Harbin Institute of Technology

数据库系统

万晓珑 博士

大数据计算研究中心

wxl@hit.edu.cn

Harbin Institute of Technology

数据库系统

第十章　数据库恢复技术

第十章 数据库恢复技术

10.1 事务的基本概念

10.2 数据库恢复概述

10.3 故障的种类

10.4 恢复的实现技术

10.5 恢复策略

10.6 具有检查点的恢复技术

10.7 数据库镜像

10.8 小结

10.1 事务的基本概念

1.事务

2.事务的ACID特性

1.事务

- 事务(Transaction)是用户定义的一个数据库操作序列，这些操作要么全做，要么全不做，是一个不可分割的工作单位。
- 事务和程序是两个概念
  - 在关系数据库中，一个事务可以是一条SQL语句，一组SQL语句或整个程序
  - 一个程序通常包含多个事务
- 事务是恢复和并发控制的基本单位

定义事务

❖显式定义方式

BEGIN TRANSACTION
SQL 语句1
SQL 语句2
。。。。。
COMMIT

BEGIN TRANSACTION
SQL 语句1
SQL 语句2
。。。。。
ROLLBACK

❖隐式方式

当用户没有显式地定义事务时，数据库管理系统按缺省规定自动划分事务

事务结束

- **COMMIT**
  - 事务正常结束
  - 提交事务的所有操作（读+更新）
  - 事务中所有对数据库的更新写回磁盘的物理数据库
- **ROLLBACK**
  - 事务异常终止
  - 事务运行的过程中发生了故障，不能继续执行
  - 系统将事务中对数据库的所有已完成的操作全部撤销
  - 事务滚回到开始时的状态

10.1 事务的基本概念

1.事务

2.事务的ACID特性

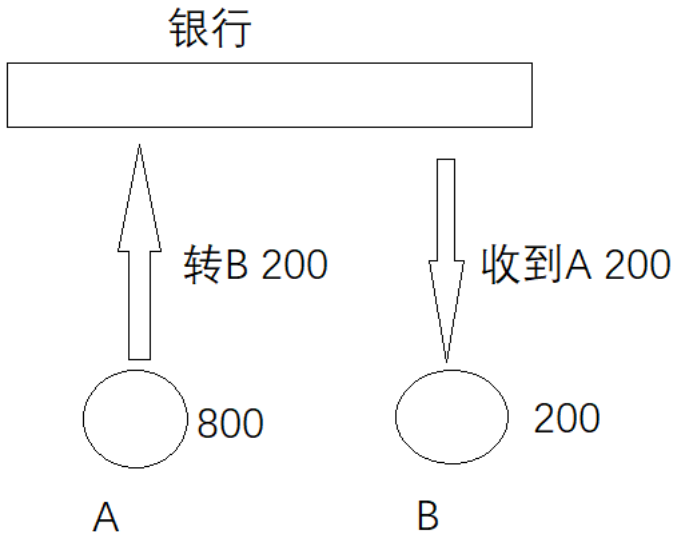
2.事务的特性（ACID特性）

事务的ACID特性：

- 原子性（Atomicity）
- 一致性（Consistency）
- 隔离性（Isolation）
- 持续性（Durability ）

（1）原子性

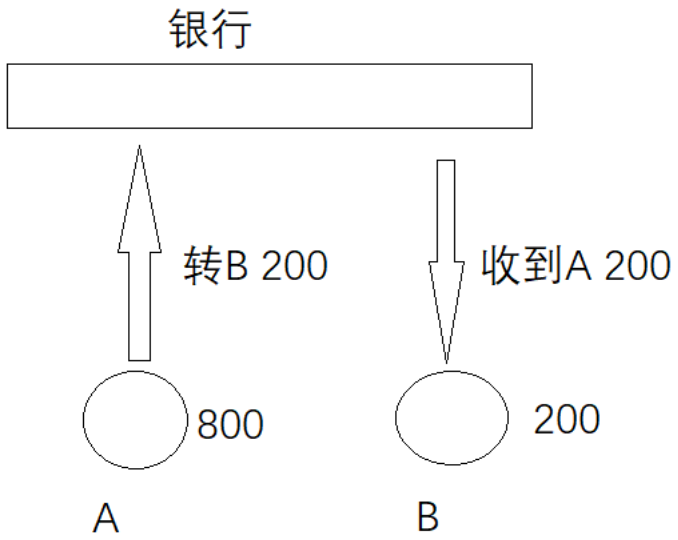
- 事务是数据库的逻辑工作单位
  - 事务中包括的诸操作要么都做，要么都不做



原子性表示，**A: 800-200=600和B:200+200=400**，这两个步骤一起成功，或者一起失败，不能只发生其中一个动作

（2）一致性

- 事务执行的结果必须是使数据库从一个一致性状态变到另一个一致性状态



一致性状态1，操作前：A=800，B=200

一致性状态2，操作后：A=600，B=400

（2）一致性

- 一致性状态
  - 数据库中只包含成功事务提交的结果
- 不一致状态
  - 数据库系统运行中发生故障，有些事务尚未完成就被迫中断；
  - 这些未完成事务对数据库所做的修改有一部分已写入物理数据库，这时数据库就处于一种不正确的状态

一致性与原子性

银行转帐：从帐号A中取出一万元，存入帐号B。

- 定义一个事务，该事务包括两个操作

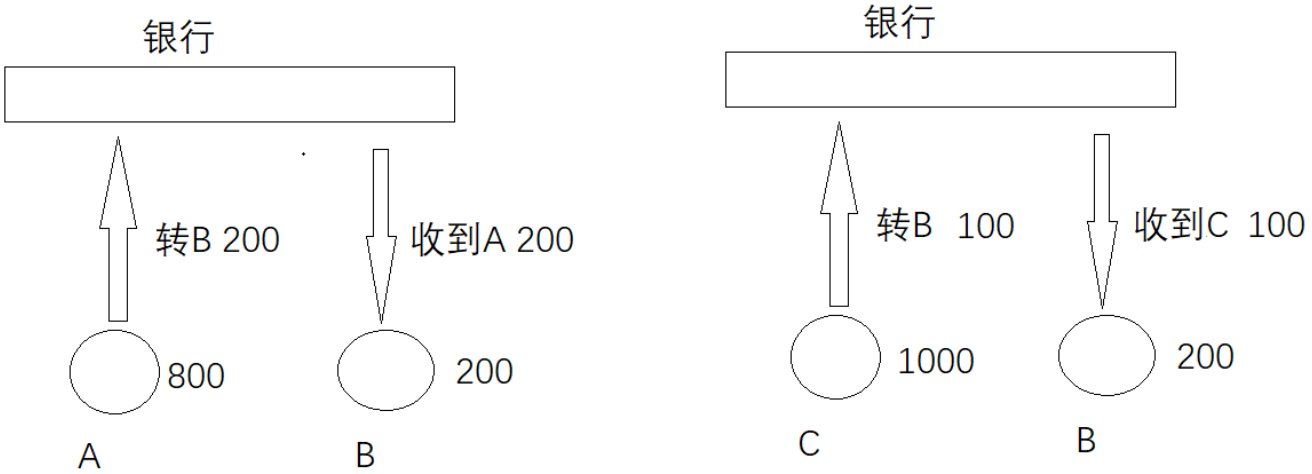
A	B
A=A-1	B=B+1

- 这两个操作要么全做，要么全不做
  - 全做或者全不做，数据库都处于一致性状态。
  - 如果只做一个操作，用户逻辑上就会发生错误，少了一万元，数据库就处于不一致性状态。

