



操作系统 Operating System

第四章 进程与并发程序设计(6) ——死锁

沃天宇

woty@buaa.edu.cn

2024年4月26日





内容提要

- 死锁的概念
- 处理死锁的基本方法
- 小结





亿房网
www.fdc.com.cn

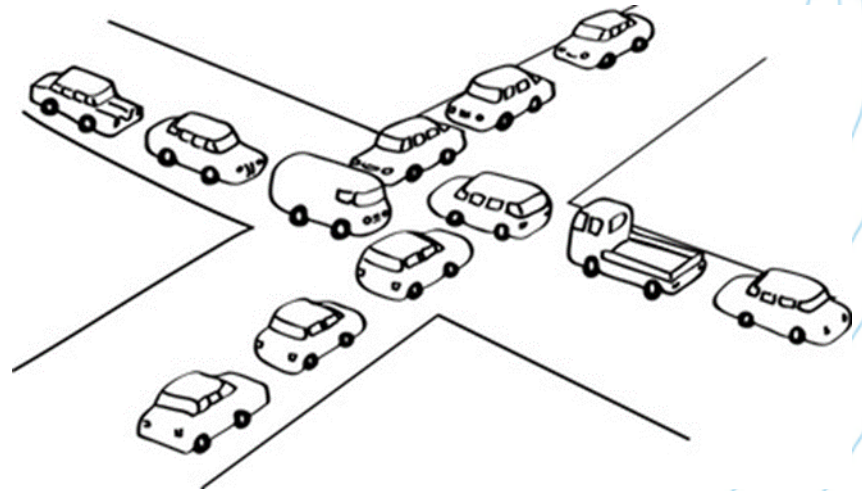
死锁问题 (Deadlock)

死锁定义：

- 一组进程中，每个进程都无限等待被该组进程中其它进程所占有的资源，在无外力介入的条件下，将因永远分配不到资源而无法运行的现象。
 - 浪费大量系统资源
 - 甚至导致系统崩溃

死锁发生原因

- 资源竞争
- 并发执行的顺序不当





死锁的例子

进程P1

...

申请文件F

申请打印机T

...

释放打印机T

释放文件F

...

进程P2

...

申请打印机T

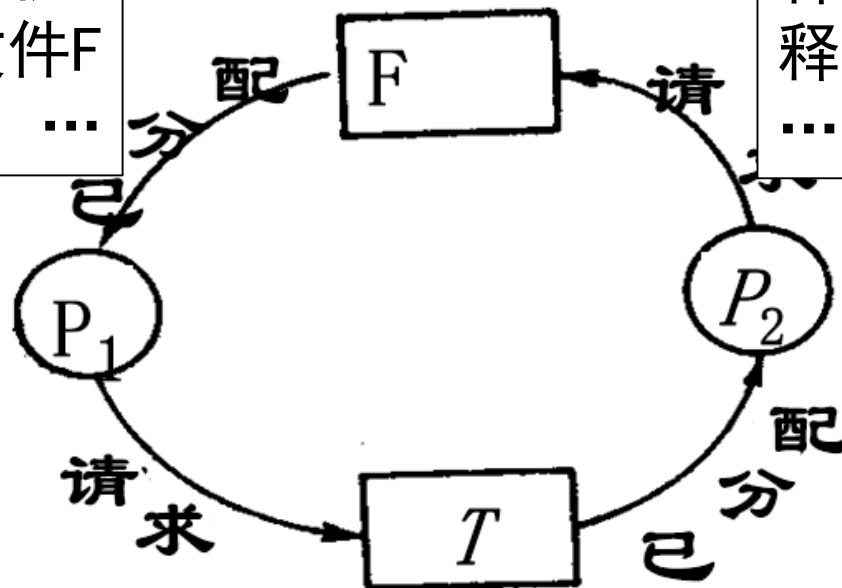
申请文件F

...

释放文件F

释放打印机T

...



简单的死锁例子

竞争资源引起死锁

- **可剥夺资源**：是指某进程在获得这类资源后，该资源可以再被其他进程或系统剥夺。如**CPU，内存**；
- **非可剥夺资源**：当系统把这类资源分配给某进程后，再不能强行收回，只能在进程用完后自行释放。如**磁带机、打印机**；
- **临时性资源**：这是指由一个进程产生，被另一个进程使用，短时间后便无用的资源，故也称为消耗性资源。如**消息、中断**；

临时性资源竞争示例

例如，S1，S2，S3是临时性资源，进程P1产生消息S1，又要求从P3接收消息S3；进程P3产生消息S3，又要求从进程P2处接收消息S2；进程P2产生消息S2，又要求从P1处接收产生的消息S1。如果消息通信按如下顺序进行：

