This lecture is based on a number of different resources as indicated per slide.
Concurrency

What is concurrency?

What makes concurrent programming different from sequential programming?

What are the core components of a concurrent language?
Concurrency

• Possible inter-thread communication mechanisms:
  • Read/write to shared memory.
  • Locks.
  • Monitors (a.k.a. wait/notify).
  • Buffered streams.
  • Unbuffered streams.
  • ...

• Which of these does Java support?
• Which should we include in a foundational calculus?
History

- Models of concurrency (late 1970s-80s): Communicating Sequential Processes (Hoare), Petri Nets (Petri), Calculus of Communicating Systems (Milner), ...

- Additional features to model dynamic network topologies (late 1980s-90s): Pi-calculus (Milner), Higher order pi-calculus (Sangiorgi), Ambients (Cardelli and Gordon), ...
In need of designated calculi
Program meanings

Program Meanings = Memories → Memories.

Program Meanings = Memories → P(Memories)

Ok for sequential programs

Ok for non-deterministic programs

© Ralf Lämmel, 2009-2012 unless noted otherwise
Parallelism and shared memory

Program $P_1 : x := 1 ; x := x + 1$
Program $P_2 : x := 2$

Semantics($P_1$) = Semantics($P_2$)
Parallelism and shared memory

Program $P_1 : x := 1 ; x := x + 1$
Program $P_2 : x := 2$
Program $Q : x := 3$

Program $R_1 : P_1 \text{ par } Q$
Program $R_2 : P_2 \text{ par } Q$

Semantics($R_1$) $\neq$ Semantics($R_2$)

Lack of compositionality
“Once the memory is no longer at the behest of a single master, then the master-to-slave (or: function-to-value) view of the program-to-memory relationship becomes a bit of a fiction. An old proverb states: He who serves two masters serves none. It is better to develop a general model of interactive systems in which the program-to-memory interaction is just a special case of interaction among peers.”
The shared memory model

Passive “thing”

Active process
Memory as an interactive process

Program variables as channels

Process

Process

© Ralf Lämmel, 2009-2012 unless noted otherwise
Memory as a distributed process

Memory cells are processes.

Memories are no longer monolithic.
The Calculus of Communicating Systems
Agents and ports

- **Agent** $C$
  - Dynamic system is network of agents.
  - Each agent has own identity persisting over time.
  - Agent performs *actions* (external communications or internal actions).
  - *Behavior* of a system is its (observable) capability of communication.

- **Agent has labeled ports.**
  - Input port $\text{in}$.
  - Output port $\overline{\text{out}}$. 
A simple example

Behavior of $C$:

- $C := \text{in}(x).C'(x)$
- $C'(x) := \text{out}(x).C$

Process behaviors are described as (mutually recursive) equations.
Example: bounded buffers

Bounded buffer $\text{Buff}_n(s)$

- $\text{Buff}_n() := \text{in}(x).\text{Buff}_n(x)$
- $\text{Buff}_n(v_1, \ldots, v_n) := \overline{\text{out}}(v_n).\text{Buff}_n(v_1, \ldots, v_{n-1})$
- $\text{Buff}_n(v_1, \ldots, v_k) := \overline{\text{in}}(x).\text{Buff}_n(x, v_1, \ldots, v_k) + \overline{\text{out}}(v_k).\text{Buff}_n(v_1, \ldots, v_{k-1})(0 < k < n)$
Used language elements

• Basic combinator ‘+’
  – $P + Q$ behaves like $P$ or like $Q$.
  – When one performs its first action, other is discarded.
  – If both alternatives are allowed, selection is non-deterministic.

• Combining forms
  – Summation $P + Q$ of two agents.
  – Sequencing $\alpha.P$ of action $\alpha$ and agent $P$.

Later we add “composition”.