（3）隔离性

一个事务的执行不能被其他事务干扰

- 一个事务内部的操作及使用的数据对其他并发事务是隔离的
- 并发执行的各个事务之间不能互相干扰

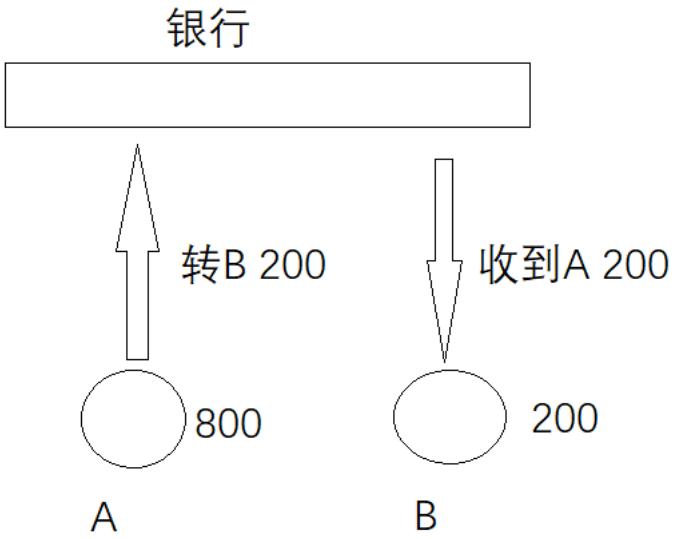


操作后：**A=600，C=900，B=500**

（4）持续性

❖持续性也称永久性（Permanence）

- 一个事务一旦提交，它对数据库中数据的改变就应该是永久性的。接下来的其他操作或故障不应该对其执行结果有任何影响。



- ✓ 操作前A：800，B：200
  操作后A：600，B：400
- ✓ 如果事务还没有提交，服务器宕机或者断电，重启数据库，数据状态为，A：800，B：200
- ✓ 如果事务已经提交，服务器宕机或者断电，重启数据库，数据状态为，A：600，B：400

事务的特性

- 保证事务ACID特性是事务处理(transaction processing)的重要任务
- 破坏事务ACID特性的因素

（1） 多个事务并行运行时，不同事务的操作交叉执行

- 数据库管理系统必须保证多个事务的交叉运行不影响这些事务的隔离性

（2）事务在运行过程中被强行停止

- 数据库管理系统必须保证被强行终止的事务对数据库和其他事务没有任何影响

第十章 数据库恢复技术

10.1 事务的基本概念

10.2 数据库恢复概述

10.3 故障的种类

10.4 恢复的实现技术

10.5 恢复策略

10.6 具有检查点的恢复技术

10.7 数据库镜像

10.8 小结

10.2 数据库恢复概述

- 故障是不可避免的
  - 计算机硬件故障
  - 软件的错误
  - 操作员的失误
  - 恶意的破坏
- 故障的影响
  - 运行事务非正常中断，影响数据库中数据正确性
  - 破坏数据库，全部或部分丢失数据

数据库恢复概述（续）

- 数据库的恢复
  - 数据库管理系统必须具有把数据库从错误状态恢复到某一已知的正确状态(也称为一致状态或完整状态)的功能，这就是数据库的恢复管理系统对故障的对策
- 恢复子系统是数据库管理系统的一个重要组成部分
- 恢复技术是衡量系统优劣的重要指标

第十章 数据库恢复技术

10.1 事务的基本概念

10.2 数据库恢复概述

10.3 故障的种类

10.4 恢复的实现技术

10.5 恢复策略

10.6 具有检查点的恢复技术

10.7 数据库镜像

10.8 小结

故障的种类

1.事务内部的故障

2.系统故障

3.介质故障

4.计算机病毒

1.事务内部的故障

- 事务内部的故障
  - 有的是可以通过事务程序本身发现的(见下面转账事务的例子)
  - 有的是非预期的，不能由事务程序处理的。

事务内部的故障（续）

- 例如，银行转账事务，把一笔金额从账户甲转给账户乙。

```
BEGIN TRANSACTION
    读账户甲的余额BALANCE;
    BALANCE=BALANCE-AMOUNT;    /*AMOUNT 为转账金额*/
    写回BALANCE;
    IF(BALANCE < 0 ) THEN
        {打印‘金额不足，不能转账’;  /*事务内部造成回滚的情况*/
         ROLLBACK; }                  /*撤销刚才的修改，恢复事务*/
    ELSE
        {读账户乙的余额BALANCE1;
         BALANCE1=BALANCE1+AMOUNT;
         写回BALANCE1;
         COMMIT;}
```

事务内部的故障（续）

- 事务内部更多的故障是非预期的，是不能由应用程序处理的。
  - 运算溢出
  - 并发事务发生死锁而被选中撤销该事务
  - 违反了某些完整性限制而被终止等

以后，事务故障仅指这类非预期的故障

事务内部的故障（续）

- 事务故障意味着
  - 事务没有达到预期的终点(COMMIT、或者显式的ROLLBACK)
  - 数据库可能处于不正确状态。
- 事务故障的恢复：事务撤消（UNDO）
  - 强行回滚（ROLLBACK）该事务
  - 撤销该事务已经作出的任何对数据库的修改，使得该事务像根本没有启动一样

2.系统故障

- 系统故障：也称为软故障，是指造成系统停止运转的任何事件，使得系统要重新启动。
  - 整个系统的正常运行突然被破坏
  - 所有正在运行的事务都非正常终止
  - 不破坏数据库
  - 内存中数据库缓冲区的信息全部丢失

系统故障的常见原因

- 特定类型的硬件错误（如CPU故障）
- 操作系统故障
- 数据库管理系统代码错误
- 系统断电

系统故障的恢复

- 发生系统故障，一些尚未完成的事务的结果可能已送入物理数据库，造成数据库可能处于不正确状态。
  - 恢复策略：系统重新启动时，恢复程序让所有非正常终止的事务回滚，强行撤消（UNDO）所有未完成事务

```
BEGIN TRANSACTION
        读账户甲的余额BALANCE;
        BALANCE=BALANCE-AMOUNT;    /*AMOUNT 为转账金额*/
        写回BALANCE;
        IF(BALANCE < 0 ) THEN
          ……
```

系统故障的恢复

- 发生系统故障时，有些已完成的事务可能有一部分甚至全部留在缓冲区，尚未写回到磁盘上的物理数据库中，系统故障使得这些事务对数据库的修改部分或全部丢失
  - 恢复策略：系统重新启动时，恢复程序需要重做（REDO）所有已提交的事务

