Concurrency

A *process* is a program executing on a virtual computer.

Issues such as *processor speed* and *multiplexing of shared resources* are abstracted away.

Processes may either explicitly share or implicitly multiples memory (*thread* or *lightweight process*).
Creating processes

A possible syntax for creating processes:

```c
ID fork(int (*proc)(int), int p);
int join(ID i);

int foo(int p);
int r;
ID i = fork(foo, 3);
...
r = join(i);
```

Creating processes, II

Another syntax for creating processes:

```c
cobegin
  code executed by process 1;
  |
  code executed by process 2;
  |
  ...
coend
```
Properties

Concurrent programs are specified using properties, which is a predicate that evaluated over a run of the concurrent program.

° Thus, it has the value true or false in each run of the program.
° We say that the property holds if it is true in each run.
  • A property: the value of $x$ is always at least as large as the value of $y$, and $x$ has the value of 0 at least once.
  • Not a property: the average number of processes waiting on a lock is less than 1.

Safety and liveness properties

Any property is either a safety property, a liveness property, or a conjunction of a safety and a liveness property.
Safety properties

A safety property is of the form *nothing bad happens* (that is, all states are safe).

Examples:

The number of processes in a critical section is always less than 2.

Let $p$ be the sequence of produced values and $c$ be the sequence of consumed values. $c$ is always a prefix of $p$.

Liveness properties

A liveness property is of the form *something good happens* (that is, an interesting state is eventually achieved).

Examples:

A process that wishes to enter the critical section eventually does so.

$p$ grows without bound.

For every value $x$ in $p$, $x$ is eventually in $c$. 
Safety and Liveness

Showing a safety property $P$ holds:
- find a safety property $P'$: $P' \Rightarrow P$;
- show that $P'$ initially holds;
- show that each step of the program maintains $P'$.

Showing a liveness property holds is usually done by induction.

Basic properties of environment

- *Finite progress axiom*
  Each process takes a step infinitely often.
  - Do all schedulers implement this?
  - If not, do such schedulers pose problems?

- *Atomic shared variables*

Consider
\[
\begin{align*}
\{ x = A \} & \quad \text{any concurrent read of } x \text{ will return} \\
 x = B ; & \quad \text{either } A \text{ or } B. \\
\{ x = B \} & 
\end{align*}
\]
Atomic Variables

\{x = 0\} 
\textbf{cobegin} 
\hspace{1em} x = x + 1; 
\hspace{1em} || 
\hspace{1em} x = x - 1; 
\textbf{coend} 
\{x \in \{-1, 0, 1\}\}

---

Producer/Consumer problem

Let $p$ be the sequence of produced values and $c$ be the sequence of consumed values.

- $c$ is always a prefix of $p$.
- For every value $x$ in $p$, $x$ is eventually in $c$.

\textit{Bounded buffer} variant:

- Always $|p| - |c| \leq \text{max}$
Solving producer-consumer

```c
int buf, produced = 0;      /* produced ∈ \{0, 1\} */

Producer
while (1) {
    while (produced) ;
    buf = v;           /* logically appends v to p */
    produced = 1;
}

Consumer
while (1) {
    while (!produced) ;
    c = append(c, buf);
    produced = 0;
}

Note that this satisfies max = 1.
How do you generalize this for values of max greater than 1?
```

Mutual exclusion

- The number of processes in the critical section is never more than 1.
- If a process wishes to enter the critical section then it eventually does so.
Solving mutual exclusion

```c
int in1, in2, turn = 1;

while (1) {
    in1 = 1;
    turn = 2;
    while (in2 && turn == 2) {
        Critical section for process 1;
        in1 = 0;
    }
}

while (1) {
    in2 = 1;
    turn = 1;
    while (in1 && turn == 1) {
        Critical section for process 2;
        in2 = 0;
    }
}
```