Process definitions may be parameterized.
Example: a vending machine

- Big chocolate costs 2p, small one costs 1p.
- $V := 2p \text{big.c} \text{ollect}.V$
  + $1p \text{little.c} \text{ollect}.V$

Exercises:
Identify input vs. output.
What behaviors make sense for users?
Example: a multiplier

- \( \text{Twice} := \text{in}(x).\overline{\text{out}(2 \times x)}.\text{Twice}. \)
- Output actions may take expressions.
Example: The JobShop

- A simple production line:
  - Two people (the jobbers).
  - Two tools (hammer and mallet).
  - Jobs arrive sequentially on a belt to be processed.

- Ports may be linked to multiple ports:
  - Jobbers compete for use of hammer.
  - Jobbers compete for use of job.
  - Source of non-determinism.

- Ports of belt are omitted from system:
  - in and out are external.

- Internal ports are not labelled:
  - Ports by which jobbers acquire and release tools.
Example: The JobShop

• A simple production line:
  – Two people (the jobbers).
  – Two tools (hammer and mallet).
  – Jobs arrive sequentially on a belt to be processed.

• Ports may be linked to multiple ports.
  – Jobbers compete for use of hammer.
  – Jobbers compete for use of job.
  – Source of non-determinism.

• Ports of belt are omitted from system.
  – in and out are external.

• Internal ports are not labelled:
  – Ports by which jobbers acquire and release tools.
The tools of the JobShop

• Behaviors:
  - \( Hammer := \text{geth.Busyhammer} \)
    \( Busyhammer := \text{puth.Hammer} \)
  - \( Mallet := \text{getm.Busymallet} \)
    \( Busymallet := \text{putm.Mallet} \)

• Sort = set of labels
  - \( P : L \ldots \) agent \( P \) has sort \( L \)
  - \( Hammer: \{\text{geth, puth}\} \)
    \( Mallet: \{\text{getm, putm}\} \)
    \( Jobshop: \{\text{in, out}\} \)
The jobbers of the JobShop

• Different kinds of jobs:
  – Easy jobs done with hands.
  – Hard jobs done with hammer.
  – Other jobs done with hammer or mallet.

• Behavior:
  – $\text{Jobber} := \text{in}(\text{job}).\text{Start}(\text{job})$
  – $\text{Start}(\text{job}) := \text{if } \text{easy}(\text{job}) \text{ then } \text{Finish}(\text{job})$
    
    \text{else if } \text{hard}(\text{job}) \text{ then } \text{Uhammer}(\text{job})$
    \text{else } \text{Usetool}(\text{job})$
  – $\text{Usetool}(\text{job}) := \text{Uhammer}(\text{job}) + \text{Umallet}(\text{job})$
  – $\text{Uhammer}(\text{job}) := \text{geth}.\text{puth}.\text{Finish}(\text{job})$
  – $\text{Umallet}(\text{job}) := \text{getm}.\text{putm}.\text{Finish}(\text{job})$
  – $\text{Finish}(\text{job}) := \text{out}(\text{done}(\text{job})).\text{Jobber}$
Composition of the agents

- **Jobber-Hammer** subsystem
  - Jobber | Hammer
  - Composition operator |
  - Agents may proceed independently or interact through complementary ports.
  - Join complementary ports.

- **Two jobbers sharing hammer:**
  - Jobber | Hammer | Jobber
  - Composition is commutative and associative.
Further composition

- **Internalisation** of ports:
  - No further agents may be connected to ports:
  - *Restriction* operator \( L \)
  - \( L \) internalizes all ports \( L \).
  - \((Jobber \mid Jobber \mid Hammer)\)\{geth,puth\}

- **Complete system**:
  - \( Jobshop := (Jobber \mid Jobber \mid Hammer \mid Mallet)\)\( L \)
  - \( L := \{geth,puth,getm,putm\} \)
“... sequential composition is indeed a special case of parallel composition ... in which the only interaction between occurs when $P$ finishes and $Q$ begins ...”

