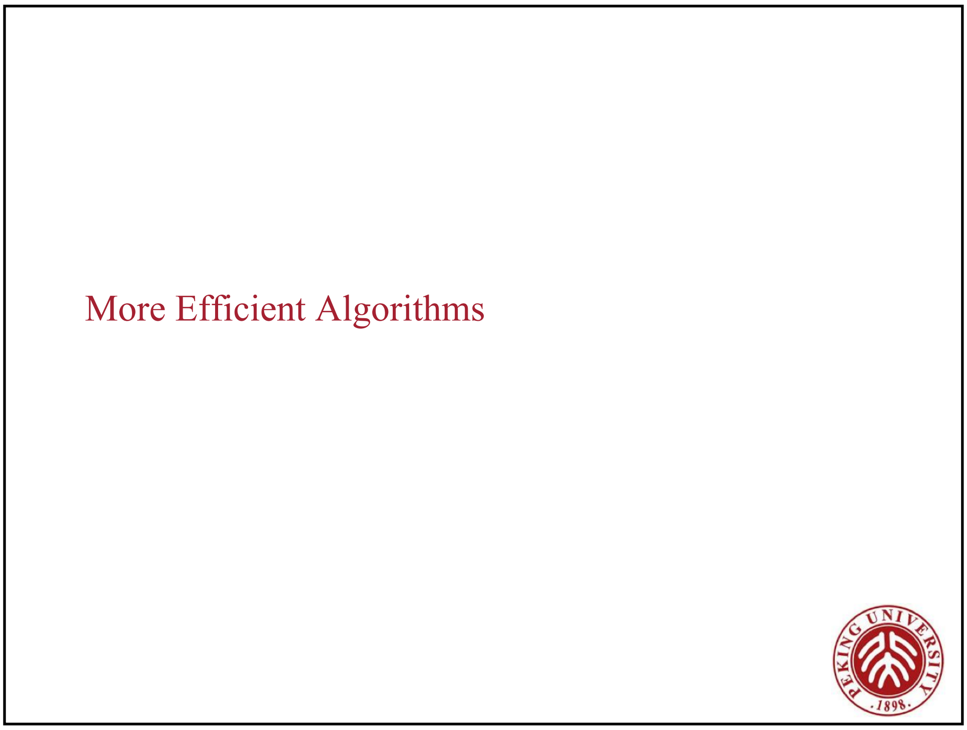
Definition: Suppose F is an invertible generating function. Define the Boolean-valued function gfp_F (or just gfp) as follows:

$$\begin{aligned} gfp(X) \quad = \quad & \text{if } support(X)\uparrow, \text{ then } false \\ & \text{else if } support(X) \subseteq X, \text{ then } true \\ & \text{else } gfp(support(X) \cup X). \end{aligned}$$

