CS 5323 – OS II

Lecture 8 – Deadlocks

Logistics

- Quiz 4 will be posted today. Due: Sunday 02/20/2022 11:59 pm
- Assignment 2 posted. Due 02/25/2022 11:59 pm
- Midterm on Monday 02/21/2022 **IN-CLASS**
  - **Comprehensive.** Will cover everything up to and including deadlocks
  - Closed book, closed notes. No cheat sheets.
  - Exact distribution of grades will be discussed on Wednesday

System Model

- System consists of resources
- Resource types $R_1, R_2, . . ., R_m$

  CPU cycles, memory space, I/O devices
- Each resource type R_i has W_i instances.
- Each process utilizes a resource as follows:
  - **request**
  - **use**
  - **release**

Deadlock Characterization

Deadlock can arise if four conditions hold simultaneously.

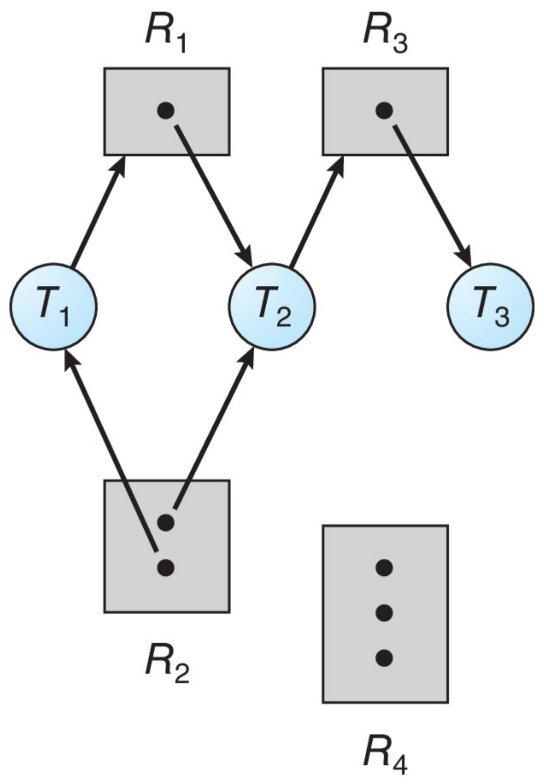
- **Mutual exclusion**: only one process at a time can use a resource
- **Hold and wait**: a process holding at least one resource is waiting to acquire additional resources held by other processes
- **No preemption**: a resource can be released only voluntarily by the process holding it, after that process has completed its task
- **Circular wait**: there exists a set $\{P_0, P_1, \ldots, P_n\}$ of waiting processes such that P_0 is waiting for a resource that is held by P_1, P_1 is waiting for a resource that is held by P_2, …, P_{n-1} is waiting for a resource that is held by P_n, and P_n is waiting for a resource that is held by P_0.

Resource-Allocation Graph

- A set of vertices *V* and a set of edges *E*.
- V is partitioned into two types:
  - $P = \{P_1, P_2, \ldots, P_n\}$, the set consisting of all the processes in the system
  - $R = \{R_1, R_2, \ldots, R_m\}$, the set consisting of all resource types in the system
- **request edge** – directed edge $P_i \rightarrow R_j$
- **assignment edge** – directed edge $R_j \rightarrow P_i$