Proof of Peterson’s algorithm: I

```c
int in1, in2, turn = 1, at1 = 0, at2 = 0;

while (1) {
    ( in1 = 1; at1 = 1; )
    ( turn = 2; at1 = 0; )
    while (in2 && turn == 2) {
        Critical section for process 1;
        in1 = 0;
    }
}

while (1) {
    ( in2 = 1; at2 = 1; )
    ( turn = 1; at2 = 0; )
    while (in1 && turn == 1) {
        Critical section for process 2;
        in2 = 0;
    }
}
Proof of Peterson’s algorithm: II

while (1) {
    {-in1 ∧ (turn = 1 ⊕ turn = 2) ∧ ¬at1}
    ⟨ in1 = 1; at1 = 1; ⟩
    {in1 ∧ (turn = 1 ⊕ turn = 2) ∧ at1}
    ⟨ turn = 2; at1 = 0; ⟩
    {in1 ∧ (turn = 1 ⊕ turn = 2) ∧ ¬at1}
    while (in2 && turn == 2) ;
    {in1 ∧ (turn = 1 ⊕ turn = 2) ∧ ¬at1 ∧ (¬in2 ⊕ turn = 1 ⊕ at2)}
    Critical section for process 1 ;
    {in1 ∧ (turn = 1 ⊕ turn = 2) ∧ ¬at1 ∧ (¬in2 ⊕ turn = 1 ⊕ at2)}
    in1 = 0 ;
    {¬in1 ∧ (turn = 1 ⊕ turn = 2) ∧ ¬at1} 
}

Proof of Peterson’s algorithm: III

while (1) {
    {-in2 ∧ (turn = 1 ⊕ turn = 2) ∧ ¬at2}
    ⟨ in2 = 1; at2 = 1; ⟩
    {in2 ∧ (turn = 1 ⊕ turn = 2) ∧ at2}
    ⟨ turn = 1; at2 = 0; ⟩
    {in2 ∧ (turn = 1 ⊕ turn = 2) ∧ ¬at2}
    while (in1 && turn == 1) ;
    {in2 ∧ (turn = 1 ⊕ turn = 2) ∧ ¬at2 ∧ (¬in1 ⊕ turn = 2 ⊕ at1)}
    Critical section for process 2 ;
    {in2 ∧ (turn = 1 ⊕ turn = 2) ∧ ¬at2 ∧ (¬in1 ⊕ turn = 2 ⊕ at1)}
    in2 = 0 ;
    {¬in2 ∧ (turn = 1 ⊕ turn = 2) ∧ ¬at2} 
}
Proof of Peterson’s algorithm: IV

at CS1 and at CS2 implies false:

\[ \text{in}_1 \land \text{turn} = 1 \lor \text{turn} = 2 \land \neg \text{at}_1 \land (\neg \text{in}_2 \lor \text{turn} = 1 \lor \text{at}_2) \land \]
\[ \text{in}_2 \land \text{turn} = 1 \lor \text{turn} = 2 \land \neg \text{at}_2 \land (\neg \text{in}_1 \lor \text{turn} = 2 \lor \text{at}_1) \]
\[ \Rightarrow (\text{turn} = 1) \land (\text{turn} = 2) \]

process 1 in non-critical, process 2 trying to enter critical section and is blocked implies false:

\[ \neg \text{in}_1 \land (\text{turn} = 1 \lor \text{turn} = 2) \land \neg \text{at}_1 \land \]
\[ \text{in}_2 \land (\text{turn} = 1 \lor \text{turn} = 2) \land \neg \text{at}_2 \land \]
\[ \text{in}_1 \land \text{turn} = 1 \]
\[ \Rightarrow \neg \text{in}_1 \land \text{in}_1 \]

Proof of Peterson’s algorithm: V

process 1 trying to enter critical section, process 2 trying to enter critical section, and both blocked implies false:

\[ \text{in}_2 \land \text{turn} = 2 \land \]
\[ \text{in}_1 \land \text{turn} = 1 \land \]
\[ \Rightarrow (\text{turn} = 1) \land (\text{turn} = 2) \]
The Bakery Algorithm, I

int turn[n] = 0, 0, ..., 0;
int number = 1, next = 1;

// code for process i
int j;
while (1) {
    turn[i] = number; number = number + 1;
    for (j = 0; j < n; j++)
        if (j != i) { await (turn[i] == next); }

    critical section

    next = next + 1;

    noncritical code
}

The Bakery Algorithm, II

int turn[n] = 0, 0, ..., 0;

// code for process i
int j;
while (1) {
    turn[i] = max(turn[0], ..., turn[n-1]) + 1;
    for (j = 0; j < n; j++)
        if (j != i) { await (turn[i] == next || turn[i] < turn[j]); }

    critical section

    turn[i] = 0;

    noncritical code
}
The Bakery Algorithm, III