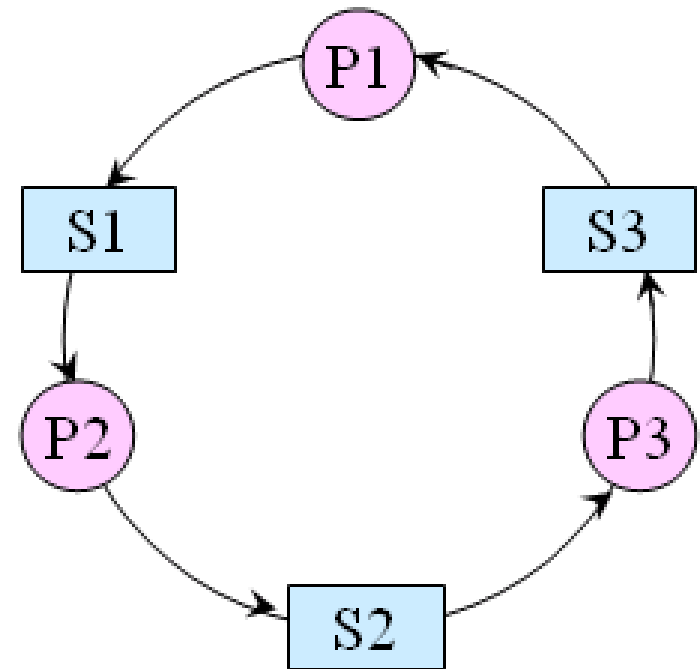
P1: Release (S1) ; Request (S3) ;
P2: Release (S2) ; Request (S1) ;
P3: Release (S3) ; Request (S2) ;

并不会发生死锁。

若改成下述的运行顺序：

P1: Request (S3) ; Release (S1) ;
P2: Request (S1) ; Release (S2) ;
P3: Request (S2) ; Release (S3) ;

则可能发生死锁。



使用信号量实现汇合(Rendezvous)

- 使用信号量实现线程A和线程B的汇合 (Rendezvous)。使得a1永远在b2之前执行，而b1永远在a2之前执行。
- 定义两个信号量，aArrived, bArrived, 并且初始化为0，表示a和b是否执行到汇合点。

Thread A

```
1 statement a1
2 bArrived.wait()
3 aArrived.signal()
4 statement a2
```

Thread B

```
1 statement b1
2 aArrived.wait()
3 bArrived.signal()
4 statement b2
```

死锁版本

- # V(mutex)



哲学家就餐问题

Var chopstick : array[0..4] of semaphore;

P(chopstick[i]);

P(chopstick[(i+1)mod 5]);

eat

V(chopstick[i]);

V(chopstick [(i+1)mod 5]);

think

同时拿起右边的筷子，等待左边筷子，发生死锁！

死锁发生的四个必要条件

1. **互斥条件**：指进程对所分配到的资源进行排它性使用，即在一段时间内某资源只由一个进程占用。如果此时还有其它进程请求资源，则请求者只能等待，直至占有资源的进程用毕释放。
2. **请求且占有条件**：指进程已经占有至少一个资源，但又提出了新的资源请求，而该资源已被其它进程占有，此时请求进程阻塞，但又对自己已获得的其它资源保持不放。
3. **不可剥夺条件**：指进程已获得的资源，在未使用完之前，不能被剥夺，只能在使用完时由自己释放。
4. **环路等待条件**：指在发生死锁时，必然存在一个进程——资源的环形链，即进程集合 $\{P_0, P_1, P_2, \dots, P_n\}$ 中的 P_0 正在等待一个 P_1 占用的资源； P_1 正在等待 P_2 占用的资源，……， P_n 正在等待已被 P_0 占用的资源。

活锁和饥饿

- **活锁 (livelock)**：是指任务或者执行者没有被阻塞，由于某些条件没有满足，导致一直重复尝试，失败，尝试，失败。
 - 活锁和死锁的区别在于，处于活锁的实体是在不断的改变状态，即所谓的“活”，而处于死锁的实体表现为等待；活锁有可能自行解开，死锁则不能。避免活锁的简单方法是采用先来先服务的策略。
- **饥饿 (starvation)**：某些进程可能由于资源分配策略的不公平导致长时间等待。当等待时间给进程推进和响应带来明显影响时，称发生了进程饥饿，当饥饿到一定程度的进程所赋予的任务即使完成也不再具有实际意义时称该进程被饿死(starve to death)。



内容提要

- 死锁的概念
- 处理死锁的基本方法
 - 死锁预防 (Deadlock Prevention)
 - 死锁避免 (Deadlock Avoidance)
 - 死锁检测 (Deadlock Detection)
- 小结

处理死锁方法

• 不允许死锁发生

- 预防死锁（静态）：防患于未然，破坏死锁的产生条件
- 避免死锁（动态）：在资源分配之前进行判断

• 允许死锁发生

- 检测与解除死锁
- 无所作为：鸵鸟算法

条件要求

死锁预防（1/4）

1. **打破互斥条件**：即允许进程同时访问某些资源。但是，有的资源是不允许被同时访问的，像打印机等等，这是资源本身的属性。
2. **打破申请且占有条件**：可以实行资源预先分配策略。只有当系统能够满足当前进程的全部资源需求时，才一次性地将所申请的资源全部分配给该进程，否则不分配任何资源。由于运行的进程已占有了它所需的全部资源，所以不会发生占有资源又申请资源的现象，因此不会发生死锁。

死锁预防 (2/4)

但是，这种策略也有如下缺点：

- a) 在许多情况下，由于进程在执行时是动态的，**不可预测**的，因此不可能知道它所需要的全部资源。
- b) **资源利用率低**。无论资源何时用到，一个进程只有在占有所需的全部资源后才能执行。即使有些资源最后才被用到一次，但该进程在生存期间却一直占有。这显然是一种极大的资源浪费；
- c) **降低进程的并发性**。因为资源有限，又加上存在浪费，能分配到所需全部资源的进程个数就必然少了。