Resource Allocation Graph Example

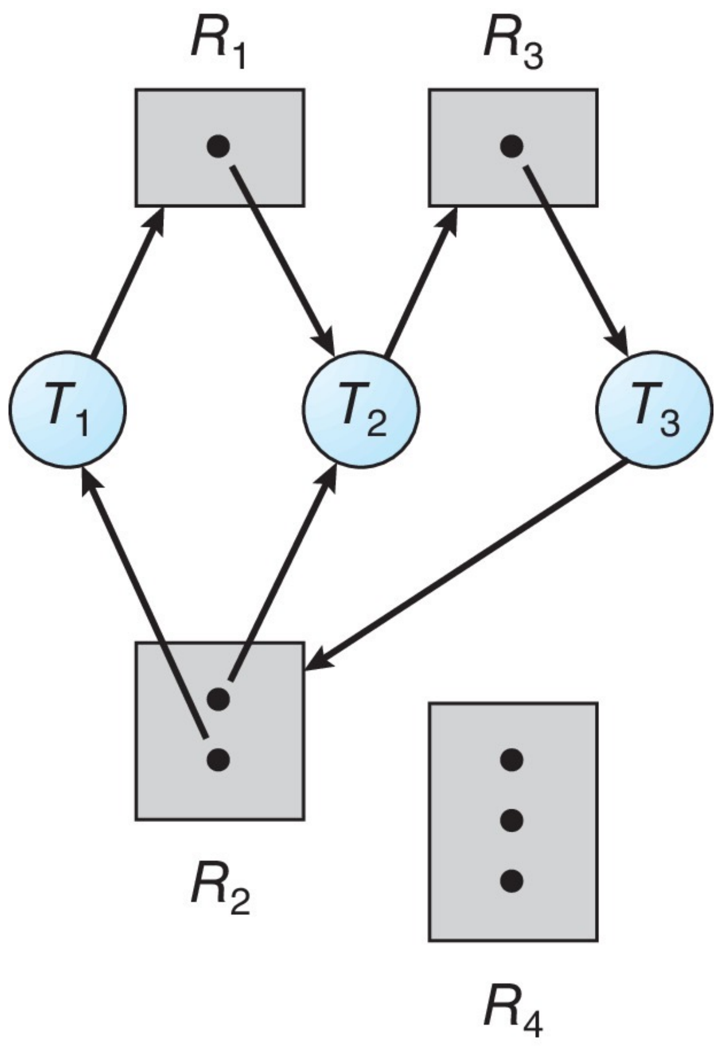
- One instance of R1
- Two instances of R2
- One instance of R3
- Three instance of R4
- T1 holds one instance of R2 and is waiting for an instance of R1
- T2 holds one instance of R1, one instance of R2, and is waiting for an instance of R3
- T3 is holds one instance of R3



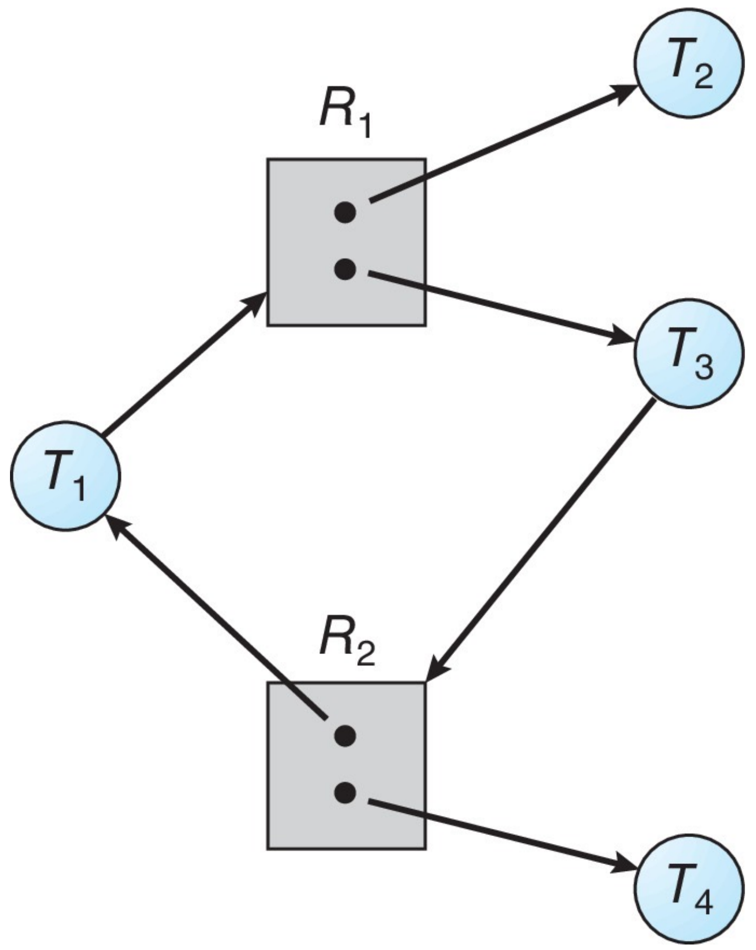
Basic Facts

- If graph contains no cycles $\Rightarrow$ no deadlock
- If graph contains a cycle $\Rightarrow$
  - if only one instance per resource type, then deadlock
  - if several instances per resource type, possibility of deadlock