$P; Q$ not part of CCS

$P|Q$ part of CCS
Reformulations

• **Relabelling Operator**
  
  \[- P[l'_1/l_1, \ldots, l'_n/l_n] \]
  
  \[- f(l) = f(l) \]

• Semaphore agent

  \[- Sem := get.put.Sem \]

• Reformulation of tools

  \[- Hammer := Sem[geth/get, puth/put] \]
  
  \[- Mallet := Sem[getm/get, putm/put] \]
In need of equality of agents

- **Strongjobber** only needs hands:
  - $\text{Strongjobber} := \text{in}(\text{job}).\overline{\text{out}}(\text{done(job)}).\text{Strongjobber}$

- **Claim:**
  - $\text{Jobshop} = \text{Strongjobber} \mid \text{Strongjobber}$
  - Specification of system Jobshop
  - Proof of equality required.

*In which sense are the processes equal?*
Formalization of CCS

Let's skip this and look at the “simpler” Pi-calculus.
The core calculus
No value transmission: just synchronization

- **Agent expressions**
  - Agent constants and variables
    - Prefix $\alpha.E$
  - Summation $\sum E_i$
  - Composition $E_1|E_2$
  - Restriction $E \setminus L$
  - Relabelling $E[f]$

- **Names and co-names**
  - Set $A$ of names (geth, ackin, ...)
  - Set $\mathcal{A}$ of co-names ($\overline{\text{geth}}, \overline{\text{ackin}}, ...$)
  - Set of labels $L = A \cup \mathcal{A}$

- **Actions**
  - Completed (perfect) action $\tau$.
  - $\text{Act} = L \cup \{\tau\}$

- **Transition** $P \xrightarrow{l} Q$ with action $l$
  - Hammer $\xrightarrow{\text{geth}}$ Busyhammer
Transition rules of the core calculus

- **Act** \( \alpha \cdot E \xrightarrow{\alpha} E \)
- **Sum** \( \sum_i E_i \xrightarrow{\alpha} E_i' \)
- **Com\(_1\)** \( E \xrightarrow{\alpha} E' \quad E|F \xrightarrow{\alpha} E'|F \)
- **Com\(_2\)** \( F \xrightarrow{\alpha} F' \quad E|F \xrightarrow{\alpha} E'|F' \)
- **Com\(_3\)** \( E \xrightarrow{l} E' \quad F \xrightarrow{t} F' \quad E|F \xrightarrow{t} E'|F' \)
- **Res** \( E \xrightarrow{\alpha} E' \quad E\setminus\alpha \xrightarrow{\alpha} E'\setminus\alpha \) (\( \alpha \), \( \overline{\alpha} \) not in \( L \))
- **Rel** \( E \xrightarrow{\alpha} E' \quad E[f] \xrightarrow{f(\alpha)} E'[f] \)
- **Con** \( P \xrightarrow{\alpha} P' \quad A \xrightarrow{\alpha} A' \) (\( A := P \))

This rule rules out transitions with hidden names.

This rule makes clear that no more than two agents participate in communication.

This is about the application of definitions for agents.
The value-passing calculus

- Values passed between agents
  - Can be reduced to basic calculus.
  - $C := \text{in}(x).C'(x)$
  - $C'(x) := \text{out}(x).C$
  - $C := \Sigma_v \text{in}_v.C'_v$
    - $C'_v := \text{out}_v.C$ ($v \in V$)
  - Families of ports and agents.

- The full language
  - Prefixes $a(x).E$, $\overline{a}(e).E$, $\tau.E$
  - Conditional if $b$ then $E$

- Translation
  - $a(x).E \Rightarrow \Sigma_v.E\{v/x\}$
  - $\overline{a}(e).E \Rightarrow \overline{a}_e.E$
  - $\tau.E \Rightarrow \tau.E$
  - if $b$ then $E \Rightarrow (E$, if $b$ and 0, otherwise)
Bisimulation (very informally)

- Two agent expressions $P$, $Q$ are bisimilar:
  - If $P$ can do an $\alpha$ action towards $P'$,
  - then $Q$ can do an $\alpha$ action towards $Q'$,
  - such that $P'$ and $Q'$ are again bisimilar,
  - and v.v.