3.介质故障

- 介质故障：称为硬故障，指外存故障
  - 磁盘损坏
  - 磁头碰撞
  - 瞬时强磁场干扰
- 介质故障破坏数据库或部分数据库，并影响正在存取这部分数据的所有事务
- 介质故障比前两类故障的可能性小得多，但破坏性大得多

4.计算机病毒

- 计算机病毒
  - 一种人为的故障或破坏，是一些恶作剧者研制的一种计算机程序
  - 可以繁殖和传播，造成对计算机系统包括数据库的危害
- 计算机病毒种类
  - 小的病毒只有20条指令，不到50B
  - 大的病毒像一个操作系统，由上万条指令组成

4.计算机病毒

❖CIH、冲击波、熊猫烧香

- **CIH(1998年)：**硬盘数据全部丢失，甚至主板上BIOS中的内容也会被彻底破坏，主机无法启动。
- **冲击波(2003年)：**系统的操作异常，不停地重启。
- **熊猫烧香(2006年)：**C盘、D盘等盘符无法打开，所有exe图标都变成了熊猫。一开机自启动，自添加，自传播。每隔1秒搜索杀毒软件并关闭，每隔6秒删除杀毒软件的注册表键值，每隔10秒下载指定的文件。

计算机病毒（续）

- 计算机病毒的危害
  - 有的病毒传播很快，一旦侵入系统马上摧毁系统
  - 有的病毒有较长的潜伏期，计算机在感染后数天或数月才开始发病
  - 有的病毒感染系统所有的程序和数据
  - 有的只对某些特定的程序和数据感兴趣
- 计算机病毒已成为计算机系统的主要威胁，自然也是数据库系统的主要威胁
- 数据库一旦被破坏仍要用恢复技术把数据库加以恢复

故障小结

- 各类故障，对数据库的影响有两种可能性
  - 一是数据库本身被破坏
  - 二是数据库没有被破坏，但数据可能不正确，这是由于事务的运行被非正常终止造成的。

恢复

- 恢复操作的基本原理：冗余
  - 利用存储在系统别处的冗余数据来重建数据库中已被破坏或不正确的那部分数据
- 恢复的实现技术：比较复杂
  - 一个大型数据库产品，恢复子系统的代码要占全部代码的10%以上

第十章 数据库恢复技术

10.1 事务的基本概念

10.2 数据库恢复概述

10.3 故障的种类

10.4 恢复的实现技术

10.5 恢复策略

10.6 具有检查点的恢复技术

10.7 数据库镜像

10.8 小结

10.4 恢复的实现技术

恢复机制涉及的关键问题

1. 如何建立冗余数据
   - 数据转储（backup）
   - 登记日志文件（logging）
2. 如何利用这些冗余数据实施数据库恢复

10.4 恢复的实现技术

10.4.1 数据转储

10.4.2 登记日志文件

10.4.1 数据转储

1.什么是数据转储

2.转储方法

1.什么是数据转储

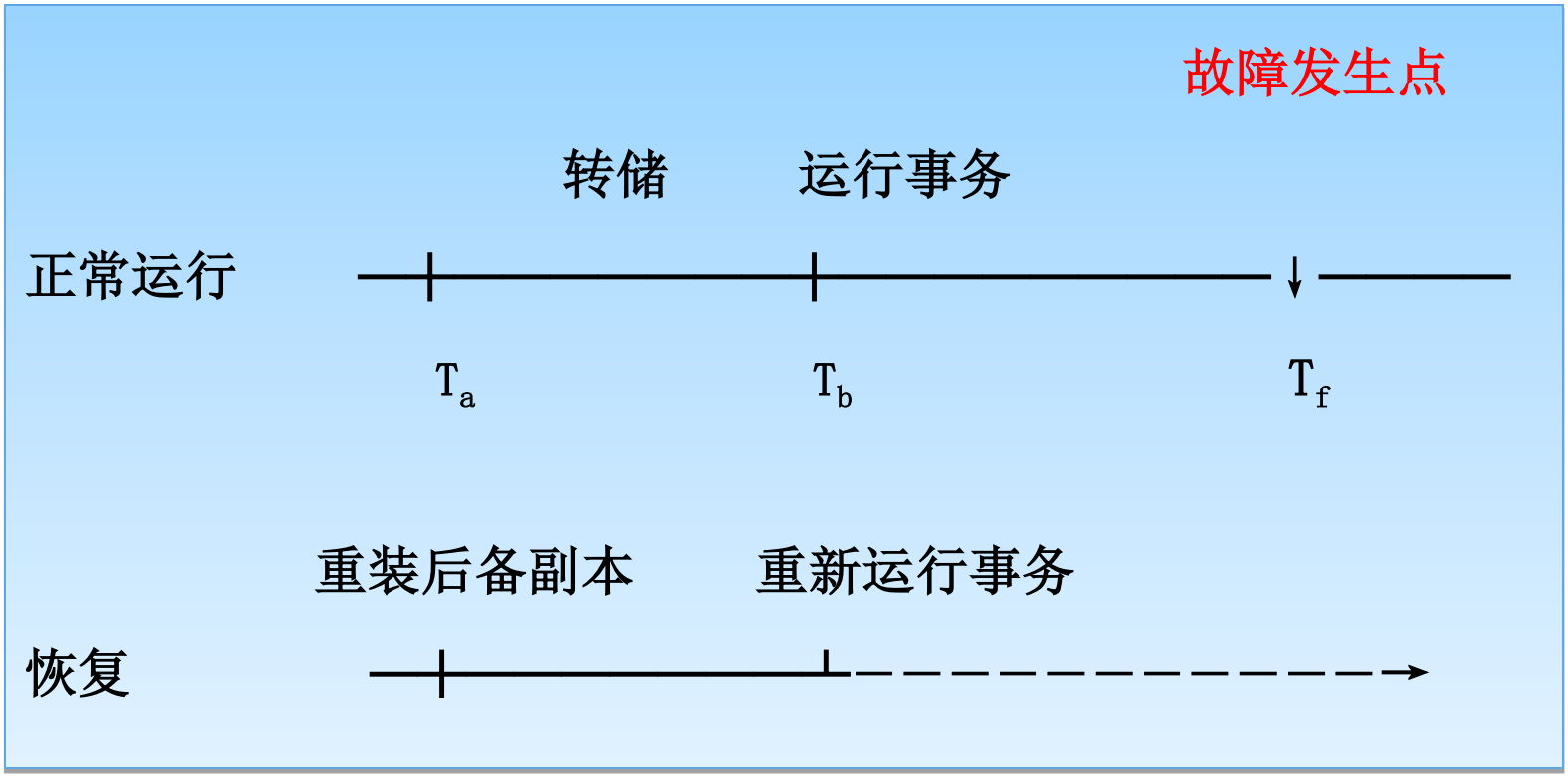
- 转储是指数据库管理员定期地将整个数据库复制到磁带、磁盘或其他存储介质上保存起来的过程
- 备用的数据文本称为**后备副本(backup)或后援副本**

数据转储（续）

- 数据库遭到破坏后可以将后备副本重新装入
- 重装后备副本只能将数据库恢复到转储时的状态
- 要想恢复到故障发生时的状态，必须重新运行自转储以后的所有更新事务

数据转储（续）

[例]