Resource Allocation Graph With A Deadlock



Graph With A Cycle But No Deadlock



Methods for Handling Deadlocks

- Ensure that the system will ***never*** enter a deadlock state:
  - Deadlock prevention
  - Deadlock avoidance
- Allow the system to enter a deadlock state and then recover
- Ignore the problem and pretend that deadlocks never occur in the system.
  - Ostrich Algorithm

Deadlock Prevention

Invalidate one of the four necessary conditions for deadlock:

- **Mutual Exclusion** – not required for sharable resources (e.g., read-only files); must hold for non-sharable resources
- **Hold and Wait** – must guarantee that whenever a process requests a resource, it does not hold any other resources
  - Require process to request and be allocated all its resources before it begins execution, or allow process to request resources only when the process has none allocated to it.
  - Low resource utilization; starvation possible

Deadlock Prevention (Cont.)

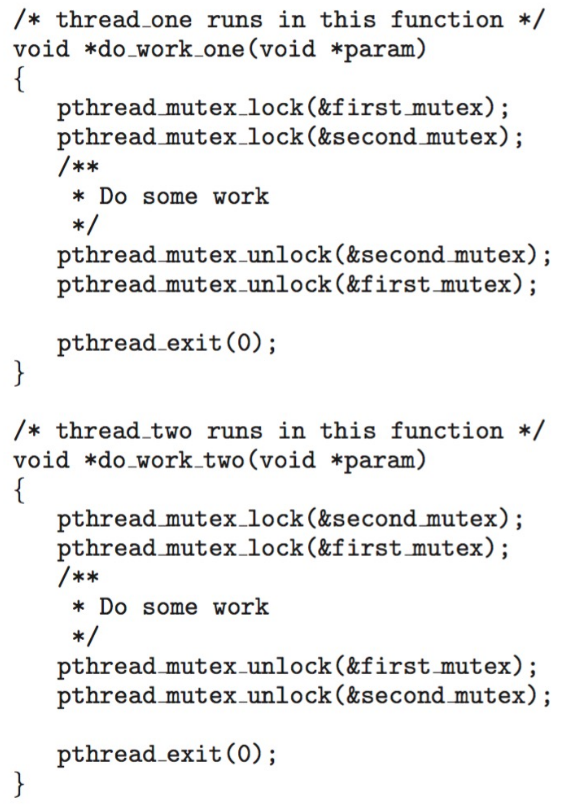
- **No Preemption** –
  - If a process that is holding some resources requests another resource that cannot be immediately allocated to it, then all resources currently being held are released
  - Preempted resources are added to the list of resources for which the process is waiting
  - Process will be restarted only when it can regain its old resources, as well as the new ones that it is requesting
- **Circular Wait** – impose a total ordering of all resource types, and require that each process requests resources in an increasing order of enumeration

Circular Wait

- Invalidating the circular wait condition is most common.
- Simply assign each resource (i.e. mutex locks) a unique number.
- Resources must be acquired in order.
- If:

  `first_mutex = 1`
  `second_mutex = 5`

  code for **`thread_two`** could not be written as follows:



```
/* thread_one runs in this function */
void *do_work_one(void *param)
{
   pthread_mutex_lock(&first_mutex);
   pthread_mutex_lock(&second_mutex);
   /**
    * Do some work
    */
   pthread_mutex_unlock(&second_mutex);
   pthread_mutex_unlock(&first_mutex);

   pthread_exit(0);
}

/* thread_two runs in this function */
void *do_work_two(void *param)
{
   pthread_mutex_lock(&second_mutex);
   pthread_mutex_lock(&first_mutex);
   /**
    * Do some work
    */
   pthread_mutex_unlock(&first_mutex);
   pthread_mutex_unlock(&second_mutex);

   pthread_exit(0);
}
```