```c
int turn0 = 0, turn1 = 0;
cobegin
    while (1) {
        turn0 = turn1 + 1;
        while (turn1 != 0 && turn0 > turn1) ;
        critical section
        turn0 = 0;
        noncritical code
    }
||
    while (1) {
        turn1 = turn0 + 1;
        while (turn0 != 0 && turn1 > turn0) ;
        critical section
        turn1 = 0;
        noncritical code
    }
coend

... but this isn't safe.
```

The Bakery Algorithm, IV

```c
int turn0 = 0, turn1 = 0;
cobegin
    while (1) {
        turn0 = turn1 + 1;
        while (turn1 != 0 && turn0 > turn1) ;
        critical section
        turn0 = 0;
        noncritical code
    }
||
    while (1) {
        turn1 = turn0 + 1;
        while (turn0 != 0 && turn1 >= turn0) ;
        critical section
        turn1 = 0;
        noncritical code
    }
coend

... but this still isn't safe - suppose each finds the other's turn value 0.
```
The Bakery Algorithm, V

```c
int turn0 = 0, turn1 = 0;

cobegin
  while (1) {
    turn0 = turn1 + 1;
    while (turn1 != 0 && turn0 > turn1) ;
    critical section
    turn0 = 0;
    noncritical code
  } ||
  while (1) {
    turn1 = turn0 + 1;
    while (turn0 != 0 && turn1 >= turn0) ;
    critical section
    turn1 = 0;
    noncritical code
  }

coend

... but this still isn't safe! Have both see turn values 0, and then let process 1 enter first.
```

The Bakery Algorithm, VI

```c
int turn0 = 0, turn1 = 0;

cobegin
  while (1) {
    turn0 = 1;
    turn0 = turn1 + 1;
    while (turn1 != 0 && turn0 > turn1) ;
    critical section
    turn0 = 0;
    noncritical code
  } ||
  while (1) {
    turn1 = 1;
    turn1 = turn0 + 1;
    while (turn0 != 0 && turn1 >= turn0) ;
    critical section
    turn1 = 0;
    noncritical code
  }

coend

... can symmetrize by defining [a, b] > [c, d] (a > b) || ((a = b) && (c > d))
```
... can symmetrize by defining \([a, b] > [c, d]\) to be \((a > b) \lor ((a = b) \land (c > d))\)

```c
int turn0 = 0, turn1 = 0;

cobegin
    while (1) {
        turn0 = 1;
        turn0 = turn1 + 1;
        while (turn1 != 0 && [turn0, 0] > [turn1, 1])
            critical section
            turn0 = 0;
            noncritical code
    }
|| ...

coend
```

---

The Bakery Algorithm, VIII

```c
int turn[n] = 0, 0, ..., 0;
// code for process i
int j;
while (1) {
    turn[i] = 1;
    turn[i] = max(turn[0], ..., turn[n-1]) + 1;
    for (j = 0; j < n; j++) if (j != i) do
        do (turn[j] != 0 && [turn[i], i] > [turn[j], j])

    critical section

    turn[i] = 0;