转储和恢复

数据转储（续）

上图中：

- 系统在T_a时刻停止运行事务，进行数据库转储
- 在T_b时刻转储完毕，得到T_b时刻的数据库一致性副本
- 系统运行到T_f时刻发生故障
- 为恢复数据库，首先由数据库管理员重装数据库后备副本，将数据库恢复至T_b时刻的状态
- 重新运行自T_b～T_f时刻的所有更新事务，把数据库恢复到故障发生前的一致状态

2.转储方法

（1）静态转储与动态转储

（2）海量转储与增量转储

（3）转储方法小结

（1）静态转储与动态转储

- 静态转储
  - 在系统中无运行事务时进行的转储操作
  - 转储开始时数据库处于一致性状态
  - 转储期间不允许对数据库的任何存取、修改活动
  - 得到的一定是一个数据一致性的副本
  - 优点：实现简单
  - 缺点：降低了数据库的可用性，转储必须等待正运行的用户事务结束，新的事务必须等转储结束

静态转储与动态转储（续）

- 动态转储
  - 转储操作与用户事务并发进行，转储期间允许对数据库进行存取或修改
  - 优点：不用等待正在运行的用户事务结束，不会影响新事务的运行
  - 缺点：不能保证副本中的数据正确有效
    - 例：在转储期间的某时刻Tc，系统把数据A=100转储到磁带上，而在下一时刻Td，某一事务将A改为200，后备副本上的A过时了

静态转储与动态转储（续）

- 利用动态转储得到的副本进行故障恢复
  - 需要把动态转储期间各事务对数据库的修改活动登记下来，建立日志文件
  - 后备副本加上日志文件就能把数据库恢复到某一时刻的正确状态

（2）海量转储与增量转储

- 海量转储: 每次转储全部数据库
- 增量转储: 只转储上次转储后更新过的数据
- 海量转储与增量转储比较
  - 从恢复角度看，使用海量转储得到的后备副本进行恢复往往更方便
  - 如果数据库很大，事务处理又十分频繁，则增量转储方式更实用更有效

（3）转储方法小结

❖转储方法分类

转储方式	转储状态	
	动态转储	静态转储
海量转储	动态海量转储	静态海量转储
增量转储	动态增量转储	静态增量转储

10.4 恢复的实现技术

10.4.1 数据转储

10.4.2 登记日志文件

10.4.2 登记日志文件

1.日志文件的格式和内容

2.日志文件的作用

3.登记日志文件

1.日志文件的格式和内容

- 什么是日志文件
  - 日志文件(log file)是用来记录事务对数据库的更新操作的文件
- 日志文件的格式
  - 以记录为单位的日志文件
  - 以数据块为单位的日志文件

日志文件的格式和内容（续）

- 以记录为单位的日志文件内容
  - 各个事务的开始标记(BEGIN TRANSACTION)
  - 各个事务的结束标记(COMMIT或ROLLBACK)
  - 各个事务的所有更新操作

  以上均作为日志文件中的一个日志记录 (log record)

日志文件的格式和内容（续）

- 以记录为单位的日志文件，每条日志记录的内容
  - 事务标识（标明是哪个事务）
  - 操作类型（插入、删除或修改）
  - 操作对象（记录ID、Block No.）
  - 更新前数据的旧值（对插入操作，此项为空值）
  - 更新后数据的新值（对删除操作，此项为空值）

日志文件的格式和内容（续）

- 以数据块为单位的日志文件，每条日志记录的内容
  - 事务标识
  - 被更新的数据块（更新前后的整个块分别存入日志文件，日志记录不需要更多其他信息）

2.日志文件的作用

- 用途
  - 进行事务故障恢复
  - 进行系统故障恢复
  - 协助后备副本进行介质故障恢复

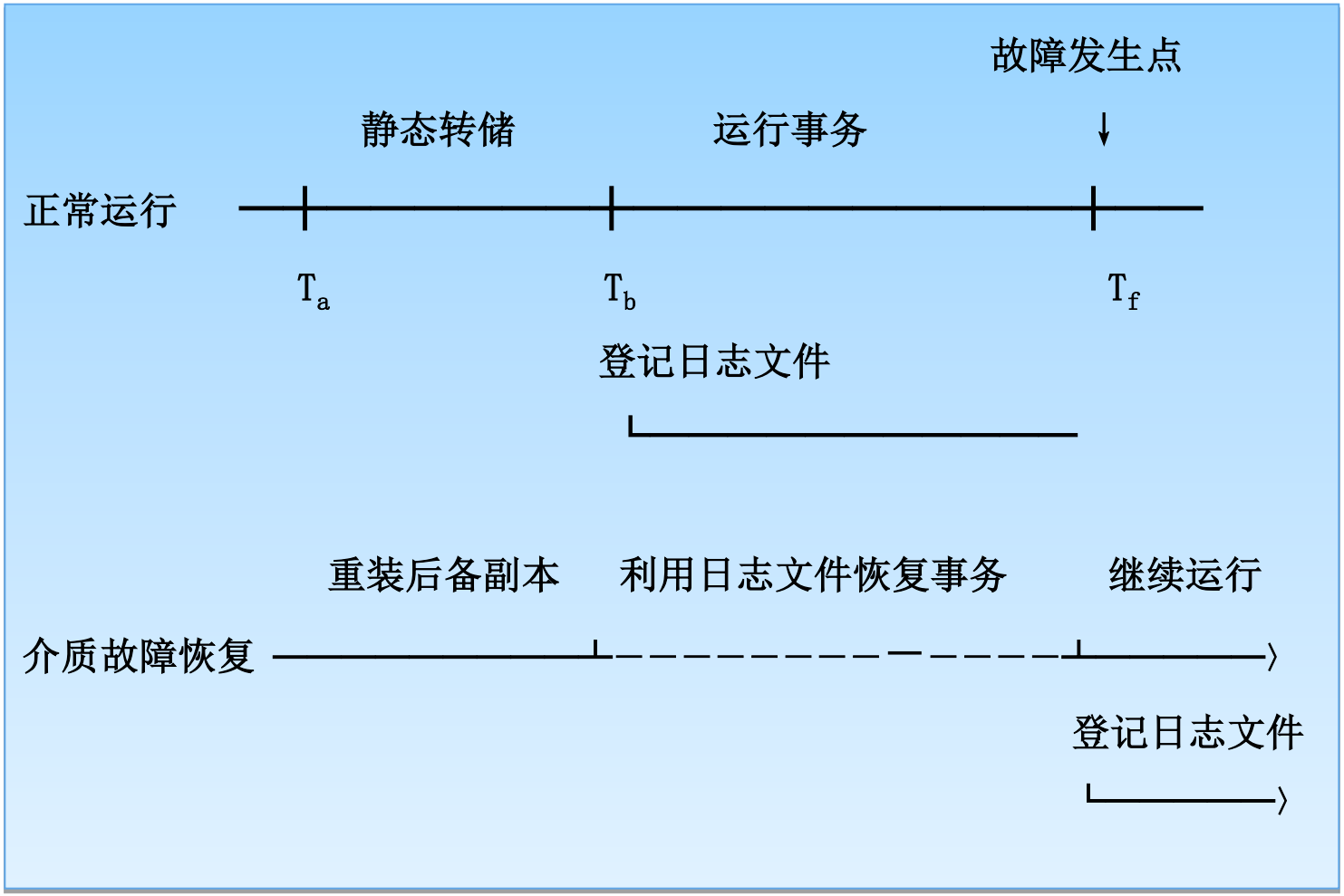
日志文件的作用（续）

- 具体作用
  - 事务故障恢复和系统故障恢复必须用日志文件。
  - 在动态转储方式中必须建立日志文件，后备副本和日志文件结合起来才能有效地恢复数据库。

日志文件的作用（续）

- 在静态转储方式中，也可以建立日志文件。
  - 当数据库毁坏后可重新装入后援副本把数据库恢复到转储结束时刻的正确状态
  - 利用日志文件，把已完成的事务进行重做处理
  - 对故障发生时尚未完成的事务进行撤销处理