Deadlock Avoidance

Requires that the system has some additional *a priori* information available

- Simplest and most useful model requires that each process declare the ***maximum number*** of resources of each type that it may need
- The deadlock-avoidance algorithm dynamically examines the resource-allocation state to ensure that there can never be a circular-wait condition
- Resource-allocation *state* is defined by the number of available and allocated resources, and the maximum demands of the processes

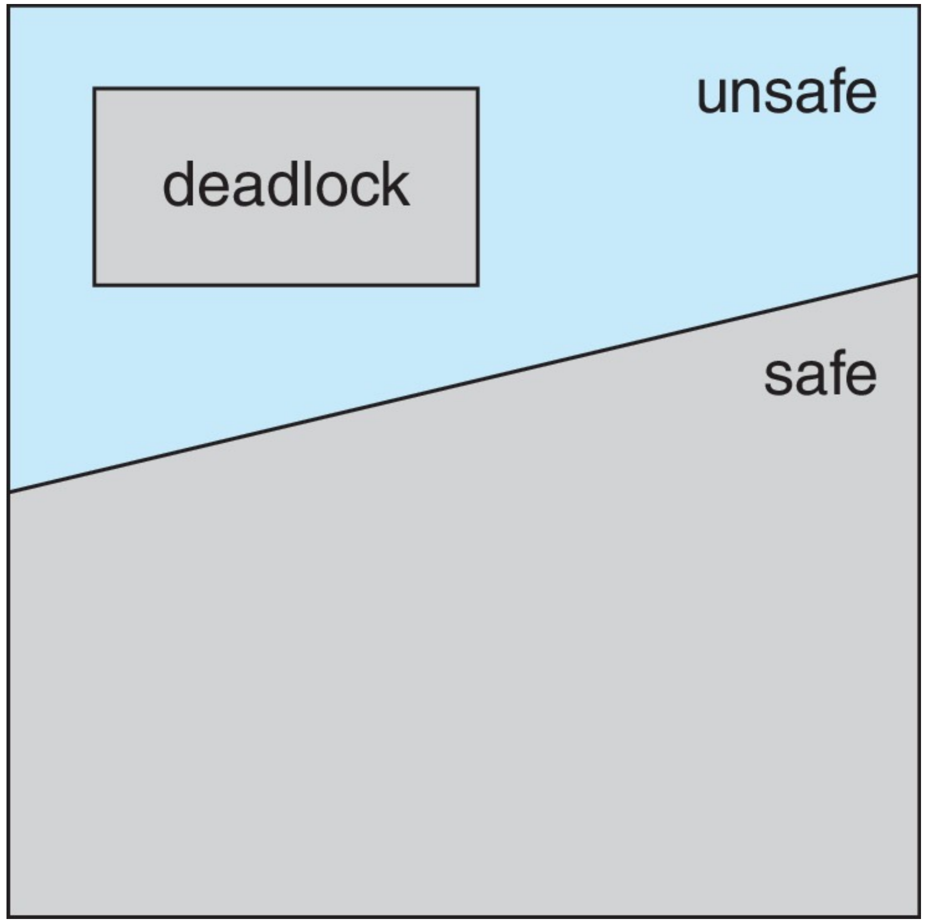
Safe State

- When a process requests an available resource, system must decide if immediate allocation leaves the system in a safe state
- System is in **safe state** if there exists a sequence <P_1, P_2, …, P_n> of ALL the processes in the systems such that for each P_i, the resources that P_i can still request can be satisfied by currently available resources + resources held by all the P_j, with $j < I$
- That is:
  - If P_i resource needs are not immediately available, then P_i can wait until all P_j have finished
  - When P_j is finished, P_i can obtain needed resources, execute, return allocated resources, and terminate
  - When P_i terminates, P_{i+1} can obtain its needed resources, and so on

Basic Facts

- If a system is in safe state $\Rightarrow$ no deadlocks
- If a system is in unsafe state $\Rightarrow$ possibility of deadlock
- Avoidance $\Rightarrow$ ensure that a system will never enter an unsafe state.