死锁预防（3/4）

3. **打破不可剥夺条件**：即允许进程强行从占有者那里夺取某些资源。就是说，当一个进程已占有了某些资源，它又申请新的资源，当不能立即被满足时，须释放所占有的全部资源，以后再重新申请。它所释放的资源可以分配给其它进程。这就相当于该进程占有的资源被隐蔽地抢占了。这种预防死锁的方法实现起来困难，会降低系统性能。



死锁预防（4/4）

4. **打破循环等待条件**：实行资源有序分配策略。即把资源事先分类编号，按号分配，使进程在申请，占用资源时不会形成环路。所有进程对资源的请求必须严格按资源序号递增的顺序提出。进程占用了小号资源，才能申请大号资源，就不会产生环路，从而预防了死锁。这种策略与前面的策略相比，资源的利用率和系统吞吐量都有很大提高，但存在以下缺点：

- a) 限制了进程对资源的请求，同时给系统中所有资源合理编号也是件困难事，并**增加了系统开销**；
- b) 为了遵循按编号申请的次序，暂不使用的资源也需要提前申请，从而**增加了进程对资源的占用时间**。



有序资源分配法示例

例如：进程PA，使用资源的顺序是R1，R2；
进程PB，使用资源的顺序是R2，R1。

采用有序资源分配法：R1的编号为1，R2的编号为2；

PA：申请次序应是：R1，R2；

PB：申请次序应是：R1，R2。

死锁避免

- **死锁预防**是排除死锁的**静态策略**，它使产生死锁的四个必要条件不能同时具备，从而对进程申请资源的活动加以限制，以保证死锁不会发生。
- **死锁避免**是排除死锁的**动态策略**，它不限制进程有关资源的申请，而是对进程所发出的每一个申请资源命令加以动态地检查，并根据检查结果决定是否进行资源分配。即分配资源时判断是否会出现死锁，有则加以避免。如不会死锁，则分配资源。
- 死锁避免不那么严格限制产生死锁的四个必要条件（区别于死锁预防）

安全序列

- **安全序列的定义**：一个进程序列 $\langle P_1, P_2, \dots, P_n \rangle$ 是安全的，是指若对于每一个进程 P_i ，它需要的**附加资源**可以被系统中当前可用资源加上所有进程 P_j ($j < i$) 当前占有资源之和所满足，则 $\langle P_1, P_2, \dots, P_n \rangle$ 为一个安全序列。
- 如果系统不存在这样一个安全序列，则系统是不安全的。

安全状态

- 安全状态：系统存在一个安全序列 $\langle P_1, P_2, \dots, P_n \rangle$ （则所有进程均可顺利完成）
- 不安全状态：不存在可完成的序列
- 系统进入不安全状态（四个死锁的必要条件同时发生）也未必会产生死锁。当然，产生死锁后，系统一定处于不安全状态。

安全状态

不安全状态

死锁状态



安全状态示例

已有数量 最大需求

A	3	9
B	2	4
C	2	7

空闲：3

A	3	9
B	4	4
C	2	7

空闲：1

A	3	9
B	0	—
C	2	7

空闲：5

A	3	9
B	0	—
C	7	7

空闲：0

A	3	9
B	0	—
C	0	—

空闲：7

安全

已有数量 最大需求

A	3	9
B	2	4
C	2	7

空闲：3

A	4	9
B	2	4
C	2	7

空闲：2

A	4	9
B	4	4
C	2	7

空闲：0

A	4	9
B	0	—
C	2	7

空闲：4

不安全

原因：为进程A分配了资源导致

银行家算法

- 银行家算法 (Dijkstra, 1965)
 - 一个银行家把他的固定资金 (**capital**) 贷给若干顾客。只要不出现一个顾客借走所有资金后还不够, 银行家的资金应是安全的。银行家需一个算法保证借出去的资金在有限时间内可收回。
- 为了保证资金的安全, 银行家规定:
 - 当一个顾客对资金的最大需求量不超过银行家现有资金时就可接纳顾客
 - 顾客可以分期贷款, 但贷款总数不能超过最大需求量
 - 当银行家现有的资金不能满足顾客尚需的贷款数额时, 对顾客的贷款可推迟支付, 但总能使顾客在有限的时间里得到贷款
 - 当顾客得到所需的全部资金后, 一定能在有限的时间里归还所有的资金

具体算法

- 假定顾客借款分成若干次进行；并在第一次借款时，能说明他的最大借款额。

具体算法：


- 顾客的借款操作依次顺序进行，直到全部操作完成；
- 银行家对当前顾客的借款操作进行判断，以确定其安全性（能否支持顾客借款，直到全部归还）；
- 安全时，贷款；否则，暂不贷款。

具体算法

- n 为进程数量， m 为资源类型数量
- 可利用资源向量**Available**: m 维向量
 - 具有 m 个元素的向量，其中每一个元素代表一类可利用的资源数目，其初值是系统中所配置的该类全部可用资源数目。如果 $\text{Available}[j]=k$ ，表示系统中现有 R_j 类资源 k 个。
- 最大需求矩阵**Max**: $n \times m$ 矩阵
 - 定义了系统中 n 个进程中的每一个进程对 m 类资源的最大需求。如果 $\text{Max}(i, j)=k$ ，表示进程 i 需要 R_j 类资源的最大数目为 k 。