Intuitively two systems are bisimilar if they match each other's moves. In this sense, each of the systems cannot be distinguished from the other by an observer. [Wikipedia]
Summation laws

- \( P + Q = Q + P \)
- \( P + (Q + R) = (P + Q) + R \)
- \( P + P = P \)
- \( P + 0 = P \)
• Composition laws
  - \( P|Q = Q|P \)
  - \( P|(Q|R) = (P|Q)|R \)
  - \( P|0 = P \)

• Restriction laws
  - \( P\backslash L = P, \text{ if } L(P) \cap (L \cup T) = \emptyset \).
  - \( P\backslash K\backslash L = P\backslash(K \cup L) \)
  - \( \ldots \)

• Relabelling laws
  - \( P[id] = P \)
  - \( P[f][f'] = P[f' \circ f] \)
  - \( \ldots \)
Non-laws

• \( \tau . P = P \)
  
  - \( A = a . A + \tau . b . A \)
  
  - \( A' = a . A' + b . A' \)
  
  - \( A \) may switch to state in which only \( b \) is possible.
  
  - \( A' \) always allows \( a \) or \( b \).

• \( \alpha . (P + Q) = \alpha . P + \alpha . Q \)
  
  - \( a . (b . P + c . Q) = a . b . P + a . c . Q \)
  
  - \( b . P \) is \( a \)-derivative of right side, not capable of \( c \) action.
  
  - \( a \)-derivative of left side is capable of \( c \) action!
  
  - Action sequence \( a, c \) may yield deadlock for right side.
Pi-calculus

A minimal model with ‘enough stuff’ to perform interesting computation (e.g. is more powerful than the lambda-calculus).
First shot:

\[ P, Q, R ::= 0 \]
\[ \text{out } x \ y; \ P \]
\[ \text{in } x \ (y); \ P \]
\[ P \mid Q \]

- **Completed process**
- **Output prefixing:** emit name \( y \) on channel \( x \)
- **Input prefixing:** wait for a name on channel \( x \) to be bound to \( y \)
- **Concurrency**
Example programs

1. out stdout hello; out stdout world; 0
2. in stdin (name); out stdout hello; out stdout name; 0
3. (out c fred; 0) | (in c (name); out d name; 0)
4. (out c fred; out c wilma; 0) | (in c (x); out d x; 0) | (in c (y); out e y; 0)
5. (out c fred; in d x; 0) | (in c (y); out d wilma; 0)
6. (in d x; out c fred; 0) | (in c (y); out d wilma; 0)
7. (out c fred; in d (x); 0) | (out d wilma; in c (y); 0)

What do these programs do?
Dynamic semantics

Structural congruence $P \equiv Q$ is generated by:

1. If $P =_\alpha Q$ then $P \equiv Q$.
2. $P \mid Q \equiv Q \mid P$.
3. $(P \mid Q) \mid R \equiv P \mid (Q \mid R)$.

Dynamic semantics $P \rightarrow Q$ is generated by:

1. $(\text{out } x \ y; P) \mid (\text{in } x \ (z); Q) \rightarrow P \mid Q[y/z]$
2. If $P \rightarrow Q$ then $P \mid R \rightarrow Q \mid R$.
3. If $P \equiv \rightarrow \equiv Q$ then $P \rightarrow Q$. 
Recursion? Looping? Infinite Behavior?

Minimal solution \textit{replication}: \(!P \text{ ‘acts like’ } P \parallel P \parallel P \parallel \ldots\)

Examples:

1. \(!\text{in } x (z); \text{out } y z; 0\)
2. \(\text{out acquire lock}; 0 \parallel \!\text{in release (lock)}; \text{out acquire lock}; 0\)

Replicated input \(!\text{in accept (socket)}; P\) acts a lot like a multithreaded server (Java ServerSocket).