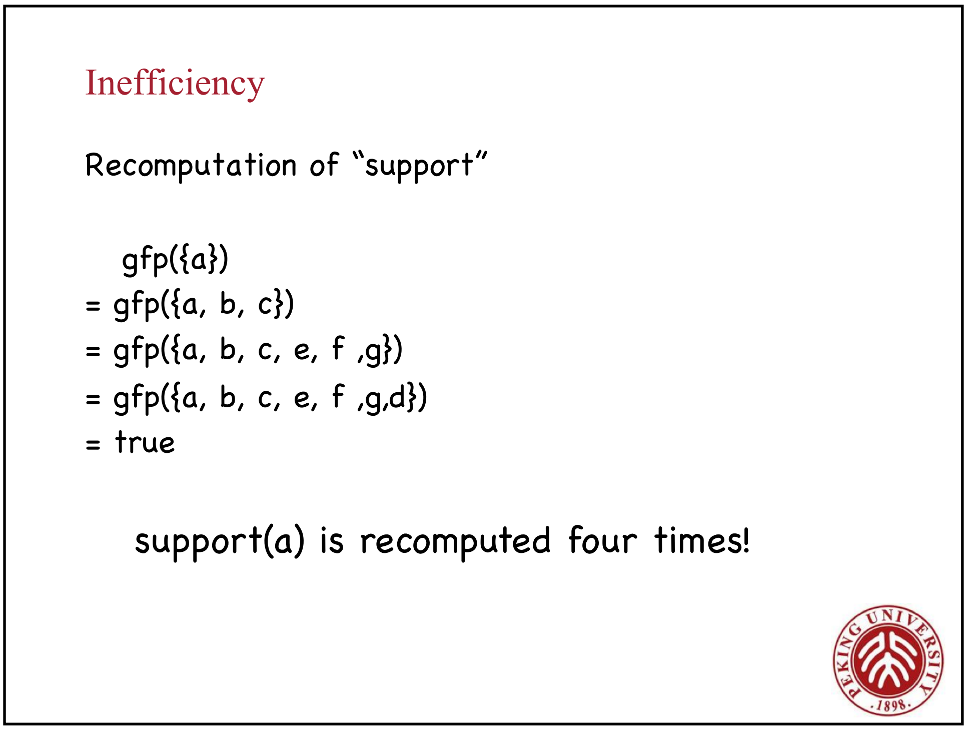
Theorem (Sound):

1. If $gfp_F(X)$ = true, then $X \subseteq \nu F$.
2. 2If $gfp_F(X)$ = false, then $X \not\subseteq \nu F$.

Theorem (Terminate): If $reachable_F(X)$ is finite, then $gfp_F(X)$ is defined. Consequently, if F is finite state, then $gfp_F(X)$ terminates for any finite $X \subseteq U$.



More Efficient Algorithms



Inefficiency

Recomputation of “support”

```
   gfp({a})
= gfp({a, b, c})
= gfp({a, b, c, e, f ,g})
= gfp({a, b, c, e, f ,g,d})
= true
```

support(a) is recomputed four times!

A More Efficient Algorithm

Definition: Suppose F is an invertible generating function. Define the function gfp^a as follows

$$\begin{aligned} gfp^a(A,X) \;=\; & \text{if } support(X)\uparrow\text{, then } false \\ & \text{else if } X=\varnothing\text{, then } true \\ & \text{else } gfp^a(A\cup X,\; support(X)\setminus(A\cup X)). \end{aligned}$$

Tail-recursion

Example:

$$\begin{aligned} & gfp^a(\varnothing,\ \{a\}) \\ = \; & gfp^a(\{a\},\ \{b,c\}) \\ = \; & gfp^a(\{a,b,c\},\ \{e,f,g\}) \\ = \; & gfp^a(\{a,b,c,e,f,g\},\ \{d\}) \\ = \; & gfp^a(\{a,b,c,e,f,g,d\},\ \varnothing) \\ = \; & true. \end{aligned}$$

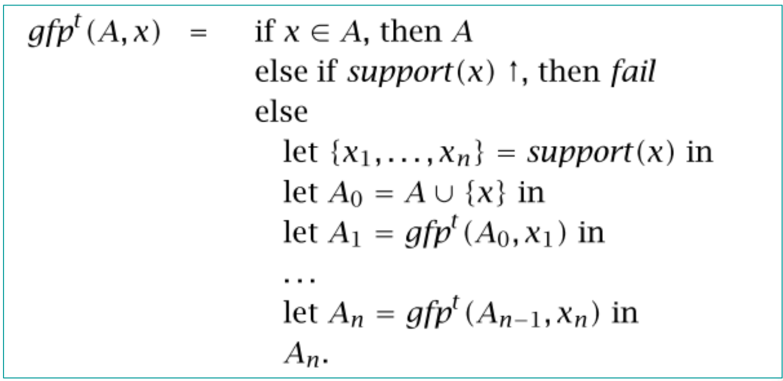
Variation 1

Definition: A small variation on gfp^s has the algorithm pick just one element at a time from X and expand its support. The new algorithm is called gfp^s

```
$gfp^s(A,X)$  =  if $X=\varnothing$, then $true$
                 else let $x$ be some element of $X$ in
                     if $x \in A$ then $gfp^s(A,\ X\setminus\{x\})$
                     else if $support(x)\uparrow$ then $false$
                     else $gfp^s(A\cup\{x\},\ (X\cup support(x))\setminus(A\cup\{x\}))$.
```