具体算法

- 分配矩阵Allocation: $n \times m$ 矩阵
 - 定义了系统中每一类资源当前已分配给每一进程的资源数。如果Allocation(i, j)= k , 表示进程*i*当前已分得 R_j 类资源*k*个。
- 需求矩阵Need: $n \times m$ 矩阵
 - 表示每一个进程尚需的各类资源数。如果Need(i, j)= k , 表示进程*i*还需要 R_j 类资源*k*个, 方能完成其任务。


$$\text{Need}(i, j) = \text{Max}(i, j) - \text{Allocation}(i, j)$$

银行家算法

- 设 $Request_i$ 是进程 P_i 的请求向量，如果进程 P_i 需要 K 个 R_j 类资源，当 P_i 发出资源请求后，系统按下述步骤进行检查：
 - 1 如果 $Request_i \leq Need_i$ ，则转向步骤2；否则认为出错。（因为它所需要的资源数已超过它所宣布的最大值）
 - 2 如果 $Request_i \leq Available$ ，则转向步骤3；否则，表示系统中尚无足够的资源， P_i 必须等待
 - 3 系统试探把要求的资源分配给进程 P_i ，并修改下面数据结构中的数值：
$$Available := Available - Request_i;$$
$$Allocation := Allocation + Request_i;$$
$$Need_i := Need_i - Request_i;$$
 - 4 系统执行安全性算法，检查此次资源分配后，系统是否处于安全状态。若安全，正式将资源分配给进程 P_i ，以完成本次分配；否则，将试探分配作废，恢复原来的资源分配状态，让进程 P_i 等待。



安全性算法

1 设置两个向量

- 工作向量**Work**: 它表示系统可提供给进程继续运行所需要的各类资源的数目, 它含有 m 个元素, 执行安全算法开始时, **Work:=Available**。
- **Finish**: 它表示系统是否有足够的资源分配给进程, 使之运行完成。开始时先做**Finish[i]:=false**; 当有足够的资源分配给进程时, 令**Finish[i]:=true**。

2 从进程集合中找到一个能满足下述条件的进程:

- **Finish[i]=false; Need_i≤Work**. 如找到, 执行步骤3; 否则执行步骤4。

3 当进程P_i获得资源后, 可顺利执行, 直至完成, 并释放出分配给它的资源, 故执行:

- **Work:=Work+Allocation; Finish[i]:=true; Goto step2;**

4 如果所有进程的**Finish[i]=true**, 则表示系统处于安全状态; 否则, 系统处于不安全状态。



银行家算法示例

- 假定系统中有五个进程{P0、P1、P2、P3、P4}和三种类型的资源{A, B, C}, 每一种资源的数量分别为10、5、7, 在T0时刻的资源分配情况如下表所示:

资源情况 进程	Max			Allocation			Need			Available		
	A	B	C	A	B	C	A	B	C	A	B	C
P0	7	5	3	0	1	0	7	4	3	3	3	2
P1	3	2	2	2	0	0	1	2	2			
P2	9	0	2	3	0	2	6	0	0			
P3	2	2	2	2	1	1	0	1	1			
P4	4	3	3	0	0	2	4	3	1			

10,5 7

资源情况 进程		最大值	已分配	还需要	可用
		Max	Allocation	Need	Available
		A B C	A B C	A B C	A B C
P0		7 5 3	0 1 0	7 4 3	3 3 2
P1		3 2 2	2 0 0	1 2 2	
P2		9 0 2	3 0 2	6 0 0	
P3		2 2 2	2 1 1	0 1 1	
P4		4 3 3	0 0 2	4 3 1	

工作向量Work. 它表示系统可提供给进程继续运行所需要的各类资源的数目

资源情况 进程		work	Need	Allocation	Work+Alloc	finish
		A B C	A B C	A B C	A B C	
P1		3 3 2	1 2 2	2 0 0	5 3 2	true
P3		5 3 2	0 1 1	2 1 1	7 4 3	true
P4		7 4 3	4 3 1	0 0 2	7 4 5	true
P2		7 4 5	6 0 0	3 0 2	10 4 7	true
P0		10 4 7	7 4 3	0 1 0	10 5 7	true



假定系统中有五个进程{P0、P1、P2、P3、P4}和三种类型的资源{A, B, C}，每一种资源的数量分别为10、5、7，在T0时刻的资源分配情况如图

请找出该表中T0时刻以后存在的安全序列（至少2种）

资源情况 进程	Max			Allocation			Need			Available		
	A	B	C	A	B	C	A	B	C	A	B	C
P0	7	5	3	0	1	0	7	4	3	3	3	2
P1	3	2	2	2	0	0	1	2	2			
P2	9	0	2	3	0	2	6	0	0			
P3	2	2	2	2	1	1	0	1	1			
P4	4	3	3	0	0	2	4	3	1			

