



# 数据恢复技术

经典重现版

戴士剑 涂彦晖 编著

张喜平 审校



数据恢复与电子证据调查必备基础  
最好的“恢复”永远是备份、备份、再备份

## 内 容 简 介

数据恢复技术是一门新兴技术，它通过各种手段把丢失和遭到破坏的数据还原为正常数据。本书通过多种典型实例详细介绍了 Windows 系统下数据恢复技术的原理和方法，内容包括硬盘数据组织、文件系统原理、数据恢复技术、文档修复技术、密码遗失处理技术、数据安全技术 and 数据备份技术。

本书作者戴士剑是知名数据恢复专家，有多年的数据恢复工作经验。本书是作者工作经验和技术理论的总结，适合 IT 系统客户服务人员、技术支持工程师、技术培训人员、数据恢复技术工程师、信息安全工作人员、系统管理人员、安全保密部门人员、计算机取证人员、操作系统开发人员、存储技术相关人员、学生，以及任何对相关技术和工作感兴趣的读者，作为学习材料、参考资料或培训教材使用。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。  
版权所有，侵权必究。

### 图书在版编目 (CIP) 数据

数据恢复技术：经典重现版 / 戴士剑，涂彦晖编著. —北京：电子工业出版社，2014.7  
(安全技术大系)

ISBN 978-7-121-23537-5

I. ①数… II. ①戴… ②涂… III. ①电子计算机—数据管理—安全技术 IV. ①TP309.3

中国版本图书馆 CIP 数据核字 (2014) 第 127695 号

责任编辑：徐津平

印 刷：北京中新伟业印刷有限公司

装 订：北京中新伟业印刷有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱

邮编 100036

开 本：787×1092 1/16 印张：43

字数：1040 千字

版 次：2003 年 5 月第 1 版

2014 年 7 月第 3 版

印 次：2014 年 7 月第 1 次印刷

印 数：4000 册

定 价：99.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010) 88254888。

质量投诉请发邮件至 zlt@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010) 88258888。

# 第 1 章 综述

本章主要讲述数据存储技术方面的基础知识和数据恢复技术的基本概念、内涵和类别，从而使读者在总体上对数据恢复知识有一个全面的了解。

## 1.1 数据存储技术总论

---

信息时代的核心无疑是信息技术，而信息技术的核心则在于信息的处理与存储。随着数据量的剧增，数据存储技术已经面临着巨大的挑战。当我们每天关注 CPU 主频的不断提高、操作系统版本的不断升级和计算机网络技术的日新月异的时候，或许不应该忽略这样的事实——无论信息处理技术多么先进，我们都必须将信息存储于一定的介质之上，信息和信息技术本身都需要依托一定的存储介质而存在。

近年来，计算机在商业和个人方面的应用得到了显著的增长，现在几乎每一间办公室都拥有计算机，许多家庭都已经拥有计算机，大多数的公司都建立了计算机网络来共享应用程序和数据。所有这些变化使数据字节取代了纸张，提高了生产力和生产效率，减小了冗余，并增强了信息的可用性。

由于越来越多的信息变成了电子信息，这就使信息存储技术显得更加重要，特别是计算机网络应用的迅速增长，更大大增加了对信息存储产品的需求量和对信息存储技术的安全性、可靠性的要求。根据 3M 公司对 800 名网络计算机用户的调查发现，每次硬盘的失效将造成 5 个以上的无效工作日。而在一个典型的商业应用中，重建 1 000MB 数据平均要耗时 3.5 个月，费用为 95 000 美元。由此可见，信息存储的安全对最终用户来说是何等的重要。

### 1.1.1 数据存储介质

凡是仅有两种稳定的物理状态，能方便地检测出属于哪种稳定状态，两种稳定状态又容易相互转换的物质或元器件，都可以用来存储二进制代码“0”和“1”，这样的物质或元器件称为存储介质或记录介质。存储介质不同，存储信息的机理也不同。

信息存储技术在近几年的发展非常迅速，各种新产品、新技术层出不穷，但从总体上看，呈现出一种类似金字塔的结构，其中塔尖为 CPU，距离 CPU 越近则存储速度越快，每兆字节的存储成本越昂贵，容量也越小；反之，存储速度越慢，每兆字节的存储成本越低，容量也越大。

计算机的存储设备从体系结构上看可分为内存储器 and 外存储器。

内存储器（即内存）直接与计算机的 CPU 相连，处于金字塔的最上层。内存的存取速度要

能与 CPU 相匹配，通常由半导体存储器芯片组成，由于成本高，容量通常不太大。

对于大量数据的保存，通常要使用外存储器。外存储器又可以分成几个层次。与内存存储器相连接的是联机存储器（或称在线存储器），如硬盘机、磁盘阵列等。再下一层是后援存储器（或称近线存储器），由存取速度比硬盘更慢的光盘机、光盘库、磁带库等设备组成。最底层是脱机存储器（或称离线存储器），由磁带机和磁带库等组成仓库，存取速度比较慢，仅是秒数量级，由于存储介质可脱机保存，也可以更换，因此容量几乎是无限大。

计算机存储设备的层次关系如图 1-1 所示。



图 1-1 存储金字塔结构

对于普通的个人计算机用户，使用硬盘、软盘和光盘等存储介质来进行数据存储就已经够用了，但对于商业用户和一些网络系统来说，磁带机、磁带库和光盘库则是必不可少的数据存储与备份设备。还有正在飞速发展的存储网络，能提供更为方便的数据保存方式。下面我们通过不同的存储介质来看一看当今市场上流行的主机信息存储技术，按其存储原理可以分为：电存储技术，如内存、闪存等；磁存储技术，如磁带、磁盘等；光存储技术，如 CD-ROM、DVD-ROM 等。

### 1. 电存储技术

电存储技术主要是指半导体存储器（Semiconductor Memory, SCM）。早期的 SCM 采用典型的晶体管触发器作为存储位元，加上选择、读、写等电路构成存储器。现代的 SCM 采用超大规模集成电路工艺制成存储芯片，每个芯片中包含相当数量的存储位元，再由若干芯片构成存储器。

从集成电路类型的角度看，SCM 分为晶体管双极（Bipolar）型和场效应管（Metal Oxide Semiconductor, MOS）型。双极型分射极耦合逻辑（Emitter Couple Logic, ECL）、晶体管-晶体管逻辑（Transistor - Transistor Logic, TTL）和集成注入逻辑（Integrated Injection Logic, I<sup>2</sup>L）共 3 种类型。从制造工艺看，MOS 型有 PMOS（P channel MOS）、NMOS（N channel MOS）和 CMOS（Complementary MOS）3 类，目前广泛采用的是 NMOS 和 CMOS。从加电后能否长时间保持所存信息的角度看，SCM 又有静态存储器和动态存储器之分。静态存储器的存储位元电路是双稳态触发器，动态存储器存储位元电路的关键部件是电容。前者只要电源正常供电，

信息就能长期保存；后者即使电源正常供电，信息也只能保持几毫秒到十几毫秒，因此必须在规定时间内刷新。若电源电压不正常或断电，两者信息都会丢失。

双极型存储器都是静态存储器，而 MOS 型存储器有静态、动态之分。双极型存储器速度快，通常比 MOS 存储器至少高一个数量级，但功耗大、集成度低，适用于快速小容量存储器，如高速暂存存储器和 Cache。NMOS 静态存储器制造工艺简单、集成度高、单片容量大，主要用做快速主存。CMOS 静态存储器功耗最小，速度比 NMOS 快，集成度比双极型高很多，可靠性高，虽然制造工艺复杂，但目前应用得很广泛，主要用做快速主存和 Cache。动态 MOS 存储器内部结构最简单，在各类 SCM 中集成度最高，功耗很小，速度虽比静态 MOS 和双极型存储器低一些，但仍广泛用做主存。

综上所述，根据工作方式的不同，SCM 的分类如下。

读写存储器，或称随机存取存储器，按信息存储方式不同可分为以下两类。

- 静态 RAM (SRAM)。
- 动态 RAM (DRAM)：利用电容存储电荷的原理来记忆信息。由于电容器的漏电，存储的电荷会逐渐减少，当减少到一定程度时，RAM 中存入的信息会消失。因此，需要在信息丢失之前给电容器充电。给电容器充电的过程就叫做动态存储器的刷新。只读存储器包含以下几类。
  - 掩模式 ROM (MROM, MaskROM)：厂商写好内容后不能更改。
  - 可编程 ROM (PROM, Programmable ROM)：用户只能写入一次，写入后不能再更改。
  - 可擦除 PROM (EPROM, Erasable PROM)：通常在工作时只能读取信息，但可以用紫外线擦除已有信息，并在专用设备上高电压写入信息。
  - 电擦除 PROM (E2PROM, Electrically Erasable PROM)：用户可以通过程序的控制进行读写操作，它就是常说的闪存 (Flash Memory)。

## 2. 磁存储技术

磁存储主要是指磁表面存储器 (Magnetic Surface Memory, MSM)。磁表面存储器是用非磁性金属或塑料做基体，在其表面涂敷、电镀、沉积或溅射一层很薄的高导磁率、硬矩磁材料的磁面，用磁层的两种剩磁状态记录信息“0”和“1”。基体和磁层合称磁记录介质。依记录介质的形状可分别称为磁卡存储器、磁带存储器、磁鼓存储器和磁盘存储器。计算机中目前广泛使用的 MSM 是磁盘存储器和磁带存储器。

MSM 通过磁记录介质的高速旋转或平移，借助软磁材料制作的磁头实现读写，由于是机械运动方式，所以存取速度远低于 SCM，为毫秒级。MSM 的存储位元是磁层上非常小的磁化区域，可以小至  $20\mu\text{m}^2$ ，所以存储容量可以很大，与 SCM 相比，每位价格低得多，因此广泛用做辅存。IBM 已开发出垂直磁记录技术，可将磁记录密度提高到目前的 6 倍以上。