日志文件的作用（续）



利用日志文件恢复

3.登记日志文件

- 为保证数据库是可恢复的，登记日志文件时必须遵循两条原则
  - 登记的次序严格按并发事务执行的时间次序
  - 必须先写日志文件，后写数据库
    - 所有的修改在提交之前都要先写入日志文件，称为预写式日志**WAL: Write-Ahead Logging**
    - 写日志文件操作：把表示这个修改的日志记录写到日志文件中
    - 写数据库操作：把对数据的修改写到数据库中

3.登记日志文件

- 先写日志文件: 包括 **redo** 和 **undo** 信息。
  - 假设一个程序在执行某些操作的过程中机器掉电。在重新启动时，程序可能需要知道当时执行的操作是成功，还是部分成功，或者是失败。
  - 如果使用 **WAL**，程序可以检查日志文件，对突然掉电时，计划执行的操作内容跟实际上执行的操作内容进行比较。
  - 程序就可以决定是撤销已做的操作还是继续完成已做的操作，或者是保持原样。

登记日志文件（续）

- 为什么要先写日志文件
  - 写数据库和写日志文件是两个不同的操作，在这两个操作之间可能发生故障
  - 如果先写了数据库修改，而在日志文件中没有登记下这个修改，则以后就无法恢复这个修改了
  - 如果先写日志，但没有修改数据库，系统崩溃后，按日志文件恢复可能多执行一次不必要的**UNDO**操作，并不会影响数据库的正确性

登记日志文件（续）

- 为什么要先写日志文件
  - 保证持久性。当发生意外崩溃时，在恢复过程中那些不该写入却已经写入到磁盘的数据会被回滚，而那些应该写入磁盘却没有写入的数据会被重做。
  - 提高性能。每次提交的修改数据的事务并不会马上反映到数据库中，而是先记录到日志，在随后一并提交，否则需要每次提交数据时写入数据库。

登记日志文件（续）

- 为什么要先写日志文件-类比实际情况
  - 给定仓库，仓库有管理员，登记每次取货情况。
  - 如果先取货，后登记。中间出现紧急情况，可能忘记登记，货账不一致，无法知道谁取了什么货。
  - 必须先登记，再取货。如果登记之后，发生紧急情况，没取货，紧急情况处理完毕，检查登记记录，该取货的再去取货。

第十章 数据库恢复技术

10.1 事务的基本概念

10.2 数据库恢复概述

10.3 故障的种类

10.4 恢复的实现技术

10.5 恢复策略

10.6 具有检查点的恢复技术

10.7 数据库镜像

10.8 小结

10.5 恢复策略

10.5.1 事务故障的恢复

10.5.2 系统故障的恢复

10.5.3 介质故障的恢复

10.5.1 事务故障的恢复

- 事务故障：事务在运行至正常终止点前被终止
- 恢复方法
  - 由恢复子系统利用日志文件撤消（**UNDO**）此事务已对数据库进行的修改
- 事务故障的恢复由系统自动完成，对用户是透明的，不需要用户干预

事务故障的恢复步骤

（1） 反向扫描文件日志（即从最后向前扫描日志文件），查找该事务的更新操作。

（2） 对该事务的更新操作执行逆操作。即将日志记录中“更新前的值” 写入数据库。

- 插入操作，“更新前的值”为空，相当于做删除操作
- 删除操作，“更新后的值”为空，相当于做插入操作
- 若是修改操作，则相当于用修改前值代替修改后值

事务故障的恢复步骤（续）

（3） 继续反向扫描日志文件，查找该事务的其他更新操作，并做同样处理。

（4） 如此处理下去，直至读到此事务的开始标记，事务故障恢复就完成了。

10.5 恢复策略

10.5.1 事务故障的恢复

10.5.2 系统故障的恢复

10.5.3 介质故障的恢复

10.5.2 系统故障的恢复

- 系统故障造成数据库不一致状态的原因
  - 未完成事务对数据库的更新可能已写入数据库
  - 已提交事务对数据库的更新可能还留在缓冲区没来得及写入数据库
- 恢复方法

  1. Undo 故障发生时未完成的事务

  2. Redo 已完成的事务
- 系统故障的恢复由系统在重新启动时自动完成，不需要用户干预

系统故障的恢复步骤

（1）正向扫描日志文件（即从头扫描日志文件）

- 重做(REDO) 队列: 在故障发生前已经提交的事务
  - 这些事务既有BEGIN TRANSACTION记录，也有COMMIT记录
- 撤销 (UNDO)队列: 故障发生时尚未完成的事务
  - 这些事务只有BEGIN TRANSACTION记录，无相应的COMMIT记录

系统故障的恢复步骤（续）

（2） 对撤销(UNDO)队列事务进行撤销(UNDO)处理

- 反向扫描日志文件，对每个撤销事务的更新操作执行逆操作
- 即将日志记录中“更新前的值”写入数据库

（3）对重做(REDO)队列事务进行重做(REDO)处理

- 正向扫描日志文件，对每个重做事务重新执行登记的操作
- 即将日志记录中“更新后的值”写入数据库

10.5 恢复策略

10.5.1 事务故障的恢复

10.5.2 系统故障的恢复

10.5.3 介质故障的恢复

10.5.3 介质故障的恢复

1.重装数据库

2.重做已完成的事务

介质故障的恢复（续）

❖ 恢复步骤

（1） 装入最新的后备数据库副本(离故障发生时刻最近的转储副本)，使数据库恢复到最近一次转储时的一致性状态。

- 对于静态转储的数据库副本，装入后数据库即处于一致性状态
- 对于动态转储的数据库副本，还须同时装入转储时刻的日志文件副本，利用恢复系统故障的方法（即REDO+UNDO），才能将数据库恢复到一致性状态。

介质故障的恢复（续）

（2） 装入有关的日志文件副本(转储结束时刻的日志文件副本)，重做已完成的事务。

- 首先扫描日志文件，找出故障发生时已提交的事务的标识，将其记入重做队列。
- 然后正向扫描日志文件，对重做队列中的所有事务进行重做处理。即将日志记录中“更新后的值”写入数据库。