- 如果P4请求分配 (3,3,0)，是否可以？
- 如果P0请求分配 (0,2,0)，是否可以？



银行家算法的特点

- 允许互斥、部分分配和不可抢占，可提高资源利用率；
- 要求事先说明最大资源要求，在现实中很困难；

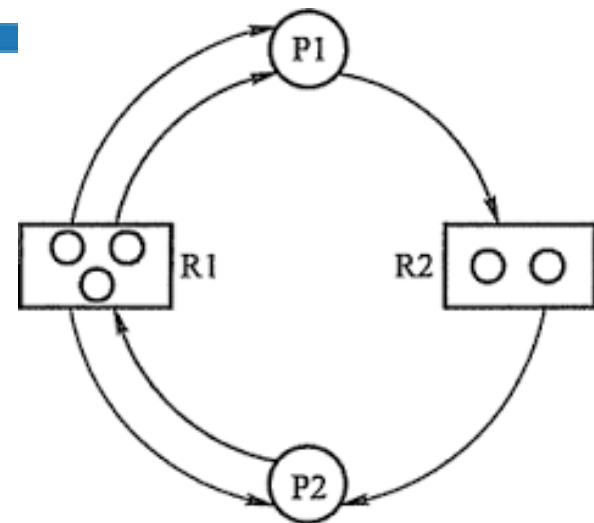
死锁检测

- 保存资源的请求和分配信息，利用某种算法对这些信息加以检查，以判断是否存在死锁。死锁检测算法主要是检查是否有循环等待。
- 在UNIX系统中，PS命令；Windows中的任务管理器



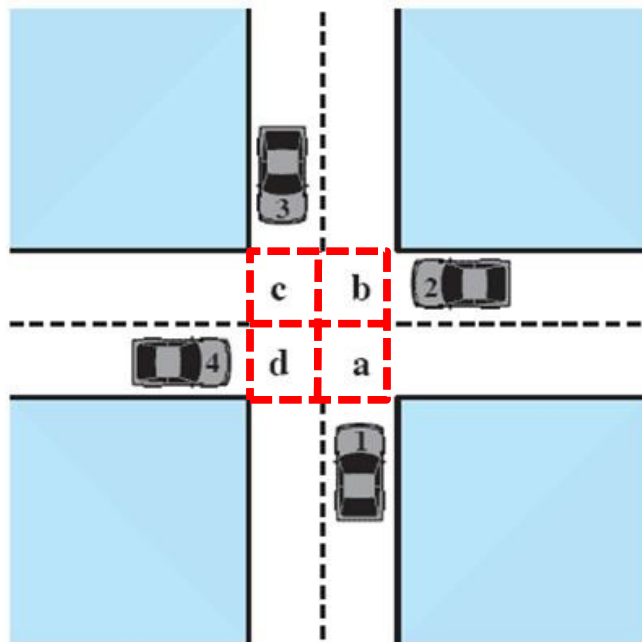
资源分配图/进程-资源图

- 用有向图描述系统资源和进程的状态。二元组 $G = (N, E)$,
 N : 结点的集合, $N = P \cup R$ 。
- P 为进程, R 为资源, $P = \{p_1, p_2, \dots, p_n\}$, $R = \{r_1, r_2, \dots, r_m\}$,
 两者为互斥资源。
- E : 有向边的集合, $e \in E$, $e = (p_i, r_j)$ 或 $e = (r_j, p_i)$ 。
 - $e = (p_i, r_j)$ 是请求边, 进程 p_i 请求一个单位的 r_j 资源;
 - $e = (r_j, p_i)$ 是分配边, 为进程 p_i 分配了一个单位的 r_j 资源。
- 在资源分配图中, 圆圈表示进程, 矩形表示一类资源, 矩形中的小圈代表每个资源。