磁盘是广大用户最为熟悉的存储介质。在目前所有的 PC 中硬盘都是必不可少的设备，而软盘则由于其便于携带的特点和通用性，曾经是计算机用户进行数据交换时广泛使用的存储介质。

磁盘技术包括磁性盘片、电机、盘上方的伸缩臂和伸缩臂 (手柄) 上的磁头。电机带动磁盘旋转，伸缩臂在盘上移动，磁头进行读盘或写盘操作。读盘时，磁头检测盘表面磁性的变化，将其转化为 0 或 1 的数据组。写盘时，通过磁头改变盘上数据的磁性，如正、负极分别与 0、1 相对应。

在外存储器中，硬盘的存取速度最快，因此它最适合存储那些需要经常访问和快速访问的程序和文件。对于个人用户来说，硬盘是最主要的存储设备，计算机的操作系统、应用程序和重要的数据资料都存储在硬盘之中，因此要求硬盘的容量越大越好，速度越快越好。对于专业用户来说，由于数据丢失将会给他们带来非常大的损失，所以他们除了要求更高的速度、更大的容量之外，对硬盘的容错能力和安全性也有很高的要求。

市场的需求就是未来技术的发展方向，硬盘技术的发展方向正是向着大容量、高速度和高可靠性的方向发展。

早期的硬盘仅有几十 MB，而且价格昂贵。在十几年前，一台家用 PC 的标准配置还是 420MB 或 1GB 的硬盘。现在，1TB、2TB 的硬盘都已经进入寻常百姓家。能够产生如此大的飞跃主要得益于盘面存储密度的不断提高，现在 90mm (3.5 英寸) 的商品盘单片容量已达 20GB 或更高，130mm (5.25 英寸) 的单片容量达到 40GB 或更高。

在硬盘的速度（即数据传输率）方面，由于市场上的硬盘都带有高速缓存，从盘面读出的数据先送到缓存中，再从缓存送到主机内存中，所以目前主要由这两个环节来决定硬盘的速度。从盘面到缓存的内部传输率等于位存储密度乘以盘面的线速度，因此在存储密度一定的情况下，提高硬盘转速可以进一步提高内部传输率。现在主流硬盘的转速已达到 7 200r/min，较高的已经达到 10 000r/min 以上。由于硬盘是一种机电设备，它的转速受到机械结构的制约，因此，除非有大的技术变革，否则硬盘转速的提高将会越来越困难。从缓存到主机内存的外部传输率则与硬盘所采用的外部接口标准有关。硬盘接口早期为 IDE (Integrated Disk Electronics) 标准，它的最大支持容量只有 528MB，传输速度慢且传输线易受干扰。此后，随着信息技术的发展，IDE 接口逐渐无法满足市场的要求，Enhanced IDE (即 EIDE) 接口的硬盘就取代 IDE 硬盘成为当前市场的主流产品。这种接口支持大于 528MB 的硬盘容量，并允许一套系统串接 4 台存储设备（不只是硬盘），数据传输速率达到 16.6MB/s。1996 年 10 月，Quantum 和 Intel 又共同提出了 Ultra-IDE 接口标准，将数据传输速率提高到 33.3MB/s，并增加了 CRC 数据传输校验功能。其他的硬盘接口新技术如 Fast SCSI 标准的传输速率可达到 80MB/s。随着技术的进步，更多更新的接口技术不断涌现，其速率也发展到 66MB/s、100MB/s、133MB/s，光纤通道 (FCAL) 则将传输速率提高到 200MB/s。

为提高硬盘在工作时的可靠性，业界推出 S.M.A.R.T 技术 (Self-Monitoring Analysis & Reporting Technology)，即自动监视分析及报告技术。它通过监视和分析硬盘工作时的状态和性能并显示出来，使用户可以随时了解硬盘的工作情况。当硬盘发生失效时，用户可以及时获得警告，从而采取适当的措施保证硬盘中的数据不受损失。对于大型的存储系统（如磁盘阵列），另一种提高可靠性的方法是进行及时的数据备份。其主要技术有：磁盘映射技术、磁盘双工技术、热备份、RAID (独立磁盘冗余阵列) 技术等。

谁也不能否认软磁盘曾经的辉煌，但由于其容量较小且容错性较差，放置较长时间后磁盘容易损坏，所以软盘一般不用作大量的数据备份，更多的是作为数据交换的介质。早期的软盘为 5.25 英寸，早已被淘汰。后来广泛使用的是 3.5 英寸的软盘，容量仅为 1.44MB。这种软盘的最大特点是便于携带，随便一个衣服口袋都可以放下，而且它的盘片是密封的，不会在携带中造成损伤。但是它的容量太小，不能满足需求，于是大容量的软磁盘便应运而生。最早推向市场的大容量软盘是 Imation 公司的 LS-120 和 Iomage 公司的 Zip，它们的容量都超过了 100MB。1997 年 10 月 SONY 公司也推出了大容量软盘产品 HiFD，其容量达到 200MB，规格依然采用

3.5 英寸，数据传输率为 3.6MB/s，并向下兼容。

大容量软磁盘作为脱机存储设备在存储金字塔中处于近底层的位置。软磁盘是许多个人计算机用户的备份介质，但实际上把软磁盘当作数据交换介质和输入/输出介质可能更适合。

当前大容量软磁盘在市面上见到的有两种：一种是其前身是 3M 公司的怡敏信 (Imation) 公司的产品 LS-120，另一种是 Iomage 公司的 Zip。1996 年 MITSUMI 公司发表了 UHC 大容量软磁盘，但没有推向市场，这 3 种盘的性能见表 1-1。

表 1-1 大容量软磁盘比较

项 目	Zip	LS-120	UHC
格式化容量 (MB)	100	120	128
盘片直径 (mm)	90	86	86
转速 (r/min)	2 945	720	3 600
最大数据传输率 (MB/s)	1.4	0.663	2.45
平均寻道时间 (ms)	29	65	20
向下兼容性*	无	有	有
接口	SCSI、并行口	IDE、SCSI、并行口	IDE、SCSI

\* 指能够读写 90mm (3.5 英寸) 1.44MB 的盘片。

磁带存储可以说是最古老的存储方式之一。从 1952 年第一台 13mm (0.5 英寸) 磁带机在 IBM 公司问世以来，它已经走过了 60 多年的历史，积累了大量的使用经验和可靠性数据。磁带存储是一种安全、可靠、易用、效费高的数据备份方法。因为磁带可以从驱动器上取出，因此可以实现非现场方式的保存或存放过去版本的数据。磁带存储系统大都易于操作，甚至可以实现无人值守的数据备份和磁带管理。磁带的速度虽然比硬盘和光盘要慢，但它也能在相对短的时间内 (如一个晚上) 备份需要的数据。由于磁带的可靠性很高 (实践证明，一盘磁带上的数据可以保存 30 年以上)，而且容量大 (以目前的存储技术，一盘磁带存储容量可达 200GB，磁带库则可扩展到几十 TB 的水平)，所以它是当之无愧的大容量数据备份的首选存储介质。

磁带品种较多，在选择时要考虑以下多方面的因素。

- 磁带的密度和容量：磁带有 0.5 英寸、8mm、4mm、0.25 英寸等规格，每盒容量从几十 MB 到几 GB，应选择适合自己系统的磁带。容量是指压缩过的容量，通常用压缩比 2 : 1 折算。但如果要存储的文件是已压缩过的，则不可能再压缩，就需要选择容量大一些的。
- 数据传输率：如果备份数据量大，就需选择数据传输率大一些的，以减少备份所需要的时间。
- 磁带寿命：包括两个指标，一是通过磁头的次数，由于磁带和磁头在读写时有摩擦，造成磁带磨损，一般螺旋扫描式磨损较严重。二是保存寿命，可保存多少年，这与磁带材料和保存环境有关。
- 向下兼容：磁带技术不断更新，要求新的机器能读出旧的保存的磁带。如果没有这个功能，就需要花费人工和时间来进行磁带转换。
- 记录技术：现在磁带记录技术主要有两类：螺旋扫描记录和直线记录。8mm 磁带和 4mm 磁带采用螺旋扫描记录技术，记录的轨迹与磁带运动方向有一夹角。这样有利于提高存储密度，但磁带与磁头间有夹角，磨损较严重，磁带机结构复杂，耐用性也差。DAT 磁带、IBM3480 系列、DLT 磁带都采用直线记录方式，磁带机结构简单，磁带的磨损小，寿命长。

- 边写边读功能：即在写入的同时读出数据进行核对，以确保数据的可靠性，如有差错可立即修改。IBM3480/3490、DLT、SLR、MLR 磁带机都有这一功能，但有此功能价格就高了许多，通常采用的是先写后读功能，一盒磁带写完后，要倒带再从头读出检查有无错误。这样做要多花许多时间，还增加了磁头和磁带的磨损。
- 接口：如 IDE 接口、并行接口、SCSI 接口、软驱接口等。要选择与机器一致的接口。下面介绍常见的几种磁带规格。

#### (1) QIC 磁带

QIC 磁带采用的带宽是 6.25mm (0.25 英寸)，有带盒，采用直线记录方法。现在常见的是两种规格：DC6000 和 DC2000。

DC6000 采用的磁带机外形尺寸类似于 130mm (5.25 英寸) 软磁盘机。这种磁带单盒的容量较大。例如，Tandberg Data 公司的 MLR3，单盒容量可达 25GB (压缩后)，持续传输率为 2MB/s，采用 Fastwide SCSI-2 接口。DC6000 由于体积大，所以单独利用的不多，多组合成磁带库使用。

DC2000 采用的磁带机外形尺寸类似于 90mm (3.5 英寸) 软磁盘机，也称 Traven。DC2000 不具备数据压缩功能，也不具备即写即读功能，因此磁带机结构简单，成本低。再加上体积小、容量大，适合个人计算机和中小型服务器使用。Seagate 公司的 Tapestor 就是一种 Traven3 磁带机，压缩后每盒磁带容量为 3.2GB，写入速度为 19MB/min。