介质故障的恢复（续）

- 介质故障的恢复需要数据库管理员介入
- 数据库管理员的工作
  - 重装最近转储的数据库副本和有关的各日志文件副本
  - 执行系统提供的恢复命令
- 具体的恢复操作仍由数据库管理系统完成

第十章 数据库恢复技术

10.1 事务的基本概念

10.2 数据库恢复概述

10.3 故障的种类

10.4 恢复的实现技术

10.5 恢复策略

10.6 具有检查点的恢复技术

10.7 数据库镜像

10.8 小结

10.6 具有检查点的恢复技术

1.问题的提出

2.检查点技术

3.利用检查点的恢复策略

1.问题的提出

- 两个问题
  - 搜索整个日志将耗费大量的时间
  - 重做处理：重新执行，浪费了大量时间

注意：更新操作不能控制缓冲区管理器何时决定将块从主存拷贝到磁盘，其所反映的改变通常发生在主存中而不是磁盘上，即日志记录是对写入内存的更新动作做出的反映，而不是对写入磁盘动作的反映。

如果让数据库修改暂时只存在于主存，可以节省磁盘I/O。

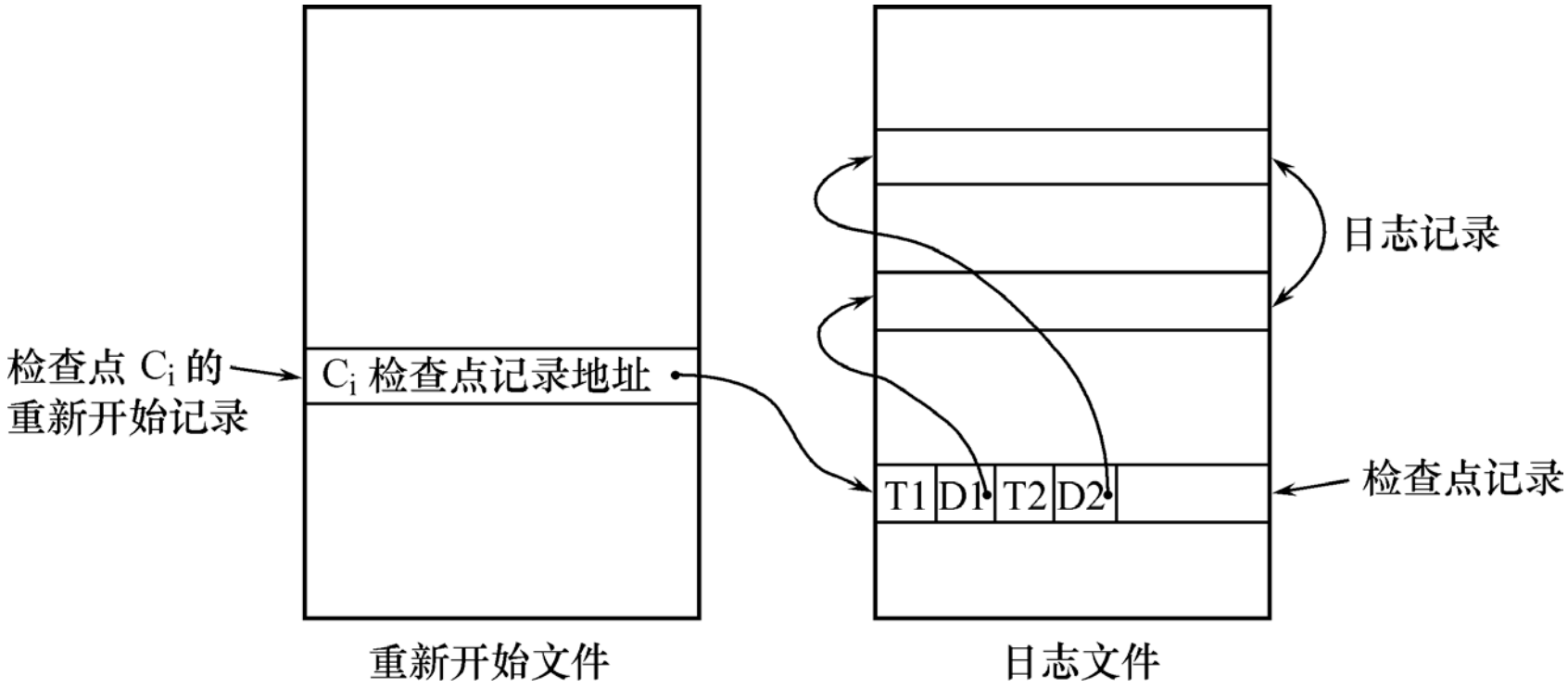
解决方案

- 具有检查点（checkpoint）的恢复技术
  - 存在的根本意义在于减少崩溃恢复时间
  - 通过检查点来确定，恢复时哪些重做日志应该被扫描并应用于恢复。
  - 通俗的说，检查点就像word的自动保存一样。
  - 基本原理就是每隔一段时间把缓冲区管理器的数据写入硬盘。

解决方案

- 具有检查点（checkpoint）的恢复技术
  - 在日志文件中增加检查点记录
  - 增加重新开始文件（存储各检查点记录的地址）
  - 恢复子系统在登录日志文件期间动态地维护日志

检查点技术（续）



具有检查点的日志文件和重新开始文件

2. 检查点技术

- 检查点记录的内容
  - 建立检查点时刻所有正在执行的事务清单
  - 这些事务最近一个日志记录的地址（指针指向该事务对应的日志记录的磁盘地址）
- 重新开始文件的内容
  - 记录各个检查点记录在日志文件中的地址