如何用描述该死锁问题？

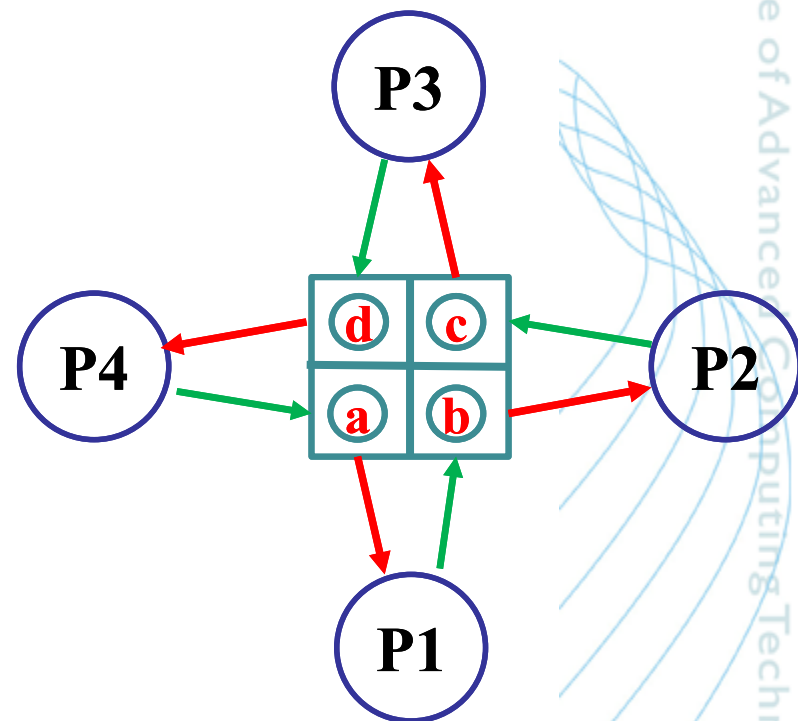
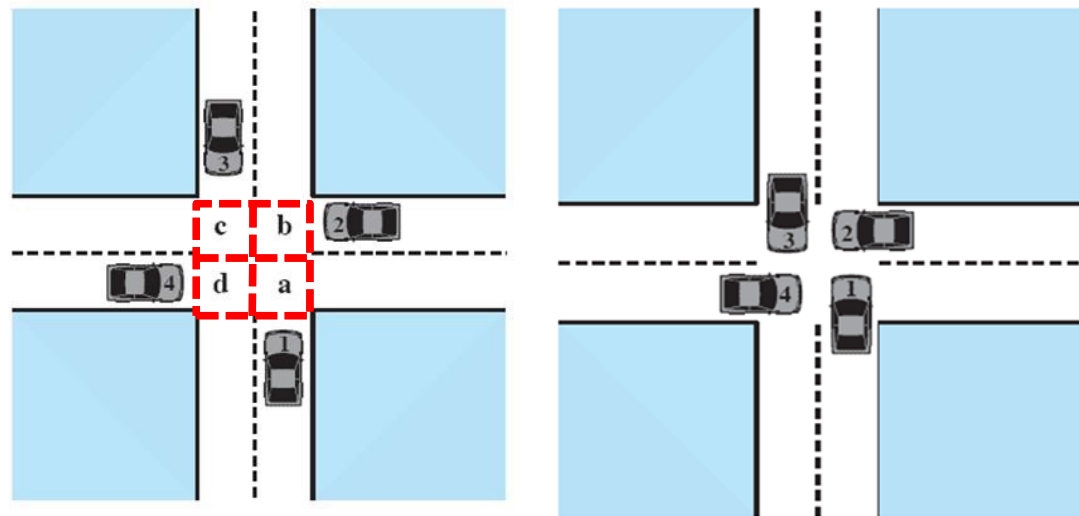
假设是双向车道：



- 路口可以分成四个方格，每个方格是一个资源 R_a, R_b, R_c, R_d ;
- 东西南北四个方向的车辆相当于四个进程 P_1, P_2, P_3, P_4 ;
- 每个车辆要通过路口需要占用两个资源。

如何用描述该死锁问题？

- 当每辆车都驶入路口，相当于占用了资源，出现环路时，产生了死锁。



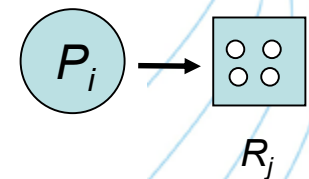
资源分配图（RAG）算法

- **RAG（Resource Allocation Graph）**
- 有向图G的顶点为资源或进程，从资源R到进程P的边表示R已分配给P，从进程P到资源R的边表示P正因请求R而处于等待状态。