#### (2) 8mm 磁带

8mm 磁带采用螺旋扫描记录方式，1987 年由 Exabyte 公司提出，长期以来也只有 Exabyte 公司生产，单盒磁带最大容量 14GB (压缩后)。Exabyte 公司发布的 Mammoth 磁带机，单盒容量提高到 40GB (压缩后)，每小时可录入 21.6GB 数据。1997 年，SONY 公司也推出 8mm 磁带机，容量为 25GB，传输率为 3MB/s。但它与现有的 8mm 记录格式不兼容。

8mm 磁带机可组成磁带库。例如，Exabyte 公司的 210 磁带库，可安装 1~2 台磁带机，放置 11 盒磁带，总容量可达 154GB (压缩后)，连续传输率为 1MB/s (压缩后)。

#### (3) DOS 磁带

DOS 磁带采用的带宽是 3.81mm (0.15 英寸，有时也称之为 4mm 磁带)。它最早用于音乐存储，通称 DAT 磁带。1991 年建立统一标准，采用 HP 等公司提出的标准，称为 DOS 磁带。

DOS 磁带采用螺旋扫描记录方式，用数据压缩技术来提高存储量，多采用 SCSI 接口。DOS 磁带单盒最大容量可达 24GB (压缩后)。DOS 磁带机生产厂商有 HP、Seagate 等，其中以 HP 所占份额最大。DOS 磁带机生产厂商多，价格较低廉，容量和传输率都适合网络做备份用。但 DOS 磁带记录面积小 (带宽太小)，限制了容量和传输率的提高。

HP 的 SaveStore DAT24 就是采用 DOS-3 格式的磁带机，在一盒磁带上可存储 24GB 数据 (压缩后)，并有即写即读功能，每小时可存储 7.2GB 数据，持续传输率为 1MB/s (未压缩)。DOS 磁带也有磁带库，如 HP 的 Savestore DAT24×6e，可放置 6 盒 DOS-3 磁带，磁带装卸时间平均仅约 14s。

#### (4) DLT 磁带

DLT 磁带由 DEC 公司开发，主要生产厂商有 HP、Quantum。DLT 磁带宽度为 13mm (0.5 英寸)，有带盒 (带盒比一般录像带略短)，采用直线记录方式。由于并行多道记录可以并行传输，传输率高，所以单盒容量可达 35GB。DLT 磁带的容量和传输率都高于 8mm 磁带和 DOS

磁带，但价格较高，适用于高档服务器。DLT 磁带记录面积大，在容量扩展上很有潜力，是很有发展前途的技术。

### (5) IBM3480/3590 系列

IBM3480 系列实际上是一个磁带库，它采用 13mm (0.5 英寸) 带盒磁带，单盒磁带容量是 630MB。现在的 IBM3590 系列，每盒容量达 10GB。IBM3480/3590 性能好，机器结构复杂，价格也高。

## 3. 光存储技术

光盘存储器 (Optical Disk Memory, ODM) 和 MSM 类似，也是将用于记录的薄层涂敷在基体上构成记录介质。不同的是，ODM 基体的圆形薄片由热传导率很小、耐热性很强的有机玻璃制成。在记录薄层的表面再涂敷或沉积保护薄层，以保护记录面。记录薄层有非磁性材料和磁性材料两种，前者构成光盘介质，后者构成磁光盘介质。

ODM 是目前辅存中记录密度最高的存储器，存储位元区域可小至  $1\mu\text{m}^2$ ，存储容量很大，盘片易于更换。ODM 的缺点是存储速度比硬盘低一个数量级。现已生产出与硬盘速度相近的 ODM，相信它不久会成为重要的辅存。

目前我们所能接触的光存储设备有 CD-ROM、CD-R、CD-RW、MO、DVD-ROM、DVD+RW、DVD-RW、DVD-RAM、COMBO、BD 等。CD-ROM 为只读光盘，多用于产品发布和电子出版领域；CD-R 允许用户自己写 CD，但只能写 1 次，可以无限次读，而且与 CD-ROM 兼容；CD-RW 为可多次读写光盘，它采用 CD-R 的格式，因此可以与 CD-R 的刻录机通用；MO 是永磁光盘，可以重复读写，具有很高的可靠性和耐久性，数据可保存 100 年。相应的 DVD 产品可以视为 CD 的后代。此外，多台光盘机组合在一起有 3 种结构：光盘库、光盘塔和光盘阵列。它们都是大型信息存储设备，一般应用在大中型网络系统和档案管理系统中。

在所有光存储设备中，最基本的产品是 CD。CD 是“Compact Disc”的简称，直译就是“小型、紧凑的盘片”，其外径为 120mm，厚度为 1.2mm，如图 1-2 所示。

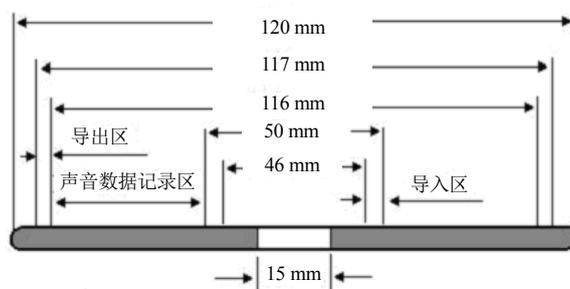


图 1-2 光盘结构

CD 由光轨 (Track) 组成。光轨是光盘上一种数据记录的单位。光盘上储存的信息资料按一定规则排列，其形状像一条条轨道，称为光轨。光轨由内至外呈螺旋线形状。数据光盘内从目录 (Table of Contents, TOC) 开始记录起始地址的多个连续的逻辑扇区为一轨，而音频光盘内一首歌曲对应一条光轨，因此，一张光盘中可能有多条光轨。光盘的光轨最多可达 99 条，如图 1-3 所示。

光轨由一系列记录信息位的坑 (Pit) 与岸 (Land) 组成。其中, 光轨上凹陷下去的部分称为“坑”, 没有凹陷的部分称为“岸”(又称“陆地”)。“坑”和“岸”都是记录的信息, 如图 1-4 所示。



图 1-3 光盘光轨

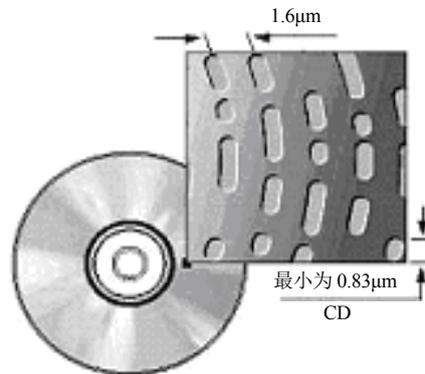
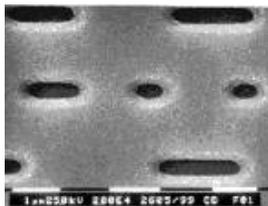


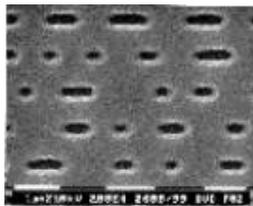
图 1-4 光盘信息位

CD-R 预先在盘片内压制有螺旋线形状的沟槽 (Groove), 称为“预刻槽”, 代替光学轨道的“坑”。刻录时, CD-R 盘片沟槽内的有机染料在激光照射下形成气泡, 这便是“岸”。气泡一旦形成, 就不能恢复原状, 因此, CD-R 只能一次写入。

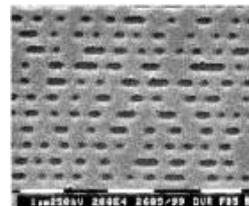
不同光盘的记录密度是不一样的, 如图 1-5 所示。



CD 光盘坑纹



DVD 光盘坑纹



DVD-R 光盘坑纹

图 1-5 不同光盘记录密度对比

光盘信息位采用 EFM (Eight-to-Fourteen Modulation) 编码方式进行编码。将所有信号经过 8 位到 14 位编码调制后, 加上 3 位间隔代码, 形成通道代码后刻录到光盘里。这样处理能保证读取信号的准确性, 如图 1-6 所示。

光驱的激光头读取光盘数据时, “坑”和“岸”的反射系数是一样的, 因此都读成“0”, “坑”和“岸”的长度决定“0”的个数。“坑”和“岸”的交界处, 即“坑”的前后沿读为“1”。如果 8 位数据中有 2 位或 2 位以上的“1”, 光盘无法实现存取。为此, 需要将两个连续的“1”(至少要用两个“0”, 最多 10 个“0”)将它们分开。EFM 编码能够在 14 位数据中提取 256 种不出现连续两个“1”的数据 (通道码) 与 8 位数据对应。为避免相邻两个数据的通道码可能出现两个“1”, 可以在通道码之间再加上 3 位合并码 (DVD 中用 2 位合并码), 形成 17 位通道码。这种通道码可直接用于刻录光盘。读取光盘时, 将 17 位通道码经过解码系统转换为 8 位二进制数据。

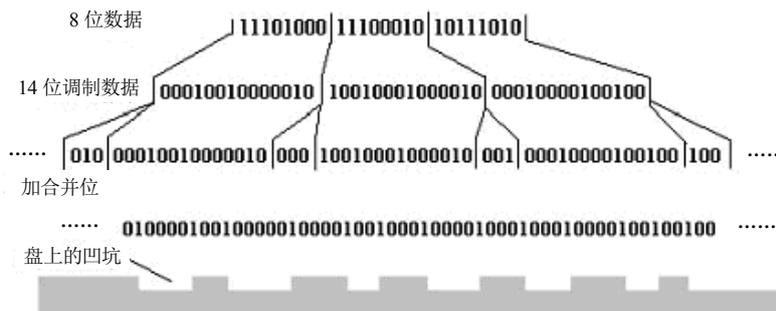


图 1-6 光盘 EFM 编码

光盘提供了存储和发布大文件的一个非常耐久的方法。光盘驱动器利用低能量的激光在光盘表面读取微小的变化。因为信息记录在盘面上，所以光盘容易损坏。光盘的存储容量比软盘大（为 650MB），存储费用比硬盘低，但光盘的访问时间要比硬盘长 2~6 倍。光盘的这些特点使其非常适合于存储那些大容量的、用硬盘存储费用太高的、可以离线操作的数据。