Safe, Unsafe, Deadlock State



Avoidance Algorithms

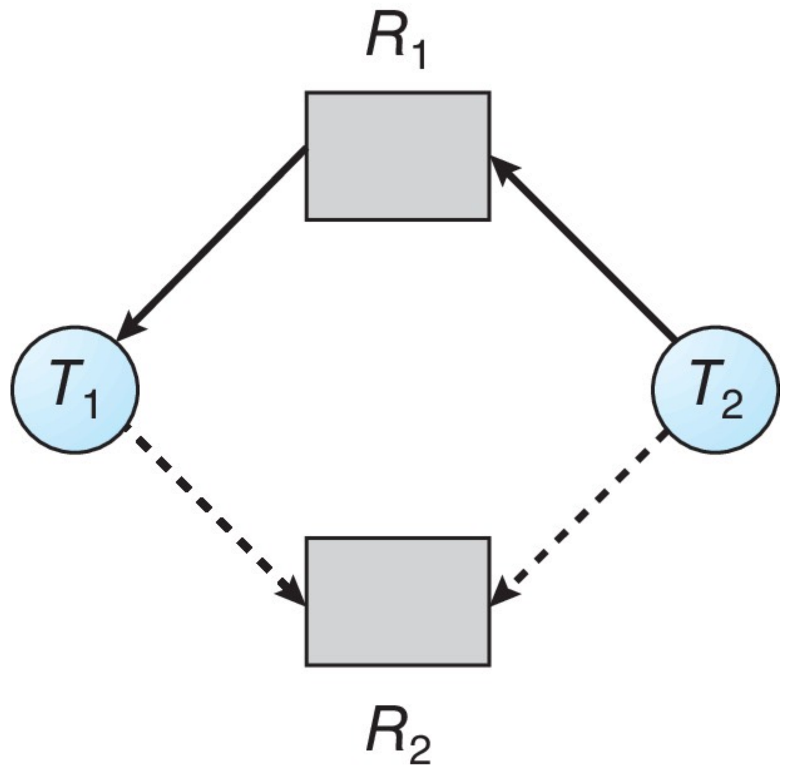
- Single instance of a resource type
  - Use a resource-allocation graph