动态维护日志文件的方法

❖ 动态维护日志文件的方法

周期性地执行如下操作：建立检查点，保存数据库状态。

（1）将当前日志缓冲区中的所有日志记录写入磁盘的日志文件上

（2）在日志文件中写入一个检查点记录

（3）将当前数据缓冲区的所有数据记录写入磁盘的数据库中

（4）把检查点记录在日志文件中的地址写入一个重新开始文件

建立检查点

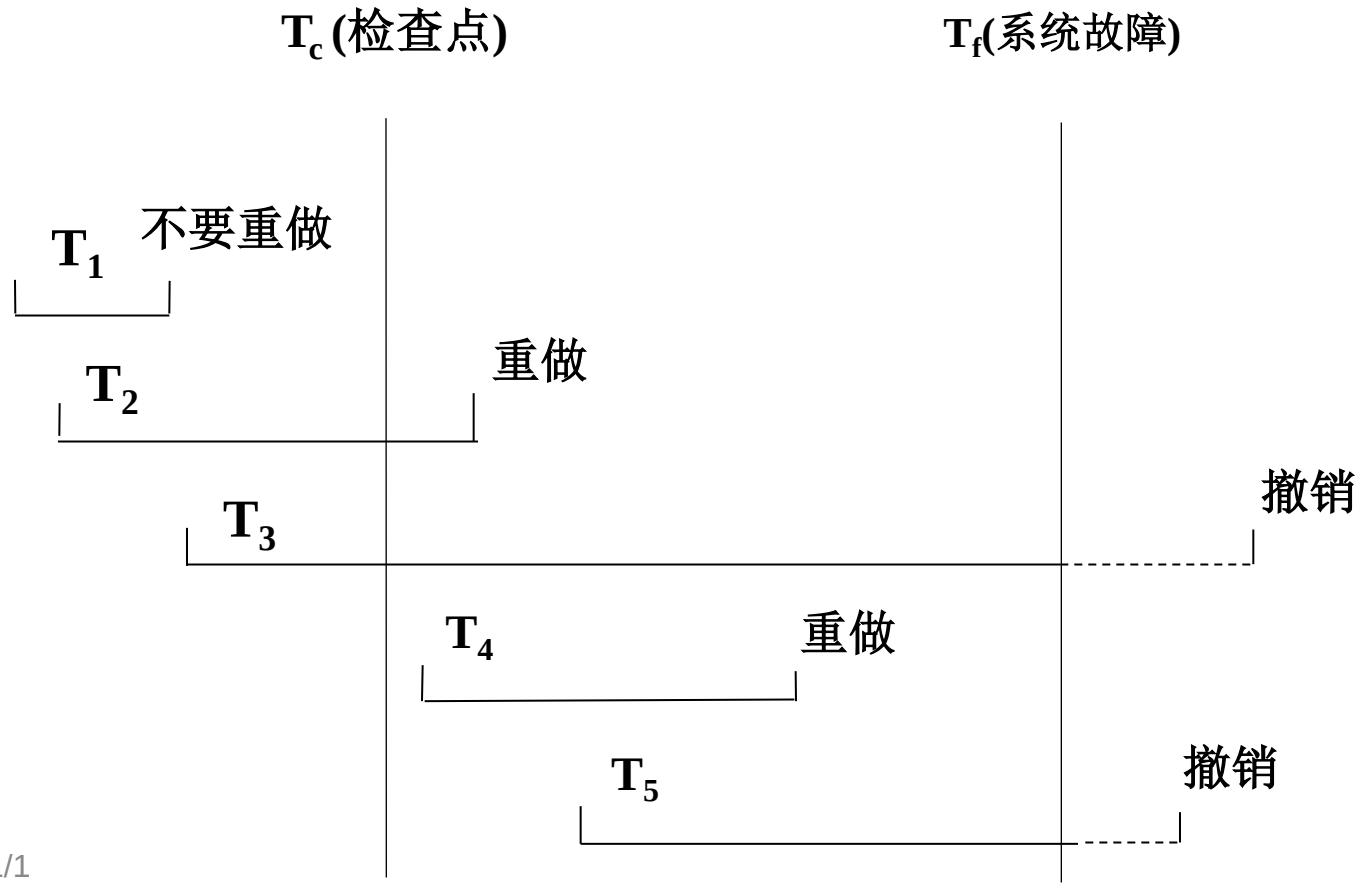
- 恢复子系统可以定期或不定期地建立检查点，保存数据库状态
  - 定期: 按照预定的一个时间间隔，如每隔一小时建立一个检查点
  - 不定期: 按照某种规则，如日志文件已写满一半建立一个检查点

3.利用检查点的恢复策略

- 使用检查点方法可以改善恢复效率
  - 当事务T在一个检查点之前提交，T对数据库所做的修改已写入数据库
  - 写入时间是在这个检查点建立之前或在这个检查点建立之时
  - 在进行恢复处理时，没有必要对事务T执行重做操作

利用检查点的恢复策略（续）

系统出现故障时，恢复子系统将根据事务的不同状态采取不同的恢复策略



利用检查点的恢复策略（续）

- **T1**：在检查点之前提交
- **T2**：在检查点之前开始执行，在检查点之后故障点之前提交
- **T3**：在检查点之前开始执行，在故障点时还未完成
- **T4**：在检查点之后开始执行，在故障点之前提交
- **T5**：在检查点之后开始执行，在故障点时还未完成

利用检查点的恢复策略（续）

恢复策略

- T3和T5在故障发生时还未完成，所以予以撤销
- T2和T4在检查点之后才提交，它们对数据库所做的修改在故障发生时可能还在缓冲区中，尚未写入数据库，所以要重做
- T1在检查点之前已提交，所以不必执行重做操作

利用检查点的恢复步骤

（1）从重新开始文件中找到最后一个检查点记录在日志文件中的地址，由该地址在日志文件中找到最后一个检查点记录

利用检查点的恢复策略（续）

（2）由该检查点记录得到检查点建立时刻所有正在执行的事务清单**ACTIVE-LIST**

- 建立两个事务队列
  - ✓ **UNDO-LIST**
  - ✓ **REDO-LIST**
- 把**ACTIVE-LIST**暂时放入**UNDO-LIST**队列，**REDO**队列暂为空。

利用检查点的恢复策略（续）

（3）从检查点开始正向扫描日志文件，直到日志文件结束

- ✓ 如有新开始的事务T_i，把T_i暂时放入UNDO-LIST队列
- ✓ 如有提交的事务T_j，把T_j从UNDO-LIST队列移到REDO-LIST队列;直到日志文件结束

（4）对UNDO-LIST中的每个事务执行UNDO操作，对REDO-LIST中的每个事务执行REDO操作

第十章 数据库恢复技术

10.1 事务的基本概念

10.2 数据库恢复概述

10.3 故障的种类

10.4 恢复的实现技术

10.5 恢复策略

10.6 具有检查点的恢复技术

10.7 数据库镜像

10.8 小结

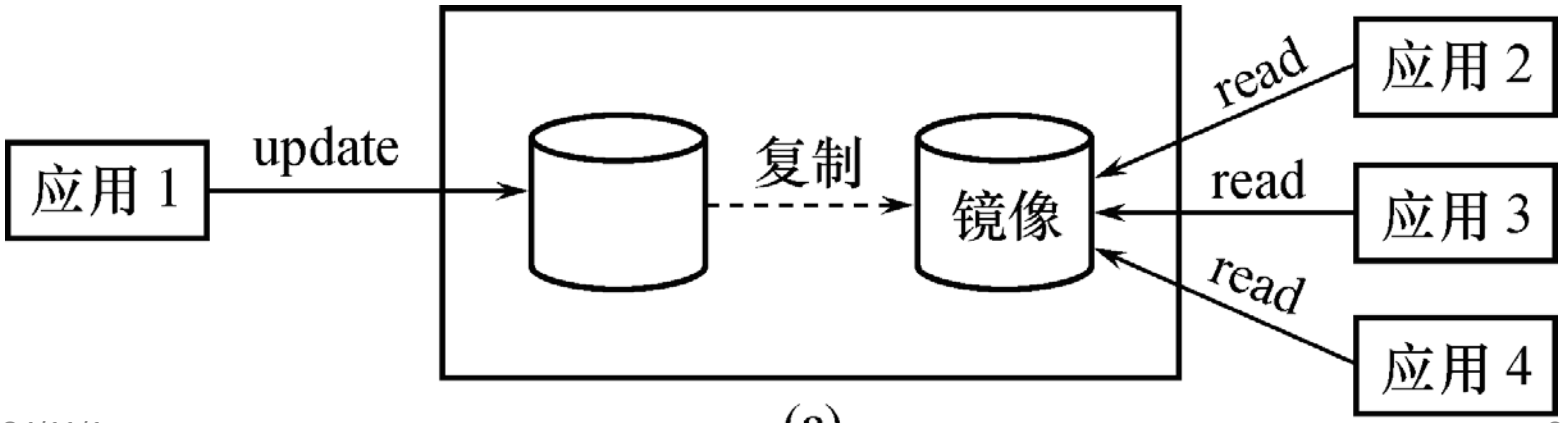
10.7 数据库镜像

- 介质故障是对系统影响最为严重的一种故障，严重影响数据库的可用性
  - 介质故障恢复比较费时
  - 为预防介质故障，数据库管理员必须周期性地转储数据库
- 提高数据库可用性的解决方案
  - 数据库镜像（Mirror）