光盘存储一般应用在以下几个方面。

- 电子出版物：作为信息时代的标志之一，电子出版物正在逐渐改变传统的出版行业，而它的存储介质正是光盘。一本厚厚的字典可以被浓缩在一张薄薄的光盘之中，一部精彩的故事片可以用一张 DVD 所收藏，这些变化无不加快了信息的传播，作为存储介质的光盘当然也功不可没。
- 电子图像管理：用计算机处理的图像、照片，其存储容量一般很大，可以使用光盘将它们存入计算机系统的在线存储器中。光盘存储同时也非常适合于存储工程图档（如 CAD 图）、测绘图（如地图）和医学文档等。
- 档案管理：这里是指数据永久性的存储。这些数据不经常被访问，但必须保留，如该公司的一个未被采纳的产品设计说明（因为以后可能需要使用）。
- 备份管理：为防止文件丢失或被破坏，经常需要对系统和用户文件进行复制。光盘系统的容量大，而且可能包括一个自动转换器，因此对光盘系统的复制能节省操作员加载介质的费用。

### 1.1.2 存储技术展望

近年来，各种存储技术不断涌现，其中最值得一提的是 Millipede。

IBM 在 2003 年 12 月 8 日于美国召开的 IEDM 2003（国际半导体制造技术会议）上，公开了高密度存储技术（开发代号：Millipede）的最新进展。该技术采用扫描数千个微小探针的方法来记录和显示信息。Millipede 使用水平方向尺寸为 10nm 左右的微小拱型装置（Cantilever，悬臂），在塑料薄膜上形成微孔（Pit，凹坑）。各凹坑支持独立的位信息。为提高记录密度和数据传输速度，同步运行数千个悬臂，每个悬臂在 100μm 的区域里进行扫描，以十几 nm 到数十 nm 间隔形成微小凹坑。

其实早在 1998 年 IBM 就发布了 Millipede 的第一个样品芯片。当时具有 1 024 个（纵向 32 个，横向 32 个）悬臂。1999 年 IBM 成功实现了 1 024 个悬臂的同步运行（读取、写入）。

在 IEDM 2003 上公布了两项成果：一项是样品芯片的记录密度实现了  $1.140\text{Tb}/\text{in}^2$ ，首次超过  $1\text{Tb}/\text{in}^2$ ，凹坑间隔为  $13\text{nm}$ ；另一项是使用实际图像数据进行信息的记录和显示，通过对当时的误码率进行实测，得到了与现有硬盘相匹敌的  $6\times 10^{-5}$ 。不过，实测采用的 Millipede 的记录密度为数百  $\text{Gb}/\text{in}^2$ 。这种记录方式类似于光盘的记录方式。

IBM 表示，其新的媒质有可能给存储市场带来巨大变革，并且可大大提高移动电话和 PDA 等大众产品的存储能力。“市场渴望更高的存储容量，我们的新型媒质材料的尺寸跟闪存差不多，存储容量则可达到  $5\sim 10\text{GB}/\text{in}^2$ ，而这才刚刚开始。”位于瑞士苏黎世的 IBM 研究所的一位项目负责人 Peter Vettiger 表示。

据 IBM 称，这种代号为“Millipede”的新型媒质在邮票大小的面积内可存储 2 500 万页的内容。Millipede 并非采用传统的磁或电存储方式，而是利用数以千计的纳米级小突起将代表每位数据的单元格挤压到一个很薄的塑料胶片上。Millipede 项目的核心是 V 字形硅悬臂的二维阵列，这些 V 字形硅悬臂厚度为  $0.5\mu\text{m}$ ，高度为  $70\mu\text{m}$ 。在每个悬臂末端是一个不足  $2\mu\text{m}$  长、指向下方的小突起。电磁脉冲在 x 轴和 y 轴方向上移动 V 字形硅悬臂阵列下的存储媒质，使得每个小突起在其自己的边长  $70\mu\text{m}$  的存储区域内执行读写操作。IBM 声称：短距离可确保低功耗。

这种材料可大大改善存储区域网络的磁带媒质，而且有可能替代主流应用中的闪存器件。但是，这种媒质的主要问题是每兆字节的成本。Vettiger 相信技术可解决成本问题：“与磁带或闪存媒质相比，我们的这种新存储材料的单位成本应能控制在合理范围内。”

其他网络存储方面的知识这里就不再做进一步的介绍了。

## 1.2 数据恢复技术总论

随着全球信息化的飞速发展，数据已经成为企业的一项最重要的资产，数据存储的可用性、完整性和安全性已不再是一个单纯的技术问题，更是企业生存力和竞争力的重要体现。这对部门、单位，甚或个人亦然。

### 1.2.1 数据的内涵

什么是数据呢？

这里我们所说的数据，仅指计算机数据，后面不再专门指出。“数据”是一个广泛的概念，不仅包括计算机文件系统或数据库系统中存储的各种文本、图形、图像、声音等形式的数据文件、软件或各种文档资料，也包括存放或管理这些信息的硬件信息，如计算机硬件及其网络地址、网络结构、网络服务等。尽管在许多文献中都大量引用“数据”与“信息”两个术语，但却没有公认的“数据”与“信息”的定义。本书中对“数据”与“信息”不加以区分，视为同义。

### 1.2.2 数据恢复的定义

什么是数据恢复呢？

简单地说，数据恢复就是把遭受破坏或由硬件缺陷导致的不可访问、不可获得或由于误操

作等各种原因而丢失的数据还原成正常数据，即恢复至本来“面目”。

数据恢复不仅对已丢失的文件进行恢复，还可以恢复物理损伤的磁盘数据，也可以恢复不同操作系统的数据库。

概括地说，数据出现问题主要包括两大类，分别是逻辑问题和硬件问题，相对应的恢复也分别称为软恢复和硬恢复。所谓软恢复是指一切可以通过“软”的方式进行的恢复，不涉及硬件修理的数据恢复操作，其故障原因不是因硬件失效造成的，如病毒感染、误格式化、误分区、误克隆、误操作、网络删除、操作时断电等，一般表现为无操作系统、读盘错误、文件找不到或打不开，以及报告无分区、未格式化、密码丢失、乱码等；对应地，一切涉及硬件修理、由硬件损坏或失效造成的数据恢复均归入硬恢复，如磁道损坏、磁盘划伤、磁组损坏、主电机损坏、电路板芯片及其他元器件烧坏等，一般表现为不认盘、常有一种“喀嚓喀嚓”的磁组撞击声、电机不转、通电后无任何声音等。两者之间最明显的特征或区别就是：存储介质本身是否需要修理或更换部件才可以正常地进行访问。当然，“正常地进行访问”也是一个有级别的问题，这里先界定为低级格式化程序这一级别，更详细的区别在后面详细介绍。

数据恢复是出现问题之后的一种补救措施，它既不是预防措施，也不是备份措施。所以，在一些特殊情况下数据将很难被恢复，如数据被覆盖、低级格式化清零、磁盘盘片严重损伤等。

### 1.2.3 数据恢复的服务范围

造成数据丢失的原因非常多，常见的主要有以下 9 种。

- 恶意的程序：最常见的恶意程序是病毒。很多人认为病毒对数据的影响仅仅是病毒的破坏性，这是不正确的，实际上病毒的感染本身就是一种破坏。但是，恶意程序造成的破坏并不一定最难恢复。
- 其他恶意的破坏：即使不借助病毒或者其他工具，只要拥有足够的权限，任何系统都有一定的“自毁”能力。例如，依靠系统正常的删除、移动、格式化等操作也可以达到破坏数据的目的。随着网络技术的发展，威胁已经不局限于本机，通过网络（局域网、城域网和广域网）进行破坏蔚然成风。特别是对于一些初学者，如连在局域网上的 Windows 2000 操作系统，为自己使用的用户名设置了必要的密码，而对“Administrator”这个具有系统最高权限的用户名密码却为空，这就使任何一个连接在网上的非法用户都可以对该系统进行不与操作系统相冲突的任何操作。
- 误操作：很多数据丢失源于使用者的操作失误，如误删除、误格式化等。
- 操作系统或应用软件的错误：随着操作系统和应用程序的代码量的成倍增加，Bug 也在不断增加。操作系统和应用软件的错误，往往会给人们的工作带来一些不可预期的影响。例如，某游戏安装在默认目录下可能会出现丢失扩展分区这样严重的问题。
- 硬件失效：这也是丢失数据的重要原因之一，如磁盘失效、电源不稳造成自动重启等。硬件失效往往是最严重的问题，包括物理损坏、失窃等，将使数据恢复的可能性降低为零。
- 加密和权限：尽管加密和权限设置是保护数据的有效手段，但是遗忘密码也会带来很大的问题。
- 掉电：机器突然掉电的后果不仅仅是内存数据丢失，还可能造成磁盘数据丢失、文件不同步、或导致系统无法正常启动等问题。

- 内存溢出：导致内存溢出或者进程非法终止等低层错误的原因很多，它就像掉电一样，会丢失当前的工作。
- 升级：软件系统升级有时也会带来一些问题，如兼容性和稳定性方面的问题等。数据出现问题后会表现出一些相应的症状，主要有以下几种情况。

### 1. 无法进入系统

有时虽然 CMOS 检测硬盘正常，但却启动不了系统，提示停机，无提示当机，或者 CMOS 能检测到硬盘而显示的容量却不正确。出现这些情况的原因有很多，如 MBR 损坏、DBR 损坏、电源质量不合格、数据线断线、CMOS 设置不正确、主从设置不正确、硬件冲突、CMOS 电池电压不足等。一般性的系统无法启动可能会有以下一些提示。