Variation 2

Definition: Given an invertible generating function F, define the function gfp^t as follows:



```
$gfp^t(A,x)$  =  if $x \in A$, then $A$
                 else if $support(x)\uparrow$, then $fail$
                 else
                    let $\{x_1,\ldots,x_n\} = support(x)$ in
                    let $A_0 = A \cup \{x\}$ in
                    let $A_1 = gfp^t(A_0,x_1)$ in
                    $\ldots$
                    let $A_n = gfp^t(A_{n-1},x_n)$ in
                    $A_n$.
```

Regular Trees

If we restrict ourselves to regular types, then the sets of reachable states will be guaranteed to remain finite and the subtype checking algorithm will always terminate.

Regular Trees

Definition: A tree type S is a subtree of a tree type T if $S = \lambda\sigma.\ T(\pi,\sigma)$ for some π.

Definition: A tree type $T \in T$ is regular if subtrees(T) is finite.

Examples:

- Every finite tree type is regular.
- T = Top x (Top x (Top x ...)) is regular.
- T = B x (A x (B x (A x (A x (B x (A x (A x (A x (B ...) is irregular.

Proposition: The restriction of the generating function S to regular tree types is finite state.

Proof: We need to show that for any pair (S,T) of regular tree types, the set reachable(S,T) is finite. Since reachable $(S,T) \subseteq$ subtrees(S) $\times$subtrees(T); the latter is finite as S and T are regular.

μ-Types

Establishes the correspondence between subtyping on μ-expressions and the subtyping on tree types

μ-Types:

Definition: Let X range over a fixed countable set {X1,X2,...} of type variables. The set of raw μ-types is the set of expressions defined by the following grammar:

$$
\begin{array}{lll}
T & ::= & X \\
 & & \mathrm{Top} \\
 & & T \times T \\
 & & T \to T \\
 & & \mu X.T
\end{array}
$$

$\mathcal{T}_m$

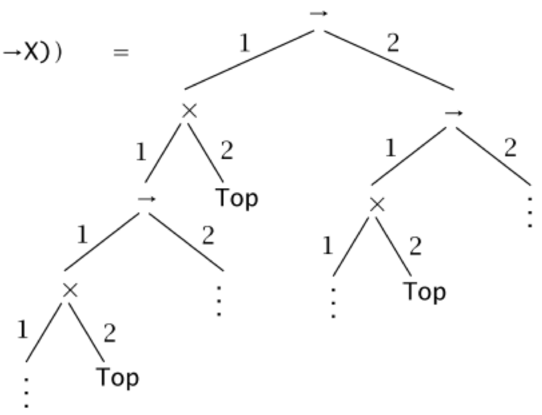
Definition: A raw μ-type T is contractive (and called μ-types) if, for any subexpression of T of the form $\mu X.\mu X1 \ldots \mu Xn.S$, the body S is not X.