Dynamic semantics just given by:

\(!P \equiv P \parallel \!P\)
Creation of new channels

Minimal solution *channel generation*: new \((x)\); \(P\) generates a fresh channel for use in \(P\).

Example:

1. new \((c)\); out \(x\) \(c\); in \(c\) \((y_1)\); .. in \(c\) \((y_n)\); \(P\)
2. in \(x\) \((c)\); out \(c\) \(z_1\); .. out \(c\) \(z_n\); \(Q\)

Put these in parallel, and what happens?

New channel generation acts a lot like new object generation / new key generation / new nonce generation / ...

Dynamic semantics just given by:

\[(\text{new} \ (x); \ P) \parallel Q \equiv \text{new} \ (x); \ (P \parallel Q) \quad \text{(as long as} \ x \not\in Q)\]

If \(P \rightarrow Q\) then new \((x); \ P \rightarrow \text{new} \ (x); \ Q\).
Derived forms

Multiple messages:

\[
\text{in } x (y_1, \ldots, y_n); P \\
\quad = \text{new } (c); \text{out } x \ c; \text{in } c \ (y_1); \ldots \ \text{in } c \ (y_n); P
\]

\[
\text{out } x (z_1, \ldots, z_n); Q \\
\quad = \text{in } x \ (c); \text{out } c \ z_1; \ldots \ \text{out } c \ z_n; Q
\]

Let’s double check:

\[
(\text{in } x (y_1, \ldots, y_n); P \mid \text{out } x (z_1, \ldots, z_n); Q) \rightarrow^* \\
\Rightarrow P[z_1/y_1, \ldots, z_n/y_n] \mid Q
\]
In need of garbage collection

new (c); $P =_{gc} P$ (when $c \not\in P$)

new (c); in $c$ (x); $P =_{gc} 0$

new (c); !in $c$ (x); $P =_{gc} 0$

new (c); out $c$ x; $P =_{gc} 0$

new (c); !out $c$ x; $P =_{gc} 0$

$P \mid 0 =_{gc} P$

Let’s double check:

$(\text{in } x (y_1,\ldots,y_n); P \mid \text{out } x (z_1,\ldots,z_n); Q)\quad \rightarrow^* =_{gc} P[z_1/y_1,\ldots,z_n/y_n] \mid Q$
Correctness of GC

Correctness of garbage collection:

If \( P =_{gc} Q \) and \( P \rightarrow P' \)
then \( P' =_{gc} Q' \) and \( Q \rightarrow Q' \)
More derived forms

Booleans:

True\( b \)
\[ = \text{!in } b (x, y); \text{out } x (); 0 \]

False\( b \)
\[ = \text{!in } b (x, y); \text{out } y (); 0 \]

if \( b \) \{ \ P \ } else \{ \ Q \ }
\[ = \text{new } (t); \text{new } (f); ( \text{out } b (t, f); 0 \mid \text{in } t (); P \mid \text{in } f (); Q ) \]

Sanity check:

True\( b \) \mid \text{if } \( b \) \{ \ P \ } else \{ \ Q \ }
\[ \rightarrow^* =_{\text{gc}} \text{True}(b) \mid P \]
Many derived forms

Can also code integers, linked lists, ...

and the lambda-calculus...

and concurrency controls like mutexes, mvars, ivars, buffers, etc.
• **Summary**: CCS and Pi-calculus
  - Modeling systems of interacting processes using channels.
  - Approach amenable to formal analysis.
  - Equivalence is based on communication behavior.

• **Recommended reading**:
  - Milner’s “Elements of Interaction”
  - CCS tutorial [AcetoLI05]

• **Outlook**:
  - End Prolog-driven section of this course
  - Begin Haskell-driven section
  - (Preparation of) Midterm