数据库镜像（续）

❖数据库镜像

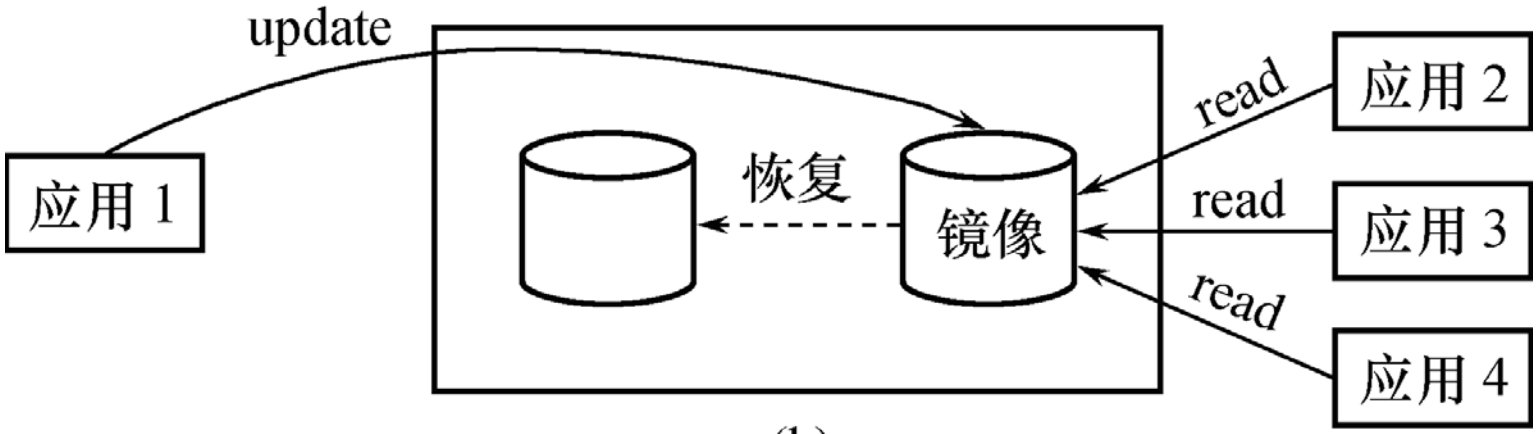
- 数据库管理系统自动把整个数据库或其中的关键数据复制到另一个磁盘上
- 数据库管理系统自动保证镜像数据与主数据库的一致性，每当主数据库更新时，数据库管理系统自动把更新后的数据复制过去



(a)

数据库镜像的用途

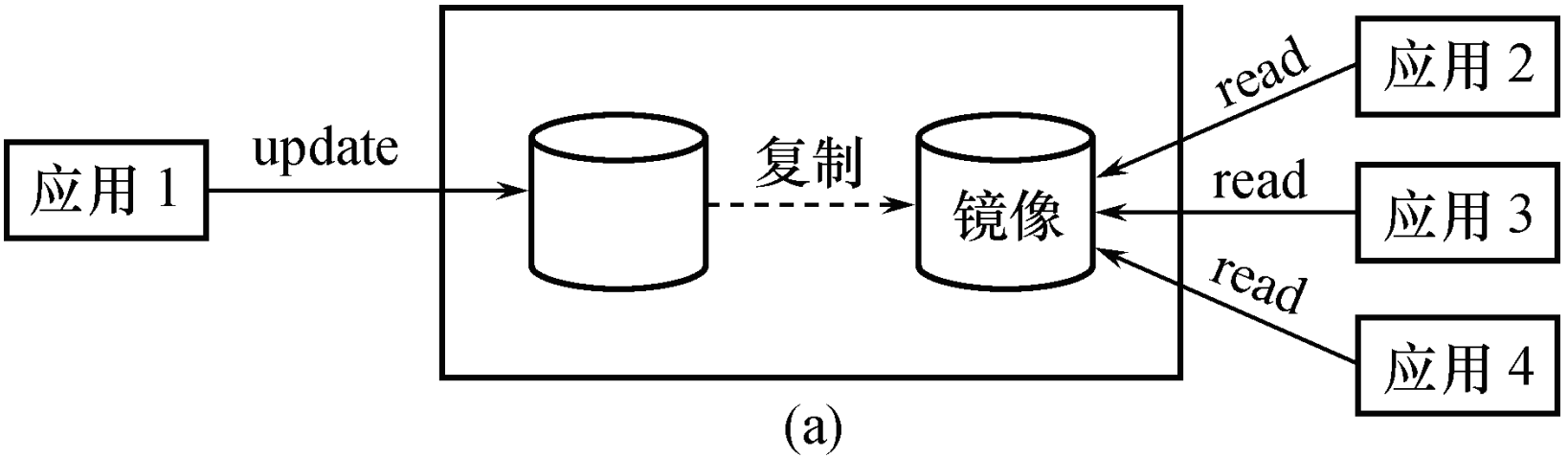
- 出现介质故障时
  - 可由镜像磁盘继续提供使用
  - 同时数据库管理系统自动利用镜像磁盘数据进行数据库的恢复
  - 不需要关闭系统和重装数据库副本



(b)

数据库镜像（续）

- 没有出现故障时
  - 可用于并发操作
  - 一个用户对数据加排他锁修改数据，其他用户可以读镜像数据库上的数据，而不必等待该用户释放锁



(a)

数据库镜像（续）

- 频繁地复制数据自然会降低系统运行效率
  - 在实际应用中用户往往只选择对关键数据和日志文件镜像
  - 不是对整个数据库进行镜像

第十章 数据库恢复技术

10.1 事务的基本概念

10.2 数据库恢复概述

10.3 故障的种类

10.4 恢复的实现技术

10.5 恢复策略

10.6 具有检查点的恢复技术

10.7 数据库镜像

10.8 小结

10.8 小结

- 事务的概念和性质
  - 事务是数据库的逻辑工作单位
  - 数据库管理系统保证系统中一切事务的原子性、一致性、隔离性和持续性，就保证了事务处于一致状态

小结（续）

- 故障的种类
  - 事务故障
  - 系统故障
  - 介质故障
- 恢复中最经常使用的技术
  - 数据库转储
  - 登记日志文件

小结（续）

- 恢复的基本原理
  - 利用存储在后备副本、日志文件和数据库镜像中的冗余数据来重建数据库
- 事务
  - 不仅是恢复的基本单位
  - 也是并发控制的基本单位