- Multiple instances of a resource type
  - Use the Banker's Algorithm

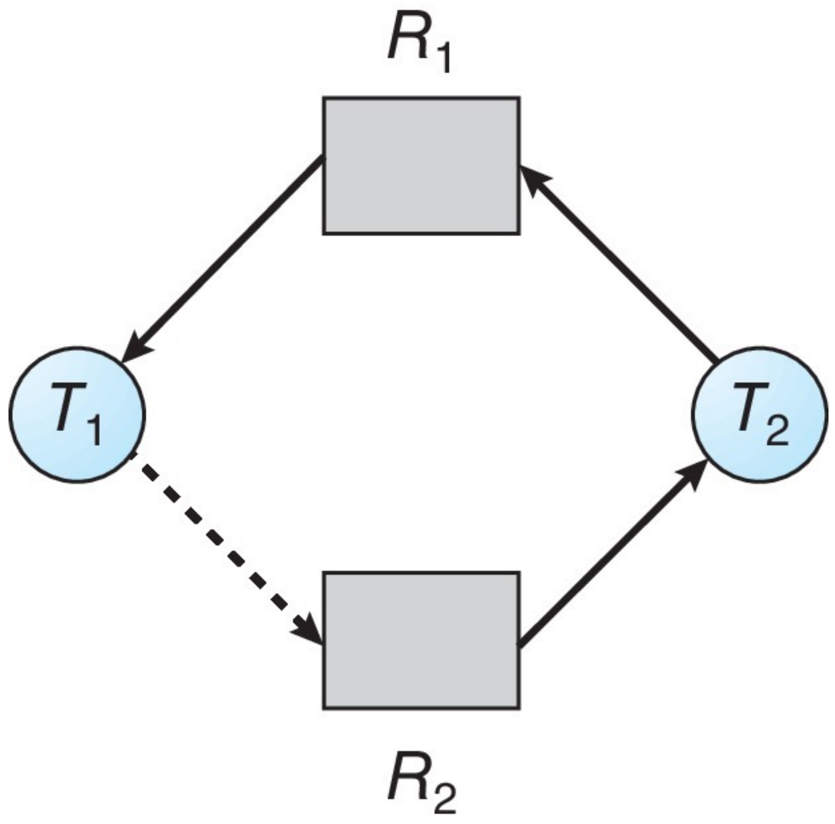
Resource-Allocation Graph Scheme

- **Claim edge** $P_i \rightarrow R_j$ indicated that process P_j may request resource R_j; represented by a dashed line
- Claim edge converts to request edge when a process requests a resource
- Request edge converted to an assignment edge when the resource is allocated to the process
- When a resource is released by a process, assignment edge reconverts to a claim edge
- Resources must be claimed *a priori* in the system

Resource-Allocation Graph



Unsafe State In Resource-Allocation Graph



Resource-Allocation Graph Algorithm

- Suppose that process P_i requests a resource R_j
- The request can be granted only if converting the request edge to an assignment edge does not result in the formation of a cycle in the resource allocation graph
- Cons: Less efficient of systems with multiple instances of a resource. Why?
  - It will hold processes if there is a possibility of a cycle. Multiple instances can lead to large wait time and overhead.

Banker’s Algorithm

- Multiple instances of resources
- Each process must a priori claim maximum use
- When a process requests a resource it may have to wait
- When a process gets all its resources it must return them in a finite amount of time
- Inspired from actual banks. Banks must not allocate resource to customers without ensuring that any existing customers can be served.

Data Structures for the Banker's Algorithm

Let *n* = number of processes, and *m* = number of resources types.

- **Available**: Vector of length *m*. If `available[j] = k`, there are *k* instances of resource type R_j available
- **Max**: *n x m* matrix. If `Max[i,j] = k`, then process P_i may request at most *k* instances of resource type R_j
- **Allocation**: *n* x *m* matrix. If `Allocation[i,j]` = *k* then P_i is currently allocated *k* instances of R_j
- **Need**: *n* x *m* matrix. If `Need[i,j] = k`, then P_i may need *k* more instances of R_j to complete its task

`Need [i,j] = Max[i,j] – Allocation [i,j]`

Safety Algorithm

1. Let ***Work*** and ***Finish*** be vectors of length *m* and *n*, respectively. Initialize:

```
Work = Available
Finish [i] = false for i = 0, 1, …, n- 1
```

2. Find an ***i*** such that both:

   (a) ***Finish [i] = false***

   (b) ***Need$_i$ ≤ Work***

   If no such ***i*** exists, go to step 4

3. ***Work = Work + Allocation$_i$***

   Finish[i] = true

   go to step 2

4. If ***Finish [i] == true*** for all ***i***, then the system is in a safe state

Resource-Request Algorithm for Process P_i

$\boldsymbol{Request_i}$ = request vector for process $\boldsymbol{P_i}$. If $\mathtt{Request}_i\,[j] = k$ then process $\boldsymbol{P_i}$ wants $\boldsymbol{k}$ instances of resource type $\boldsymbol{R_j}$

1. If $\mathtt{Request}_i \leq \mathtt{Need}_i$ go to step 2. Otherwise, raise error condition, since process has exceeded its maximum claim
2. If $\mathtt{Request}_i \leq \mathtt{Available}$, go to step 3. Otherwise $\boldsymbol{P_i}$ must wait, since resources are not available
3. Pretend to allocate requested resources to $\boldsymbol{P_i}$ by modifying the state as follows:

```
Available = Available  – Request_i;
Allocation_i = Allocation_i + Request_i;
Need_i = Need_i – Request_i;
```