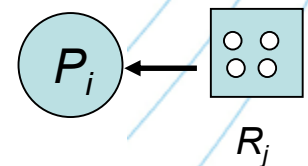
进程：

资源：

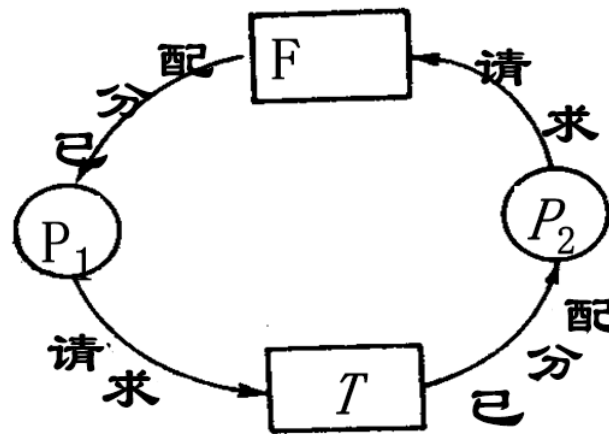
进程请求资源：



进程已分配资源：

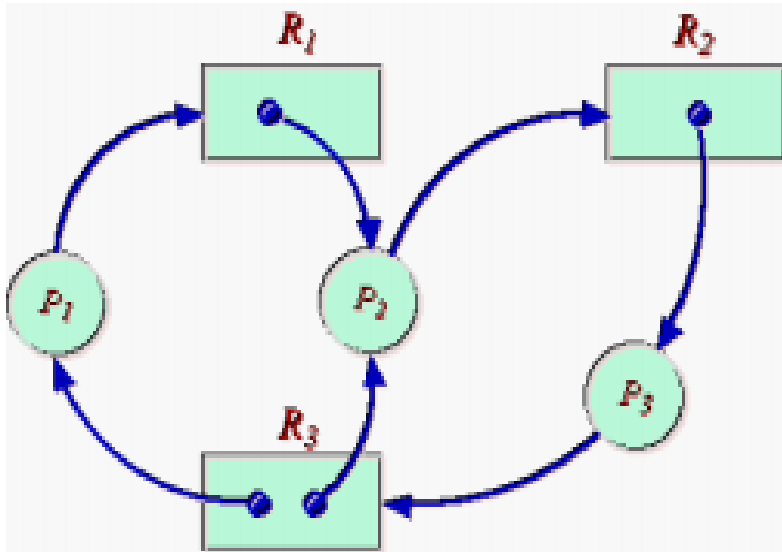


思考：如果一个资源分配图中存在环路，是否一定存在死锁？

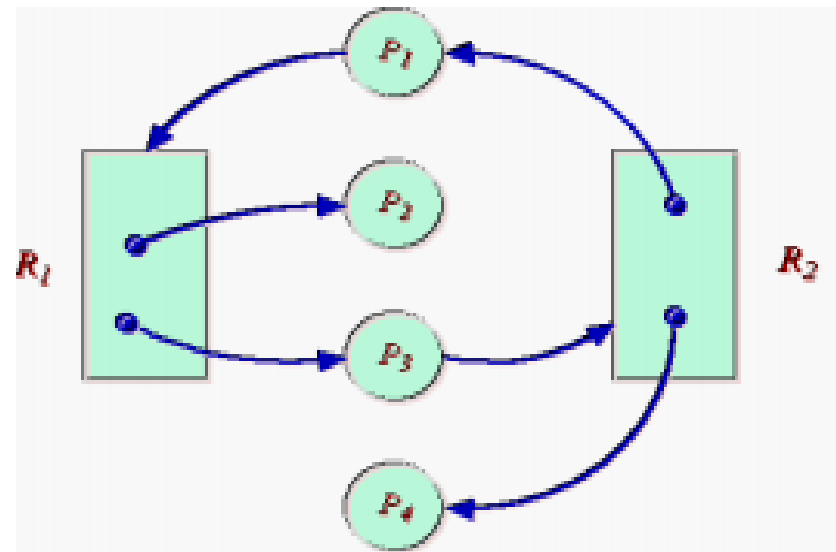


简单的死锁例子

“环”与死锁



有环有死锁



有环无死锁



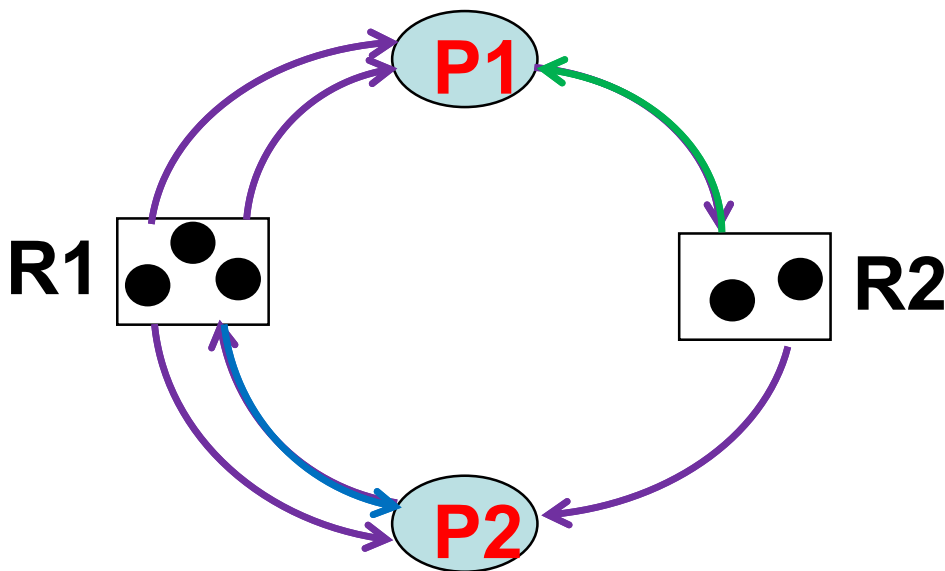
- **封锁进程**：是指某个进程由于请求了超过了系统中现有的未分配资源数目的资源，而被系统封锁的进程。
- **非封锁进程**：即没有被系统封锁的进程
- **资源分配图的化简方法**：假设某个RAG中存在一个进程 P_i ，此刻 P_i 是非封锁进程，那么可以进行如下化简：
 - 当 P_i 有请求边时，首先将其请求边变成分配边(即满足 P_i 的资源请求)，而一旦 P_i 的所有资源请求都得到满足， P_i 就能在有限的时间内运行结束，并释放其所占用的全部资源，此时 P_i 只有分配边，删去这些分配边（实际上相当于消去了 P_i 的所有请求边和分配边），使 P_i 成为孤立结点。（反复进行）



死锁定理:

系统中某个时刻 t 为死锁状态的充要条件是 t 时刻系统的资源分配图是不可完全化简的。

在经过一系列的简化后，若能消去图中的所有边，使所有的进程都成为孤立结点，则称该图是**可完全化简的**；反之的是**不可完全化简的**。



死锁解除

- 死锁解除重要的是以最小的代价恢复系统的运行,死锁解除后,释放资源的进程应恢复它原来的状态,才能保证该进程的执行不会出现错误
- 两种方法: 资源剥夺法、撤销进程法
 - **撤销进程**: 使全部死锁的进程夭折掉; 按照某种顺序逐个地撤销(回退)进程,直至有足够的资源可用,死锁状态消除为止,
 - **剥夺资源**: 使用挂起/激活挂起一些进程,剥夺它们的资源以解除死锁,待条件满足时,再激活进程。

