

8.2 故障的种类

(1) 系统故障

◆ 又称为**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**。软故障包括：

- 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

8.2 故障的种类

◆系统故障的影响

- 所有正在运行的事务都非正常终止，活跃事务没全部完成
- 内存中数据库**缓冲区的信息全部丢失**，更新丢失了
- 造成数据库可能**处于不正确的状态**，但不会破坏数据库

◆恢复系统故障的措施

- 撤销（UNDO）所有未完成的事务
- 重做（REDO）所有已提交的事务



8.2 故障的种类

(2) 介质故障

◆ **硬故障**，指外存故障。硬故障包括：

- 磁盘损坏
- 磁头碰撞
- 顺势强磁场干扰

◆ 介质故障**会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。

◆ 介质故障比系统故障的**可能性小得多**，但**破坏性大得多**。

8.3 恢复的实现技术

◆恢复技术的基本原理：冗余

利用存储在系统别处的冗余数据额，来重建数据库中已被破坏或不正确的那部分数据。

◆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)

这两种技术通常一起使用。

(2) 如何利用这些冗余数据实施数据库恢复

8.3.1 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**。
- ◆ 数据库遭到破坏后，可以将**最近一次转储**的后备副本重新装入。
- ◆ 重装后备副本只能将数据库**恢复到最近一次转储时的状态**。
- ◆ 要想恢复到故障发生时的状态，必须**重新运行**自**最近一次转储**以后的所有**更新**事务。

8.3.2 登记日志文件

◆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

是以日志记录为单位，包括两类记录：

- 事务记录.
- 检查点记录

◆日志文件的作用

- 用于系统故障的恢复
- 与后备副本同时使用，用于介质故障的恢复

使用转储和日志文件恢复数据库

- ◆ 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**结合日志文件**中的记录，才能有效地恢复数据库。
- ◆ **步骤**如下：
 - (1) 故障恢复时，重新装入后援副本，把数据库恢复到转储时刻的正确状态。
 - (2) 利用日志文件，重做（redo）已完成事务，撤销（undo）未完成的事务，才能将数据库恢复到故障前的一致性状态。

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，此时发生了故障。则在日志文件中就没有记录下这个修改，则以后就无法恢复此修改；
- ◆ 如果先写日志，但没有修改数据库，则在按日志文件恢复时，只不过是多执行一次不必要的**UNDO操作**（**用旧值覆盖目前值，并非重做一次操作**），并不会影响数据库的正确性。

8.4 具有检查点的恢复技术

◆ 为什么引入检查点机制？

- 可以使用日志文件中的信息将数据库**从故障状态恢复到正确状态**。
- 这种机制的**问题**：当故障发生时，需要搜索整个日志文件，找到需要重做的事务，即不知从日志文件的哪里开始重做。
- 为了限制**搜索**日志文件的**范围**，使用一种称为“检查点”的技术

◆ 检查点的定义

是**数据库与事务日志文件**间的同步点，在该点上所有的缓冲块都被**强制写入**辅助存储器（磁盘）中。

检查点技术

◆措施

- 在日志文件中增加**检查点记录**（checkpoint）
- 增加**重新开始文件**
- 恢复子系统在登录日志文件期间**动态地维护日志**。

◆检查点记录的内容包括：

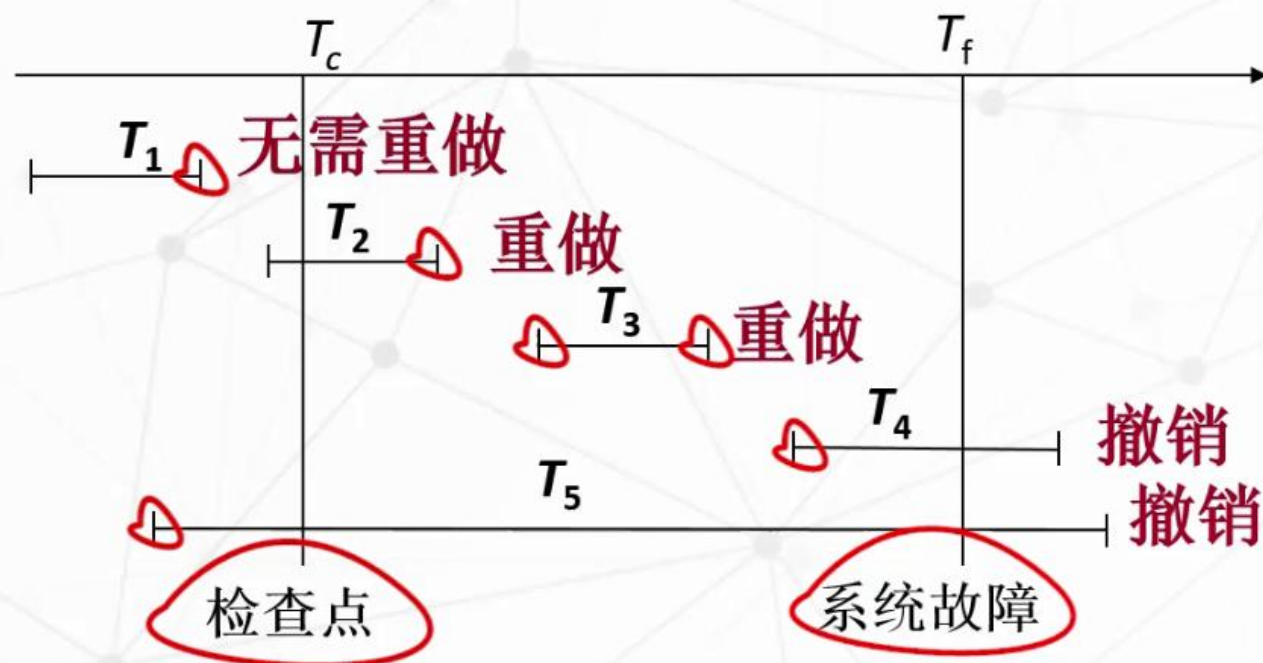
- （1）建立检查点时刻，所有**正在执行的事务清单**
- （2）这些事务**最近**一个日志**记录的地址**。

◆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**，这样就不必重头搜索日志文件了。



利用检查点恢复的示例



- 不必对**T1** 做任何操作，因为在检查点之前，T1已结束，所有更新已保存到硬盘中。
- 重做 (redo) **T2** 和 **T3**。
- 撤销 (undo) **T4** 和 **T5**