    noncritical code
}
```
Revisiting shared variables

Both solutions use busy waiting, which is often an inefficient approach:

° A process that is busy waiting cannot proceed until some other process takes a step.
° Such a process can relinquish its processor rather than needlessly looping.
° Doing so can speed up execution.

When is this an invalid argument?

Semaphores

A *semaphore* is an abstraction that allows a process to relinquish its processor.

Two kinds: *binary* and *general*.

Binary:

P(s):

\[
\langle\text{if } (s == 1) s = 0; \text{ else block;}\rangle
\]

V(s):

\[
\langle s = 1; \text{ if (there is a blocked process) then unblock one;} \rangle
\]

(Edsger Dijkstra, 1965)
Semaphores: II

General:

P(s): \( \langle \text{if } (s > 0) s--; \text{ else block; } \rangle \)

V(s): \( \langle s++; \)

\( \text{if (there is a blocked process) then unblock one;} \rangle \)

Solving producer-consumer

gensem put=max, take=0;
int buf[max], in=0, out=0;

Producer

while (1) {
    P(put);
    buf[in] = v; in = (in + 1) % max;
    V(take);
}

Consumer

while (1) {
    P(take);
    c = buf[out]; out = (out + 1) % max;
    V(put);
}
Solving mutual exclusion

```c
binsem cs=1;

while (1) {
    P(cs);
    Critical section for process i;
    V(cs);
}
```

Binary vs. general semaphores

```c
gensem s=i is replaced with
    struct s {
        binsem mtx=1, blk=(i == 0) ? 0 : 1;
        val = i;
    }

P(s) is replaced with
    P(s.blk);
    P(s.mtx);
    if (--s.val > 0) V(s.blk);
    V(s.mtx);

V(s) is replaced with
    P(s.mtx);
    if (++s.val == 1) V(s.blk);
    V(s.mtx);
```
Monitors

An object approach based on critical sections and explicit synchronization variables.

Entry procedures obtain mutual exclusion.

Condition variables (e.g., c):

- `c.wait()` causes process to wait outside of critical section.
- `c.signal()` causes one blocked process to take over critical section (signalling process temporarily leaves critical section).

Semaphores using monitors

```cpp
monitor gsem {
    long value;  // value of semaphore
    condition c; // value > 0
    public:
        void entry P(void);
        void entry V(void);
        gsem(long initial);
    }