Finite Notation for Infinite Tree Types

Definition: The function treeof , mapping closed μ-types to tree types, is defined inductively as follows:

$$
\begin{array}{lcl}
\mathit{treeof}(\mathsf{Top})(\bullet) & = & \mathsf{Top} \\[6pt]
\mathit{treeof}(\mathsf{T}_1 \to \mathsf{T}_2)(\bullet) & = & \to \\
\mathit{treeof}(\mathsf{T}_1 \to \mathsf{T}_2)(i,\pi) & = & \mathit{treeof}(\mathsf{T}_i)(\pi) \\[6pt]
\mathit{treeof}(\mathsf{T}_1 \times \mathsf{T}_2)(\bullet) & = & \times \\
\mathit{treeof}(\mathsf{T}_1 \times \mathsf{T}_2)(i,\pi) & = & \mathit{treeof}(\mathsf{T}_i)(\pi) \\[6pt]
\mathit{treeof}(\mu\mathsf{X}.\mathsf{T})(\pi) & = & \mathit{treeof}([\mathsf{X} \mapsto \mu\mathsf{X}.\mathsf{T}]\mathsf{T})(\pi)
\end{array}
$$

$\mathit{treeof}(\mu\mathsf{X}.((\mathsf{X} \times \mathsf{Top}) \to \mathsf{X}))$ =



Subtyping Correspondence: μ-Types and Tree Types

Definition: Two μ-types S and T are said to be in the subtype relation if $(S,T) \in \nu S_m$, where the monotone function $S_m \in P(\mathcal{T}_m \times \mathcal{T}_m) \to P(\mathcal{T}_m \times \mathcal{T}_m)$ is defined by:

$$\begin{array}{rcl} S_m(R) & = & \{(S, Top) \mid S \in \mathcal{T}_m\} \\ & \cup & \{(S_1 \times S_2, T_1 \times T_2) \mid (S_1, T_1),\ (S_2, T_2) \in R\} \\ & \cup & \{(S_1 \to S_2, T_1 \to T_2) \mid (T_1, S_1),\ (S_2, T_2) \in R\} \\ & \cup & \{(S, \mu X.T) \mid (S, [X \mapsto \mu X.T]T) \in R\} \\ & \cup & \{(\mu X.S, T) \mid ([X \mapsto \mu X.S]S, T) \in R,\ T \neq Top, \text{ and } T \neq \mu Y.T_1\}. \end{array}$$

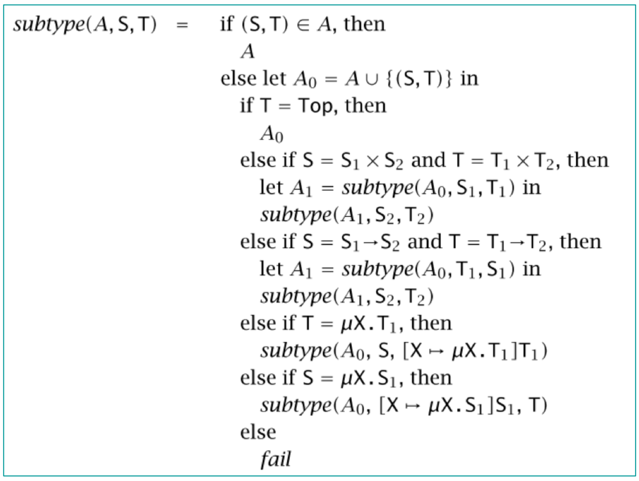
Theorem: Let $(S,T) \in \mathcal{T}_m \times \mathcal{T}_m$. Then $(S,T) \in \nu S_m$ iff (treeof S, treesof T) $\in \nu S$.

Exercise: What is the support for S_m?

$$support_{S_m}(S,T) = \begin{cases} \varnothing & \text{if } T = Top \\ \{(S_1, T_1),\ (S_2, T_2)\} & \text{if } S = S_1 \times S_2 \text{ and} \\ & \quad T = T_1 \times T_2 \\ \{(T_1, S_1),\ (S_2, T_2)\} & \text{if } S = S_1 \to S_2 \text{ and} \\ & \quad T = T_1 \to T_2 \\ \{(S, [X \mapsto \mu X.T_1]T_1)\} & \text{if } T = \mu X.T_1 \\ \{([X \mapsto \mu X.S_1]S_1, T)\} & \text{if } S = \mu X.S_1 \text{ and} \\ & \quad T \neq \mu X.T_1,\ T \neq Top \\ \uparrow & \text{otherwise.} \end{cases}$$

Subtyping Algorithm for μ-Types

Instantiating gfp† for subtyping relation on μ-Types.