- **Invalid Partition Table:** 无效的分区信息。一般是因为分区信息中 1BE、1CE、1DE、1EE 处不符合只有一个 80 而其他为 0 的原则，用工具设定解决。
- **Error Loading Operating System:** 主引导程序读 BOOT 区 5 次仍不成功。可用工具重建 BOOT 区解决。
- **Missing Operating System:** DOS 引导区的“55 AA”标记丢失或 DBR 损坏。可用工具设定解决。
- **Non-System Disk or Disk Error:** BOOT 区中的系统文件名与根目录中的前两个文件不同。可用 SYS 命令重新传递系统解决。
- **Disk Boot Failure:** 读系统文件错误。可用 SYS 命令重新传递系统解决。
- **Invalid Driver Specification:** 在试图切换到一个确实存在的逻辑分区时出现该信息，说明主分区表的分区记录遭到破坏。可根据各分区情况重建分区表，或者用自动修复工具修复。分区丢失是最常见的故障之一。一般来说，数据没有问题，如果不了解处理方法，可以使用自动修复分区工具进行处理。这种情况大多只是主分区表被改写，不会影响其他数据。特别提醒读者，这些工具具有的不支持 8.4GB 硬盘，有的与 BIOS 对硬盘的识别有关系。如果在一台机器上无法修复，可以换一台 BIOS 不同的机器尝试一下。这些工具对分区的修复能力都有限，主要是通过查找被搬移的分区表或备份的分区表来进行修复，成功率较低。所以，对于分区表的修复，主要是靠手工方式。
- **Bad or missing command interpreter:** 找不到 COMMAND.COM，或者 COMMAND.COM 文件损坏。如果复制正确的 COMMAND.COM 文件后还是如此，一般来说是感染了某种病毒。
- **Invalid media type reading drive. Abort, Retry, Fail:** 该盘没有高级格式化，或者 BOOT 区中 I/O 参数表被破坏。这种情况较多，手工处理比较复杂。特别指出，此时 DiskEdit 可能无法运行，建议用工具修复。
- **Incorrect DOS Version:** 可能是文件版本不统一。对 Windows 9x 来说，有 95、95 OSR/2、98、98 OEM/2 等版本，重传系统时，要注意选用正确版本的启动盘。另外，在引导扇区的代码区完全被破坏的情况下，系统的提示来自 BIOS，这些提示与 BIOS 的版本有关。这时，经常采用的手段是使用 FDISK/MBR 重建代码区。还有一种比较极端的情况，就是硬盘自检正常，而用软盘和硬盘都无法正常启动，这可能是病毒或恶意程序利用 DOS 3.0 以上版本启动时都要检索分区表这一特点，把分区表置为死循环，造成启动中当机。网上流传的 DOS 6.22k 修改方案，其实是修改西文 MS-DOS 6.22 的 IO.SYS 文件，把“C2 03 06 E8

0A 00 07 72 03” 替换为 “C2 03 90 E8 0A 00 72 80 90”，这样就可以启动被类似情况锁住的硬盘。

- **Primary master hard disk fail:** 硬盘数据线、电源线两者至少有一个没插好，或硬盘跳线设置变化，而 CMOS 硬盘参数没做相应修改。插好连线，或相应地修改正确即可。
- **Not Found any active partition in HDD:** 硬盘分区表中的活动分区标志 “80H” 被改成非活动分区标志 “00H”。用 DiskEdit 等工具修复为 “80H” 即可。
- **Type the name of the command, Interpreter:** 硬盘分区表中的主 DOS 分区标志 “06H” 错误，或者 COMMAND.COM 文件丢失、损坏或与其他两个启动文件版本不同，或者被病毒破坏。
- **Disk I/O error:** 主 DOS 引导记录中物理硬盘标志号错误，或介质描述错误。
- **Invalid system disk 或 Failure:** 主 DOS 引导记录损坏。

## 2. 磁盘出现坏道

硬盘坏道分为逻辑坏道和物理坏道两种。前者为软坏道，通常由软件操作或使用不当造成，可用软件修复；后者为物理性坏道，表明硬盘磁道产生物理损伤，只能通过更改硬盘分区或扇区的使用情况来解决。

出现下列情况通常表明硬盘上存在坏道。

- 在打开、运行或复制某个文件时，硬盘出现操作速度变慢，长时间操作仍不成功或表现为长时间死“啃”某一区域，或同时出现硬盘读盘异响，或干脆 Windows 系统提示“无法读取或写入该文件”，这些都表明硬盘的某部分出现了坏道。
- 每次开机，ScanDisk 磁盘扫描程序都自动运行。这肯定表明硬盘上有需要修复的重要错误，比如，坏道。在运行该程序时如不能顺利通过，表明硬盘肯定有坏道；或扫描虽然可以通过，但出现红色的“B”标记，也表明硬盘有坏道。
- 计算机启动时硬盘无法引导，用软盘或光盘启动后可看见硬盘盘符，但无法对该分区进行操作，或操作有误，或干脆就看不见盘符，都表明硬盘上可能出现了坏道。具体表现如：开机自检过程中，屏幕提示“Hard disk drive failure”、“Hard drive controller failure”等类似信息，则可以判断硬盘驱动器或硬盘控制器有硬件故障；读写硬盘时提示“Sector not found”或“General error in reading drive C”等类似错误信息，则表明硬盘磁道出现了物理损伤。
- 计算机在正常运行中出现当机或提示“该文件损坏”等情况，也可能和硬盘坏道有关。

## 3. 分区丢失

分区丢失是指找不到分区或进入不了分区，多由病毒引起。

## 4. 文件丢失

误删除、误格式化等常导致文件丢失，主要使用工具软件进行恢复。

## 5. 密码丢失

数据加密技术是一门专门的技术，从远古时代原始的加密技术，到现在的数据加解密技术，只要有信息，就一定有加密存在。密码，已经成为现代人的一个重要特征，涉及方方面面。可以说，现代人已经被各种各样的密码包围起来了。不过，这里要谈的密码，只是特定类型的应用程序在存储自己专用的数据文件时使用的一种口令保护，如 ZIP 文件的解压缩口令等。

对于这类文档的密码遗失问题，可以说是“解铃还需系铃人”，就是借助计算机强大的数据处理能力，对文档进行暴力破解，通过逐个尝试可能的组合来找回原始密码。其原理基础是：虽然不知道正确的密码是什么，但是却可以知道某一个密码正确与否。

#### 6. 文档打不开或打开后是乱码

文档修复也是一个常见的问题。它是指对某种应用文档受损不能打开或打开后为乱码的修复，是广义数据恢复的一支。通常所说的狭义数据恢复一般是相对操作系统而言的，是指文件逻辑存储上不可见的恢复。而文档修复是指对于特定的应用程序，由于数据逻辑上的原因，无法合理、正确地解释文档数据的实际意义，一般表现为文件损坏、无法打开或打开后为乱码。但从操作系统的角度来看，此时文档的读写没有任何问题（操作系统只将文档视为一个整体，可以正常地存储和管理，它并不关心文档中数据的具体含义）。

关于文件和文档，一般意义上讲，文件是一个通用概念，存储在存储介质上的所有内容都可以称为文件，是相对操作系统而言的；而文档一般是指由各种应用程序创建的特定类型的文件，大都是用户的数据文件，也就是说，文档是特定类型的文件。在本书中，文档和文件不做区分，视为同一含义。

明白了文档修复的原理，就可以给文档修复下一个定义了：文件由于数据逻辑上的原因，对于操作系统可见，却无法被相应的应用程序合理、正确地解释，从而出现如文件损坏无法打开或打开后显示乱码等情况，通过纠错、重新计算 CRC 值、改正不正确的格式等手段解决这些问题的过程称为文档修复。

例如，一个 Word 文档，由于存储时的某种原因，将字符编码类型标志位改变，从而造成格式上出现错误，使 Word 在打开它时无法正确解释其实际存储的内容，显示为乱码，但通过重新设置字符集的标志位可使文档恢复本来面目。这个过程就是文档修复。

这些问题都在数据恢复的服务范围之内。

### 1.2.4 数据恢复的一般原则

如何能让我们的数据更安全？这是每个关心数据安全的人每天的工作。但是，对于“数据安全到底是什么”这个看似简单的问题，却没有几个人能说清楚，即使是数据安全的专业人士也不例外。这就好像是“1+1=2”这个妇孺皆知的等式，却只有陈景润这样的世界顶级学者才可以给予充分的论证。现在，我们就来回答这个问题：数据安全是一个过程，而且，它是一个动态的过程。

明确理解了数据安全的动态特性后，“从根本上解决身边的安全问题”也就不会是一句空谈。安全需要以动制动。作为工程师，经常听到用户抱怨：“为什么花了那么多的钱，买了数据安全的专业产品，专门搭建了解决方案后，还是会出现数据丢失的问题？”

如果仔细品味数据安全的动态特性，就可以解答这些抱怨：因为安全产品/方案是静态的，而安全本身是过程的，是动态的。用静态的东西去应对动态的过程，显然达不到用户所期待的效果。这就是为什么所有的解决方案都不能做到万无一失的原因。

进行数据恢复，首要的一点就是要认真、细致，对每一步的操作都有一个明确的目的。因为数据安全既然是一个动态的过程，那么，所出现的问题也是千差万别的，是没有定式可言的。所以，在进行操作之前就必须考虑好做完该步之后能达到什么目的，可能造成什么后果，能不

能回退至上一状态。特别是对于一些破坏性操作，一定要考虑周到，只要条件允许，就一定要在操作之前进行备份，对每一步操作都必须有相应的记录，并能回退到上一状态。

在开始恢复数据之前，应该首先完成以下几个步骤。

第 1 步 备份当前尚能工作的驱动器上的所有数据。如果 C 盘损坏，那么，在开始任何工作之前首先备份 D 盘（及其他盘）上的数据到其他可靠的地方。

第 2 步 将损坏的硬盘拿到一个正常工作的同样的操作系统下，如果条件不允许，取下该硬盘，安装一个新的主硬盘，在重新挂上损坏硬盘之前对主硬盘分区并格式化，确信立即更改 CMOS 设置。