- If safe $\Rightarrow$ the resources are allocated to $\boldsymbol{P_i}$
- If unsafe $\Rightarrow$ $\boldsymbol{P_i}$ must wait, and the old resource-allocation state is restored

Example of Banker's Algorithm

- 5 processes P_0 through P_4;
  3 resource types:
  A (10 instances), *B* (5instances), and *C* (7 instances)
- Snapshot at time T_0:

	Allocation	*Max*	*Available*
	A B C	*A B C*	*A B C*
P_0	0 1 0	7 5 3	3 3 2
P_1	2 0 0	3 2 2	
P_2	3 0 2	9 0 2	
P_3	2 1 1	2 2 2	
P_4	0 0 2	4 3 3	

Example (Cont.)

- The content of the matrix ***Need*** is defined to be ***`Max – Allocation`***

	Need
	A B C
P_0	7 4 3
P_1	1 2 2
P_2	6 0 0
P_3	0 1 1
P_4	4 3 1

- The system is in a safe state since the sequence < P_1, P_3, P_4, P_2, P_0> satisfies safety criteria

Bankers Algorithm – Example 2

- Processes P0, P1, P2, P3, P4

Alloc			
A	B	C	D
2	0	0	1
3	1	2	1
2	1	0	3
1	3	1	2
1	4	3	2

Max			
A	B	C	D
4	2	1	2
5	2	5	2
2	3	1	6
1	4	2	4
3	6	6	5

Available			
A	B	C	D
3	3	2	1

Bankers Algorithm – Example 2

- Processes P0, P1, P2, P3, P4

Alloc			
A	B	C	D
2	0	0	1
3	1	2	1
2	1	0	3
1	3	1	2
1	4	3	2

Max			
A	B	C	D
4	2	1	2
5	2	5	2
2	3	1	6
1	4	2	4
3	6	6	5

Need				
Process	A	B	C	D
0	2	2	1	1
1	2	1	3	1
2	0	2	1	3
3	0	1	1	2
4	2	2	3	3

Bankers Algorithm – Example 2

- Processes P0, P1, P2, P3, P4

Available				
Time	**A**	**B**	**C**	**D**
0	3	3	1	2
1	5	3	2	2
2	6	6	3	4
3	7	10	6	6
4	10	11	8	7
5	12	12	8	10