死锁解除

- 实质：如何让释放资源的进程能够继续运行
 - 选择一个牺牲进程
 - 重新运行或回退到某一点开始继续运行
 - 回退到足以解除死锁即可
- 须注意的问题：
 - 怎样保证不发生“饥饿”现象，如何保证并不总是剥夺同一进程的资源
 - “最小代价”，即最经济合算的算法，使得进程回退带来的开销最小。



★死锁检测、预防和避免方法小结

原则	资源分配策略	不同方案	主要优点	主要缺点
预防	保守的；预提交资源，导致资源闲置	一次性请求所有资源	<ul style="list-style-type: none">对执行一连串活动（突发式处理）的进程非常有利不需要抢占	<ul style="list-style-type: none">低效，延迟进程的初始化须知道未来的资源情况资源利用率低
		抢占	对状态易于保存和恢复的资源非常方便	<ul style="list-style-type: none">可能导致过于频繁的抢占
		资源排序	可在系统设计时解决，在编译时实施。	<ul style="list-style-type: none">不便灵活申请新资源
避免	是“预防”与“检测”的折衷	通过资源需求检查以发现至少一条安全路径	不需要抢占	<ul style="list-style-type: none">须知道未来资源的需求，进程可能被长时间阻塞
检测	宽松的；，只要可能，请求的资源都允许	周期性地调用以检测死锁	<ul style="list-style-type: none">不会延迟进程的初始化易于在线处理	<ul style="list-style-type: none">通过抢占解除死锁，可能造成损失

哲学家就餐问题

```
semaphore fork [5] = {1};
int i;
void philosopher (int i)
{
    while (true) {
        think();
        P (fork[i]);
        P (fork [(i+1) mod 5]);
        eat();
        V (fork [(i+1) mod 5]);
        V (fork[i]);
    }
}
void main()
{
    parbegin (philosopher (0), philosopher (1), philosopher (2),
philosopher (3), philosopher (4));
}
```

产生死锁?

讨论：哲学家就餐问题

• 如何破解死锁？

– 允许死锁发生

- 无所作为？
- 检测与修复？

– 不允许死锁发生

- 动态避免？

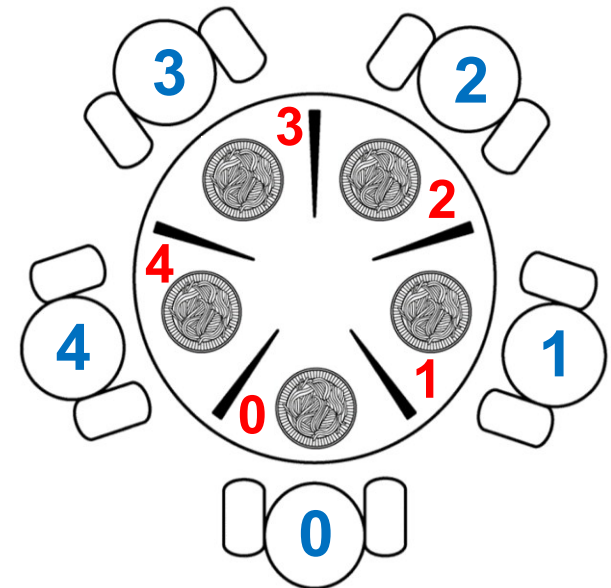
• 静态防止？

- 增加资源或者共享资源？
- 可以抢占？
- 杜绝循环等待？
- 杜绝保持或者等待？

这是什么破解死锁方法？

Try to grab chopstick either:

- Not last chopstick
- Is last chopstick but someone will have two afterwards



哲学家就餐问题的解题思路

- 至多只允许四个哲学家同时（尝试）进餐,以保证至少有一个哲学家能够进餐,最终总会释放出他所使用过的两支筷子,从而可使更多的哲学家进餐。设置信号量 $room=4$ 。（破除**循环等待**）
- 对筷子进行编号，奇数号先拿左，再拿右；偶数号相反。（破除**循环等待**）
- 同时拿起两根筷子，否则不拿起。（一次性分配，破除**保持等待**）

为防止死锁发生可采取的措施

```
semaphore fork[5] = {1};
semaphore room = {4};
int i;
void philosopher (int i)
{
    while (true) {
        think();
        P (room);
        P (fork[i]);
        P (fork [(i+1) mod 5]);
        eat();
        V (fork [(i+1) mod 5]);
        V (fork[i]);
        V (room);
    }
}
void main()
{
    parbegin ( philosopher (0), philosopher (1), philosopher (2),
philosopher(3), philosopher (4) );
}
```

最多允许4个
哲学家同时坐
在桌子周围



思考

1. 在某系统中，3个进程共享4台同类型的设备资源，这些资源一次只能一台一台地为进程服务和释放，每个进程最多需要2台设备资源，试问在系统中是否会产生死锁？
2. 某系统中有 n 个进程和 m 台打印机，系统约定：打印机只能一台一台地申请、一台一台地释放。如果 n 个进程同时**需要**使用打印机的总数小于 $m+n$ ，试讨论，该系统可能发生死锁吗？并简述理由。
3. 仅涉及一个进程的死锁有可能存在吗？为什么？



小结

- 死锁的概念
- 处理死锁的基本方法
 - 预防死锁
 - 避免死锁
 - 检测死锁
 - 解除死锁