第 3 步 调查使用者。查出在丢失数据之前发生的事情，查出是否有其他的应用程序对磁盘进行过操作。最后的用户输入非常重要，要查出使用者在送交磁盘前做过些什么，虽然他并没有说出来。

第 4 步 如果可能，备份所有扇区是一个非常不错的方法。按文件进行的转存在这里没有任何的帮助。如果进行克隆，确保是按位进行而不是按文件进行。

第 5 步 手头要有一个好的扇区编辑工具，如 WinHex 就是一款不错的基于扇区的编辑工具。

第 6 步 尽可能多地得到最后使用者的关键文件的信息。

了解完这些信息后，就该有一个基本轮廓：为什么会出现这个问题？破坏程度如何？使用什么工具能达到最好的恢复效果？其主要步骤有哪些？另外要记住的是：先抢救最有把握修复的数据，恢复一点，备份一点！

### 1.3 硬盘数据恢复与硬盘修理的区别与联系

硬盘数据恢复与硬盘修理的最直接的区别就是，它们的目的不一样：硬盘数据恢复是为了得到硬盘上的数据，而硬盘修理是为了让硬盘能够重新正常地工作，单纯的硬盘修理是不考虑其上存储的数据的，如很多硬件厂商的保修条款那样，硬盘出现问题，可以免费修理或更换，但是对其上存储的数据不进行任何的处理，其数据的处理权在用户自己。然而两者之间也不是完全独立的，因为有些时候要恢复数据，需要先对硬盘进行处理，当然，这时的硬盘处理已经不是单纯的修理硬件，而是为了获得其中的数据，并且，该过程甚至是一个破坏性的处理过程。注意这里所说的“处理”与“修理”在含义上的区别。硬盘修理与硬盘数据恢复的关系如图 1-7 所示，其他介质亦然。

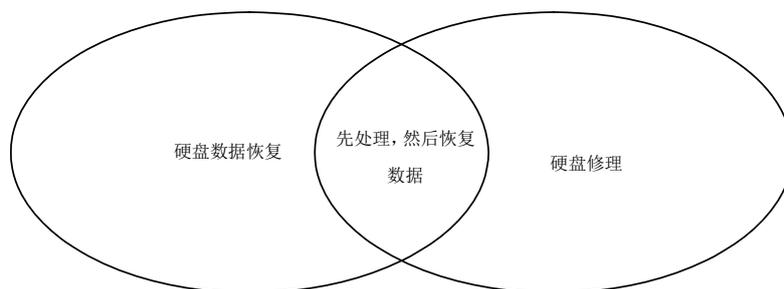


图 1-7 硬盘数据恢复与硬盘修理的关系

另外，磁盘硬件的修理与数据恢复的代价也不一样，其关系如表 1-2 所示。

表 1-2 硬件的修理与数据恢复比较

内 容	磁盘硬件修理	数据恢复
目的	硬件正常工作	得到数据
方式	维修	软硬结合
工具	测量仪器、烙铁等	系统软件、特殊工具软件、修理工具
代价	不大于新硬件成本	与硬件关系不大，取决于数据
成本	修理费用	智能劳动

## 1.4 硬盘数据保护方式介绍

目前对于数据的重要性一般用户都有认识，出了问题后即使没有重要的数据需要恢复，但重构系统也是一件十分费时费力的事情，因此，就涌现了大量的硬盘保护方式，或拦截中断，对硬盘数据进行保护，或采用镜像方式，对硬盘数据进行备份。这些方式概括起来主要有以下几种：操作系统提供的系统还原功能、随机赠送的系统恢复光盘、Ghost、杀毒软件提供的系统备份功能、硬盘保护卡（还原卡）、主板 BIOS 内置的系统保护功能、虚拟还原工具软件等。

这些保护方式与数据恢复技术最本质的区别是：数据恢复是对出现问题的系统或存储介质上的数据进行恢复，而数据保护虽然也是为了保护系统或数据，却是一种预防措施。当然，如果预防措施做得好，不出现问题，那是最好不过的了，但是，使用这些工具也有很大的缺陷，因为毕竟这些保护方式不是万能的，它无形中又增加了用户的操作，既然是操作，就无法避免误操作，这是其一。其二，它们都建立在硬件正常的基础之上，如果硬件出现问题，它们只会使事情更加糟糕。当然不是说这些保护方式不好，它们对用户数据的保护是有目共睹的，但从其机理来看，它们都对操作系统或硬盘关键数据区动过“手脚”，所以，不出现问题则已，一旦出现问题，就必然会大大增加数据恢复的难度和工作量。

### 1.4.1 操作系统提供的系统还原功能

操作系统提供的系统还原是目前使用较多的一种保护方式。微软从 Windows Me 开始提供该功能，在 Windows 2000 中取消了这一功能，而在 Windows XP 中又强化了这一功能。该功能的优点和缺点都很明显：优点是操作系统自带、免费，不存在兼容性问题，使用也很方便；缺点是只恢复操作系统数据，对用户数据无效，且 Windows 2000 没有该功能。另外，其致命缺陷是操作系统本身不能崩溃，且对硬件失效无效。

操作系统提供的系统还原功能，其使用和恢复都很简单，不再详细介绍。

### 1.4.2 随机赠送的系统恢复光盘

早期的随机赠送的系统恢复光盘只能对整个硬盘进行恢复，不能只恢复系统分区，现在已经大有改善，有些甚至可以做到只恢复系统，不覆盖用户数据。其优点与操作系统的还原功能

相类似，但它可以恢复崩溃的操作系统；缺点是各厂商相互差别很大，可以说是参差不齐，如果使用不当，可能会覆盖系统分区下的用户数据，造成数据彻底无法恢复。

随机赠送的系统恢复光盘，其使用和恢复都很简单，使用前要注意阅读光盘说明，不再具体介绍。

### 1.4.3 Ghost

使用 Ghost 对磁盘或磁盘分区做镜像，可能是最早的操作系统全盘（或逻辑盘）备份方式，曾经辉煌一个时代。最早的 Ghost 不兼容 NTFS 分区，现在的版本早就解决了这个问题。可以说，它是爱“折腾”计算机和操作系统的 DIYer 的最爱。

由于只能在 DOS 下对系统进行镜像，所以其缺点是很明显的——它只能是一种静态备份。对于 Ghost，就不做更多介绍了。

### 1.4.4 杀毒软件提供的系统备份功能

有些杀毒软件提供了备份功能。例如，瑞星提供了系统重要数据备份功能，且可以采用增量备份方式，以加快备份速度；采用超容压缩数据保护技术，无须用户干预，定时自动保护计算机系统核心数据，即使在硬盘数据遭到病毒破坏，甚至硬盘格式化后，都可以迅速恢复硬盘中的宝贵数据。

显然，这种备份方式是远远不够的。

### 1.4.5 硬盘保护卡

现在有很多厂商生产和销售一种称为“硬盘保护卡”的设备，有 ISA 接口的，也有 PCI 接口的，由于 ISA 接口已经淘汰，所以以 PCI 接口最为常见。硬盘保护卡具有不占硬盘空间（实际是需要占用硬盘空间的）、支持多种数据还原方式、安装和使用过程简单等特点，简化了机房管理工作，所以这类产品非常丰富，大量见于机房、网吧等公用机上。

其基本原理是，对一台已安装好系统并有一些数据的计算机来说，可以把它目前的数据状态 A 记录下来并锁定，从此以后，我们在计算机上的操作会形成另一种数据状态 B，数据状态 B 的变化不会对数据状态 A 产生任何影响，换句话说，数据状态 A 经过特殊的处理后，已经变得“百毒不侵”，就好像加了一层防护罩。所以当计算机遇到安全威胁时，只要将整个计算机恢复到数据状态 A 即可。由于数据状态 A 一直是很稳定、很安全的，所以那些威胁自然就消失了。换句话说，所有的威胁都产生于数据状态 B，计算机恢复到数据状态 A 就意味着数据状态 B 消失了，威胁也就不存在了。显然，计算机不能恢复到数据状态 B，数据状态 B 所做的工作仍然会丢失。

这类产品有两种保护方式，一类是采用像“再生卡”、“还原卡”之类的硬件插卡，使用“硬盘分区相互备份法”进行数据备份，另一类是把硬盘的一部分分割出来，用以备份硬盘的重要数据，以便随时还原。还原卡不对硬盘数据进行备份，只记录硬盘的读写操作，当用户设置还原点后，不论是操作系统安装新的程序还是删除文件，都记录在还原点之外，且不会影响原有的硬盘数据。当需要还原时，还原卡根据记录把还原点内的数据恢复，并删除还原点以外的数据。

### 1.4.6 主板 BIOS 内置的系统保护软件

在有些主板的 BIOS 中内置了系统保护软件，如联想的“宙斯盾”（RecoveryEasy）和捷波的“恢复精灵”（Recovery Genius）等都是这类工具。实际上，它们都是系统还原卡的另外一种形式，相当于将这个备份恢复程序移植到主板 BIOS 中。

联想的“宙斯盾”可以为用户提供硬盘数据备份与恢复、CMOS 设置备份与恢复及多重引导等功能，整个程序内置于 BIOS 中。它采用固定镜像方式进行备份，在硬盘中选择一个区域存放备份的数据，所选区域对操作系统而言不可见，在操作系统下也不能访问——甚至包括病毒。其缺点是对硬盘分区数量有限，还要占用一定的硬盘空间，兼容性也不够。

捷波的“恢复精灵”由于其强大的功能和易移植性，早已成为 DIYer 备份硬盘数据的宠儿，将它压制到各种主板 BIOS 中。“恢复精灵”采用动态备份方式，在硬盘中划分一个很小的保护区（所占比例为整个硬盘空间的 1/2 048）来备份数据，可以将误删除的数据和被格式化的数据还原（Windows XP 系统还原功能只还原程序，不还原数据；而“恢复精灵”则会将硬盘上所有数据还原），甚至可以恢复进行过 FDISK 的数据；在系统崩溃、误操作、意外掉电后迅速（不到 5 秒）恢复到备份之前的状态，而且是在进入操作系统之前（不必重新启动即可直接进入 Windows）进行恢复，根本不用担心系统受到破坏而无法恢复。