Safe sequence: P0, P3, P4, P1, P2

Bankers Algorithm – Example 3

- Processes P0, P1, P2, P3, P4

Alloc		
A	B	C
1	1	2
2	1	2
4	0	1
0	2	0
1	1	2

Max		
A	B	C
4	3	3
3	2	2
9	0	2
7	5	3
1	1	3

Available		
A	B	C
2	1	0

Total # Resources		
A	B	C
10	6	7

Bankers Algorithm – Example 2

- Processes P0, P1, P2, P3, P4

Alloc		
A	B	C
1	1	2
2	1	2
4	0	1
0	2	0
1	1	2

Max		
A	B	C
4	3	3
3	2	2
9	0	2
7	5	3
1	1	3

Need			
Process	A	B	C
P0	3	2	1
P1	1	1	0
P2	5	0	1
P3	7	3	3
P4	0	0	0

Bankers Algorithm – Example 2

- Processes P0, P1, P2, P3, P4

Available			
Time	**A**	**B**	**C**
0	2	1	0
1	4	2	2
2	6	4	6
3	10	4	7
4	10	6	7

Safe sequence: P1, P4, P0, P2, P3

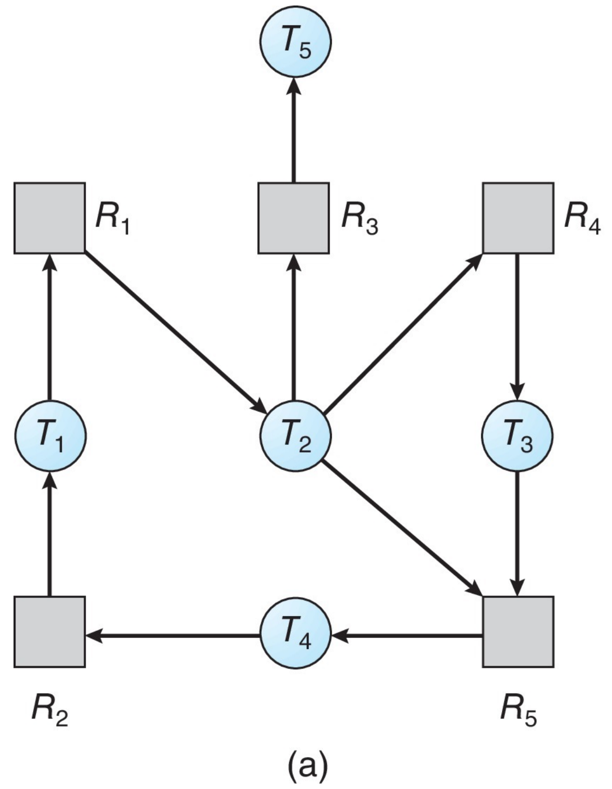
Deadlock Detection

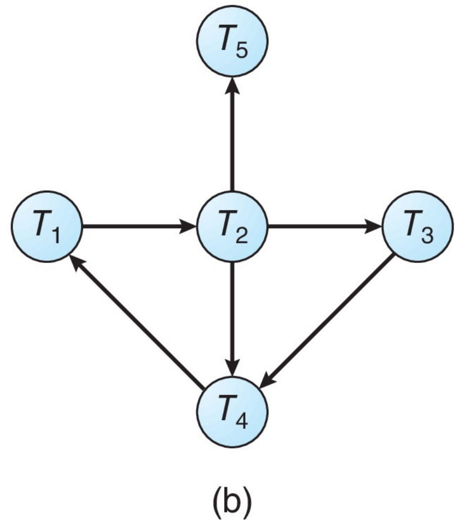
- Some systems do not have deadlock avoidance and prevention. We need a way to combat this scenario.
- Allow system to enter deadlock state
- Detection algorithm
- Recovery scheme

Single Instance of Each Resource Type

- Maintain **wait-for** graph
  - Nodes are processes
  - $P_i \rightarrow P_j$ if P_i is waiting for P_j
- Periodically invoke an algorithm that searches for a cycle in the graph. If there is a cycle, there exists a deadlock
- An algorithm to detect a cycle in a graph requires an order of n^2 operations, where n is the number of vertices in the graph

Resource-Allocation Graph and Wait-for Graph





Resource-Allocation Graph

Corresponding wait-for graph

Detection-Algorithm Usage

- When, and how often, to invoke depends on:
  - How often a deadlock is likely to occur?
  - How many processes will need to be rolled back?
    - one for each disjoint cycle
- If detection algorithm is invoked arbitrarily, there may be many cycles in the resource graph and so we would not be able to tell which of the many deadlocked processes “caused” the deadlock.
- Cannot invoke every time a resource is requested. -> Increases computation overhead.
- Solution: Run periodically or when CPU utilization is low.
  - Deadlocks typically decrease CPU utilization

Recovery from Deadlock: Process Termination

- Many ways to recover from deadlock.
  - Abort all deadlocked processes
  - Abort one process at a time until the deadlock cycle is eliminated
  - Resource preemption
- Aborting is not an arbitrary task. Need to consider many factors.
- In which order should we choose to abort?
  1. Priority of the process
  2. How long process has computed, and how much longer to completion
  3. Resources the process has used
  4. Resources process needs to complete
  5. How many processes will need to be terminated
  6. Is process interactive or batch?

Recovery from Deadlock: Resource Preemption

- **Selecting a victim** – minimize cost
  - Cost is computed as a function as
    - # of resources held
    - Amount of time consumed
- **Rollback** – return to some safe state, restart process for that state
  - Total rollback -> abort process and restart.
    - To be used when a previous safe state is ambiguous.
- **Starvation** – same process may always be picked as victim, include number of rollback in cost factor