gsem::gsem(long initial) { value = initial; }

void gsem::P(void) {
    if (value == 0) c.wait(); value--;
}

void gsem::V(void) {
    value++; if (value > 0) c.signal();
}
```
Solving producer-consumer

monitor PC {
    const long max = 10;
    long buf[max], i=0, j=0, in=0;
    condition notempty; // in > 0
    condition notfull; // in < max
    public:
        void entry put(long v);
        long entry get(void);
    };

void PC::put(long v) {
    if (in == max) notfull.wait();
    buf[i] = v; i = (i + 1) % max; in++;
    notempty.signal();
}

long PC::get(void) {
    long v;
    if (in == 0) notempty.wait();
    v = buf[j]; j = (j + 1) % max; in--;
    notfull.signal();
}

Monitors using semaphores

Assume a monitor m with a single condition c (easily generalized for multiple conditions).

Generate: struct m {
    binsem lock=1;
    gensem urgent=0, csem=0;
    long ccount=0, ucount=0
};

Wrap each entry method:
    P(m.lock);
    code for entry method
    if (m.ucount > 0) V(m.urgent);
    else V(m.lock);
Monitors using semaphores II

Replace `c.wait()` with:
\[
\begin{align*}
&\text{m.ccount}++; \\
&\text{if (m.ucount > 0) V(m.urgent);} \\
&\text{else V(m.lock);} \\
&\text{P(m.csem);} \\
&\text{m.ccount}--; \\
\end{align*}
\]

Replace `c.signal()` with:
\[
\begin{align*}
&\text{m.ucount}++; \\
&\text{if (m.ccount > 0) \{} \\
&\vspace{1em}V(m.csem); \\
&\vspace{1em}P(m.urgent); \\
&\\text{\}} \\
&\text{m.ucount}--; \\
\end{align*}
\]

Conditions vs. semaphores

A semaphore has memory while conditions do not.

\[
\begin{align*}
V(s); & \quad \ldots \\
\ldots & \quad P(s); \quad \text{does not block} \\
\vspace{1em}c.signal(); & \quad \ldots \\
\ldots & \quad c.wait(); \quad \text{blocks}
\end{align*}
\]
Programming with conditions

A monitor has an invariant (a safety property) that must hold whenever a process enters (and hence leaves) the critical region. A condition strengthens this invariant.

When a process requires the stronger property that doesn’t hold, it waits on the condition. When a process establishes the condition, it signals the condition.

Readers and Writers

Let \( r \) be the number of readers and \( w \) be the number of writers.

invariant \( I: (0 \leq r) \land (0 \leq w \leq 1) \land (r = 0 \lor w = 0) \)

readers priority version: let \( wr \) be number of waiting readers.

readOK: \( I \land (w = 0) \)

writeOK: \( I \land (w = 0) \land (r = 0) \land (wr = 0) \)
Readers and Writers II

monitor rprio {
  long r, w;  // number of active read/write
  long wr;   // number of waiting to read
  condition readOK;
  condition writeOK;
  public:
    void entry startread(void);
    void entry endread(void);
    void entry startwrite(void);
    void entry endwrite(void);
    rprio(void);
};

rprio::rprio(void) { r = w = wr = 0; }

Readers and Writers III

rprio::startread(void) {
  if (w > 0) {wr++; readOK.wait(); wr--; }
  r++;
  readOK.signal();
}

rprio::endread(void) {
  r--; if (r == 0) writeOK.signal(); }

rprio::startwrite(void) {
  if (r > 0 || w > 0 || wr > 0) writeOK.wait();
  w++;
}

rprio::endwrite(void) {
  w--;
  if (wr > 0) readOK.signal();
  else writeOK.signal();
}
Final signals

A signaling process must leave the monitor when it signals.

Signals often are performed as the last statement of an entry procedure.

This is inefficient.

Could require any signals to occur only as the process leaves the entry procedure.

Does this limit the power of monitors?

Weakening wait and signal

\{I\} 
if (!c) \{I \land \neg c\} c.wait(); \{I \land c\} 
\{I \land c\} 
have c.notify() move one process blocked on c to ready queue.

\{I\} 
while (!c) \{I \land \neg c\} c.wait(); \{I\} 
\{I \land c\} 
... and, have c.broadcast() move all processes blocked on c to ready queue.
Weakening wait and signal, II

```c
rprio::startread(void) {
    while (w > 0) {wr++; readOK.wait(); wr--; }
    r++;
}

rprio::endread(void) {
    r--; if (r == 0) writeOK.notify(); }

rprio::startwrite(void) {
    while (r > 0 || w > 0 || wr > 0)
        writeOK.wait();
    w++;
}

rprio::endwrite(void) {
    w--;
    if (wr > 0) readOK.broadcast();
    else writeOK.notify();
}
```

But...

Are explicitly named condition variables really needed? since `notifyAll` move all blocked processes onto the ready queue, we can have the guard of the `while` loop sort out who should run:

```c
{I}
while (!c) {I ∧ ¬c} wait(); {I}
{I ∧ c}
```
Having fewer condition variables

Many Unix kernels have been structured in a similar manner.

Unix kernel *sleep*

- *sleep* takes as a parameter a *wait channel*, which is typically the address of some data structure.
- This address is hashed to choose one of a set of *sleep queues*.
- *wakeup* wakes up all processes sleeping on the sleep queue.
Java monitors

Synchronized classes have single (unnamed) condition variable.

```java
public synchronized ... {
    ...
    while (!c) try { wait(); }
    catch(InterruptedException e) {
    }
    ...
}
public synchronized ... {
    ...
    notifyAll();
    ...
}
```

Moral...

Weakening an abstraction is often a good way to improve performance.

Approach used in Mesa (Xerox PARC 1970s) and in the Unix kernel.

It becomes more inefficient as the amount of contention increases, but if this holds then there are more serious problems to be addressed.