类似的工具还有奔驰主板的“数据保险柜”等，不再详细介绍。

显然，这种备份方式也是远远不够的，总是要丢失部分数据。

### 1.4.7 虚拟还原工具软件

虚拟还原的运作原理与硬盘保护卡比较类似，可备份整个硬盘内的数据。

虚拟还原有永久还原点和动态还原点两种备份方法。简单地说，永久还原点就是将整个硬盘的内容都备份起来，动态还原点就是将当前硬盘内容与最新永久还原点之间的差异备份起来。所以，在建立动态还原点之前必须建立永久还原点。

“还原精灵”也是一款提供虚拟还原功能的工具软件，号称“软件做的硬盘保护卡”，其原理也和硬盘保护卡的原理相似。由于该软件有全中文操作界面和说明手册，这里就不再做进一步的介绍了。

### 1.4.8 硬盘保护与数据恢复

硬盘保护产品还有很多，也不断有新品出现，但不管采用哪种方式，或者是静态备份，或者是动态备份，都脱不了备份这个本质，哪怕是动态备份，也不可能是实时备份。即使将来技术进步了，做到实时备份，它也只是一个备份手段，是建立在存储系统正常工作基础之上的备份手段，永远不可能代替数据恢复技术。另外，这种保护也不是绝对的，现在已经有多种方法可以绕过这些保护方式。而且，多了一步操作，就必然不可避免地增加误操作的几率，如误还原会造成还原点之后所有的工作全部丢失。当然，有些误操作可以通过数据恢复技术找回来，但有些误操作会造成数据从此“魂飞魄散”。

## 1.5 硬盘缺陷

在这里，暂不探讨在各种操作系统下硬盘中的数据结构问题及数据恢复问题，而是直接探讨硬盘本身的缺陷。

### 1.5.1 硬盘缺陷介绍

在硬盘内部，所有存在缺陷的部分都称为“Defect”（缺陷）。如果某个磁头状态不好，则这个磁头为“Defect Head”；如果盘面上某个磁道（Track）不能正常访问，则称之为“Defect Track”；如果某个扇区不能正常访问或不能正确记录数据，则该扇区也称“Defect Sector”，可以认为“Bad Sector”等同于“Defect Sector”。总的来说，某个硬盘只要有一部分存在缺陷，不能完全正常工作，就称这个硬盘为“Defect Hard Disk”。

通常可将硬盘的缺陷分为 6 大类。

#### 1. 坏扇区

坏扇区（Bad Sector），也称缺陷扇区（Defect Sector），是指不能被正常访问或不能被正确读写的扇区。一个扇区能存储 512Byte 数据，如果在某个扇区中有任何一个字节不能被正确读写，则这个扇区为坏扇区（Bad Sector）。除了存储 512Byte 数据外，每个扇区还有数十 Byte 的信息，包括标志信息、校验码、地址信息等。这些信息中的任何一个字节出错都会导致该扇区变“Bad”。例如，在低级格式化的过程中，每个扇区都分配有一个编号写在 ID 中，如果 ID 部分出错就会导致这个扇区无法访问，则这个扇区属于 Bad Sector。一般表现为：高级格式化后发现“坏簇”（Bad Cluster）；用 ScanDisk 等工具检查发现有“B”标记；用某些检测工具有扇区错误提示等。有一些 Bad Sector 能够通过低级格式化重写这些信息来纠正。

多数专业检测软件在检测过程中发现缺陷时，都有类似的错误提示信息。常见的扇区缺陷主要有以下 4 种情况。

- 校验错误（ECC Uncorrectable Errors，又称 ECC 错误）：系统每次在向扇区中写数据的同时，都根据这些数据经过一定的算法运算生成一个校验码（Error Correction Code，ECC），并将这个校验码记录在该扇区的信息区内。以后从这个扇区读取数据时，都会同时读取其校验码，并对数据重新运算以检查结果是否与校验码一致。如果一致，则认为这个扇区正常，存放的数据正确有效；如果不一致，则认为该扇区出错。这就是校验错误。这是硬盘最主要的缺陷类型。导致这种缺陷的原因主要有磁盘表面磁介质损伤、硬盘写功能不正常、校验码的算法差异。
- IDNF 错误（Sector ID Not Found）：即扇区标志出错，会造成系统在需要读写时找不到相应的扇区。造成这个错误的原因可能是系统参数错乱，导致内部地址转换错乱，系统找不到指定扇区；也有可能是某个扇区记录的标志信息出错导致系统无法正确辨别扇区。
- AMNF 错误（Address Mark Not Found）：即地址信息出错，一般是由于某个扇区记录的地址信息出错，系统在访问时发现其地址信息与系统编排的信息不一致造成的。
- 坏块标记错误（Bad Block Mark）：某些软件或病毒程序可以在部分扇区强行写上坏块标记，

让系统不使用这些扇区。这种情况严格来说不一定是硬盘本身的缺陷，但想清除这些坏块标记却不容易。

与坏扇区直接关联的就是坏簇（Bad Cluster）。在用户对硬盘分区并进行高级格式化后，每个分区都会建立文件分配表（File Allocation Table, FAT）。FAT 中记录了该分区内所有簇（Cluster）的使用情况和链接关系。如果在高级格式化（或工具软件的扫描）过程中发现某个 Cluster 使用的扇区包括坏扇区，则在 FAT 中记录该 Cluster 为“Bad Cluster”，并在以后存放文件时不再使用该 Cluster，以避免数据丢失。有时病毒或恶意软件也可能在 FAT 中将无坏扇区的正常 Cluster 标记为 Bad Cluster，导致正常 Cluster 不能被使用。这里需要强调的是：每个 Cluster 包括若干扇区，只要其中存在一个坏扇区，则整个 Cluster 中的其余扇区都不再被使用。

## 2. 磁道伺服缺陷

现在的硬盘大多采用嵌入式伺服，硬盘中每个正常的物理磁道都嵌入了一段或几段信息作为伺服信息，以便磁头在寻道时能准确定位及辨别正确编号的物理磁道。如果某个物理磁道的伺服信息受损，该物理磁道就可能无法访问，这就是磁道伺服缺陷（Track Servo Defect），一般表现为分区过程非正常中断、格式化过程无法完成、使用检测工具检测时中途退出或当机等。

## 3. 磁头组件缺陷

磁头组件缺陷（Heads Assembly Defect）是指硬盘中磁头组件的某些部分不正常，造成部分或全部物理磁头无法正常读写，包括磁头磨损、磁头接触面脏、磁头摆臂变形、音圈受损、磁铁移位等，一般表现为通电后，磁头动作发出的声音明显不正常、硬盘无法被系统 BIOS 检测到、硬盘无法分区或格式化、硬盘格式化后发现从前到后都分布有大量的坏簇等。

## 4. 系统信息错乱

下面介绍系统信息错乱（Service Information Destruction）。每块硬盘内部都有一个系统保留区（Service Area），里面分成若干模块，保存了许多参数和程序。硬盘在通电自检时，要调用其中大部分程序和参数。如果能读出这些程序和参数模块，而且校验正常，硬盘就进入准备状态。如果某些模块读不出或校验不正常，则该硬盘就无法进入准备状态，一般表现为 PC 系统的 BIOS 无法检测到该硬盘或检测到该硬盘却无法对它进行读写操作。例如，Maxtor 美钻二代系列硬盘通电后，磁头响一声，马达停转；Fujitsu 某系列硬盘在通电后，磁头正常寻道，但 BIOS 却检测不到；Quantum 火球系列硬盘，系统能正常认出型号，却不能分区及格式化；Western Digital 的 EB、BB 系列硬盘，能被系统检测到，却不能分区及格式化等。

## 5. 电子线路缺陷

电子线路缺陷（The Board of Electronics Defect）是指硬盘的电子线路板中部分线路断路或短路，某些电气元件或 IC 芯片损坏等。有些电子线路缺陷可以通过观察线路板发现，有些则要通过仪器检测才能确认，一般表现为硬盘在通电后不能正常起转、起转后磁头寻道不正常等。

## 6. 综合性能缺陷

综合性能缺陷（Complex Reliability Defect）是指：有些硬盘在使用过程中部分芯片特性改变；有些硬盘受震动后物理结构产生微小变化（如马达主轴受损）；有些硬盘在设计上存在缺陷，最终导致硬盘稳定性差，或部分性能达不到标准要求。综合性能缺陷一般表现为工作时噪

音明显增大、读写速度明显太慢、同一系列的硬盘大量出现类似故障、某种故障时有时无等。

## 1.5.2 出厂处理

硬盘厂商在生产硬盘时都有一个基本的处理流程。

第 1 步 在生产线上装配硬盘的硬件部分，用特别设备将伺服信号 (Servo Write) 写入盘片。

第 2 步 格式化硬盘的系统保留区，并向系统保留区写入程序模块和参数模块。系统保留区一般位于硬盘 0 物理面的前面几十个物理磁道。写入的程序模块一般用于硬盘内部管理，如低级格式化程序、加解密程序、自监控程序、自动修复程序等。写入的参数多达近百项，如型号、系列号、容量、口令、生产厂商与生产日期、配件类型、区域分配表、缺陷表、出错记录、使用时间记录、S.M.A.R.T 表等，数据量从几百 KB 到几 MB 不等。有些参数一经写入就不再改变，如型号、系列号、生产时间等；而有些参数则可以在使用过程中由内部管理程序自动修改，如出错记录、使用时间记录、S.M.A.R.T 表等。有些专业的维修人员可以借助专业的工具软件随意读取、修改写入硬盘中的程序模块和参数模块。