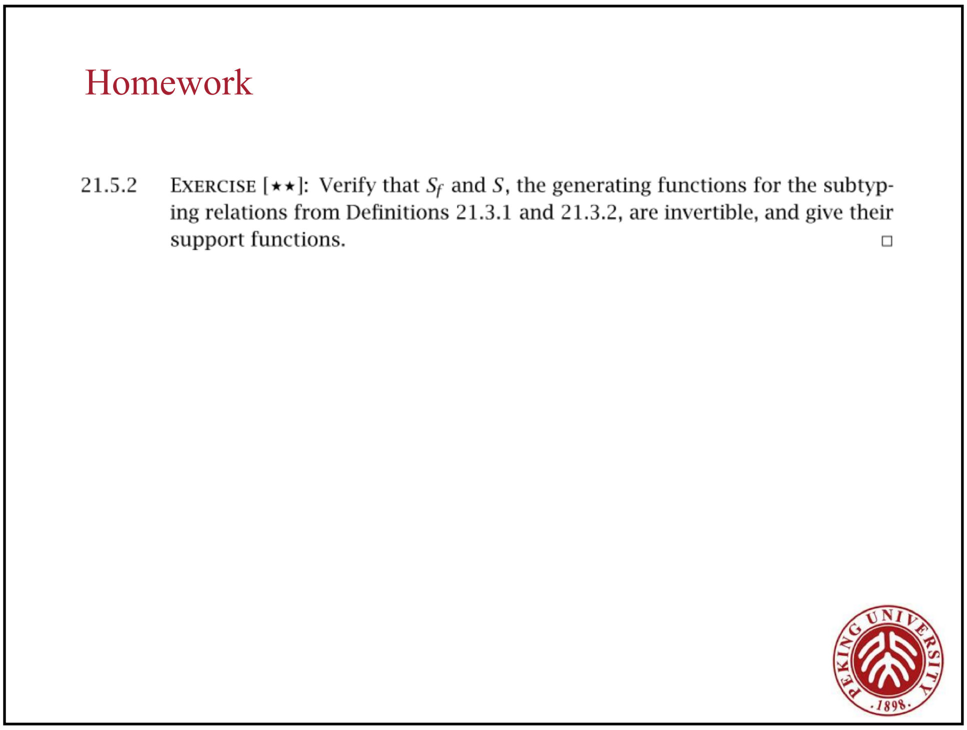


```
subtype(A, S, T)  =  if $(S,T) \in A$, then
                       $A$
                     else let $A_0 = A \cup \{(S,T)\}$ in
                       if $T = Top$, then
                         $A_0$
                       else if $S = S_1 \times S_2$ and $T = T_1 \times T_2$, then
                         let $A_1 = subtype(A_0, S_1, T_1)$ in
                         $subtype(A_1, S_2, T_2)$
                       else if $S = S_1 \to S_2$ and $T = T_1 \to T_2$, then
                         let $A_1 = subtype(A_0, T_1, S_1)$ in
                         $subtype(A_1, S_2, T_2)$
                       else if $T = \mu X.T_1$, then
                         $subtype(A_0, S, [X \mapsto \mu X.T_1]T_1)$
                       else if $S = \mu X.S_1$, then
                         $subtype(A_0, [X \mapsto \mu X.S_1]S_1, T)$
                       else
                         fail
```

Terminate?

Summary

- We study the theoretical foundation of type checkers (subtyping) for equi-recursive types.
  - Induction/coinduction & proof principles
  - Finite and Infinite Types/Subtyping
  - Membership checking algorithm



Homework

21.5.2 Exercise [★★]: Verify that S_f and S, the generating functions for the subtyping relations from Definitions 21.3.1 and 21.3.2, are invertible, and give their support functions. □