第 3 步 将所使用的盘片表面按物理地址全面扫描，检查出所有的缺陷磁道和缺陷扇区，并将这些缺陷磁道和缺陷扇区按实际物理地址记录在永久缺陷列表 (Permanent Defect List, P-List) 中。这个扫描过程非常严格，能把不稳定、不可靠的磁道和扇区也检查出来，将其视同缺陷一并处理。现在的硬盘密度极高，盘片生产过程再精密，也很难完全避免缺陷磁道或缺陷扇区。一般新硬盘的 P-List 中都有少则数百，多则上万个缺陷记录。P-List 存放在系统保留区中，一般用户无法查看或修改。如果是 SCSI 硬盘，可以找到多种通用软件查看 P-List，因为各种品牌的 SCSI 硬盘使用兼容的 SCSI 指令集。不同品牌、不同型号的 IDE 硬盘使用各自的指令集，想查看其 P-List，只能借助有针对性的专业工具软件来实现。

第 4 步 系统调用内部低级格式化程序，根据相应的内部参数进行内部低级格式化。在内部低级格式化过程中，完成对所有磁道和扇区的编号、信息重写、清零等工作。在编号时，采用跳过 (Skipped) 的方法忽略记录在 P-List 中的缺陷磁道和缺陷扇区，保证以后用户不会也不能使用到那些缺陷磁道和缺陷扇区。因此，新硬盘在出售时是无法检测到缺陷的。如果是返修的硬盘，一般在厂商特定的维修部门进行检测维修。

## 1.5.3 硬盘高级修理

如果不在硬盘工厂工作，对普通用户或维修人员来说，该如何处理硬盘的缺陷呢？前面已经把硬盘的缺陷分为 6 大类，对不同类型的缺陷自然要用不同的处理方法。

### 1. 综合性能缺陷

综合性能缺陷一般涉及稳定性问题。用户随时都有丢失数据的危险，可以说是“用之担惊，弃之可惜”。维修人员很难从根本上解决这类问题，建议用户及早更换硬盘。

### 2. 磁头组件缺陷

对于磁头组件缺陷，解决方法是更换磁头组件。这对设备及环境要求较高，维修成本也很高。除非是要求恢复其中的数据，否则不值得进行修复。有条件的维修公司可以在百级净化室

中更换硬盘的磁头组件，对数据进行拯救。

如果条件允许，打开盘体后，首先用数字万用表检测磁头机械臂驱动线圈是否断路（该线圈的正常阻值为  $20\Omega$  左右），然后检测磁头上的连线是否断开。每个盘面的两侧均有一个磁头，每个磁头均有两根连线接到磁头机械臂的集成芯片上。该芯片常见的型号为 H1710Q，作用是将磁信号转换为电信号，再送到电路控制板进行处理。磁头阻值应为  $23\sim 26\Omega$ 。若磁头阻值较大，说明磁头损坏。磁头连线与 H1710Q 芯片相连，H1710Q 芯片对应脚阻值应在  $1.7k\Omega$  左右，若在  $1.2k\Omega$  以下说明该芯片已被击穿，可与排线一起更换。

若磁头上的连线断路，可用直径  $0.2mm$  的优质漆包线替代。一端压在磁头的金属弹片上，另一端焊在 H1710Q 相应的脚上。将漆包线卡在机械臂相应的卡槽内，并用少许 502 胶水固定，防止硬盘转动时与漆包线相摩擦。将硬盘各部分复原后，用 702 硅胶将硬盘周围封死，防止灰尘进入。由于磁头体积很小，不易将漆包线卡在上面，最好在放大镜下操作。这时千万不可用力过猛，否则会造成磁头损坏，一定要小心加小心。经这样修复开机后硬盘可恢复正常。

### 3. 线路缺陷

对于线路缺陷，一般要求维修人员了解电子线路知识，要有测试线路的经验和焊接芯片的设备，当然还要有必需的配件以备更换。目前许多专业维修硬盘的公司都有条件解决这类缺陷。对普通用户而言，最简单的判别和解决办法是找一个相同的正常线路板换上试试。

### 4. 系统信息错乱

对于系统信息错乱，需要用专业的工具软件才能解决。首先，要找一块与待修硬盘参数完全相同的正常硬盘，读出其内部所有模块并保存下来。然后，检查待修硬盘的系统结构，查出出错的模块，将正常模块的参数重新写入。用这个方法成功修复的硬盘，一般不会破坏原有数据。要想写某系列硬盘的系统信息，相应的工具软件必须有严格针对性，硬盘的 CPU 专用指令集、硬盘的 Firmware 结构、内部管理程序和参数模块结构等都必须一致。一般只有硬盘厂商才能编写这样的专业工具软件，而且将其视为绝密技术，不向外界提供。但也有一些专业的硬盘研究机构开发了类似的工具软件，一般要价很高，而且很难买到。

### 5. 伺服缺陷

对于伺服缺陷，也要借助专业工具修复。相应的专业工具可以通过重写来纠正伺服信息，解决部分磁道伺服缺陷。如果部分缺陷无法纠正，则要对盘片进行物理磁道扫描，找出有伺服缺陷的磁道，并将其添加到 P-List（或另外的专门磁道缺陷列表）中。然后，运行硬盘内部的低级格式化程序。这段程序能根据需要调用相关的参数模块，自动完成硬盘的低格过程，不需要 PC 系统的干预。

### 6. 扇区缺陷

坏扇区是最常见的缺陷类型，下面着重论述。

按“三包法”规定，如果硬盘在质保期内出现缺陷，商家应该为用户更换或修理。现在大容量的硬盘出现坏扇区的概率实在很高，如果全部送修的话，硬盘商家就要为售后服务忙碌不已了。很多硬盘商家都说，硬盘出现少量坏扇区往往是病毒作怪或某些软件造成的，不是真正的坏扇区，只要运行硬盘厂商提供的某些软件就可以纠正。到底是怎么回事呢？从面对坏扇

区的说明来看，坏扇区有多种可能的原因，修复的方法有以下几种。

- ▶ 通过重写校验码、标志信息等可以纠正一部分坏扇区。现在硬盘厂商都公开提供一些基本的硬盘维护工具，如各种版本的 DM、POWERMAX、DLGDIAG 等，其中都包括“Zero Fill”（零填充）或“Low Level Format”（低级格式化）功能。这两项功能会将硬盘的数据清零，并重写每个扇区的校验码和标志信息。如果不是磁盘表面介质损伤的话，大部分的坏扇区可以纠正为正常状态。这就是我们常听说的“逻辑坏扇区可以修复”的道理。
- ▶ 调用自动修复机制替换坏扇区。为减少硬盘返修率，硬盘厂商在硬盘内部设计了一个自动修复机制（Automatic Reallocation 或 Automatic Reassign）。现在生产的硬盘都有这样的功能：在对硬盘的读写过程中，如果发现一个坏扇区，则由内部管理程序自动分配一个备用扇区来替换该扇区，并将该扇区物理位置及其替换情况记录在 G-List（Grown Defects List，增长缺陷表）中。这样一来，少量的坏扇区就在使用过程中被自动替换了，对用户的使用没有太大的影响。也有一些硬盘自动修复机制的激发条件要严格一些，需要运行某些软件来检测坏扇区，并发出相应指令激发自动修复功能。例如，常用的 Lformat（低格）、DM 中的 Zerofill、Norton 中的 Wipeinfo 和校正工具、Western Digital 工具包中的 WDdiag、IBM 的 DFT 中的 Erase，这些工具之所以能在运行过后消除一些“坏道”，很重要的原因是 Automatic Reallocation（当然还有其他原因）的作用，而不能简单地认为这些“坏道”是“逻辑坏道”或“假坏道”。还有一些半专业工具，如 HDD Speed、MHDD、HDDL、HDD Utility 等，它们之所以能在运行过后消除一些坏扇区，很重要的原因就是这些工具可以在检测到坏扇区时激发自动修复机制。如果读者能查看 G-List 就会知道，这些修复工具运行前后，G-List 中的记录有可能增加。例如，用 HDD Speed 可以查看所有 Quantum Fireball 系列硬盘的 P-List 和 G-List，用 MHDD 可以查看 IBM 和 Fujitsu 硬盘的 P-List 和 G-List。当然，G-List 的记录不会无限制增加，所有硬盘的 G-List 都会限定一个数量范围。例如，Quantum 火球系列是 500 条，Maxtor 美钻二代是 636 条，Western Digital BB 系列是 508 条。超过限度，自动修复机制就不再起作用。这就是少量的坏扇区可以通过上述工具修复，而大量坏扇区就不能通过这些工具修复的原因。
- ▶ 用专业软件将缺陷扇区记录在 P-List 中，并进行内部低级格式化。用户在使用硬盘时，是不能按物理地址模式来访问硬盘的，而是按逻辑地址模式来访问。硬盘在通电自检时，会从保留区读取一些特定参数（与内部低级格式化时调用的参数有密切关系）存在缓冲区内，作为物理地址与逻辑地址之间转换的依据。有些专业软件可以将检测到的坏扇区的逻辑地址转换为对应的物理地址，直接记录在 P-List 中，然后调用内部低级格式化程序进行低级格式化。这样可以不受 G-List 的限制，修复大量坏扇区，达到厂商修复的效果。

“坏道”（Bad Track）这个概念源于多年前小容量硬盘（如 ST506 接口、100MB 以下的硬盘）。当时的硬盘内部没有系统保留区，也就没有 P-List 或 G-List。出厂前，厂商扫描硬盘中存在坏扇区的磁道，并将其位置记录在一张表格中，贴在硬盘外壳上，注明“Bad Track List”，即常说的“坏道表”。坏道表上列出某磁头某柱面的磁道是坏磁道，这就是我们常听人说的“坏道”。当时，所有的硬盘在第一次使用前都要求做低级格式化（Low Level Format，简称“低格”），在使用过程中也可以根据需要做低级格式化。在对硬盘进行低级格式化前（如用 ADM、低版本 DM、早期主板中自带的低格工具等），要将坏道表中的记录全都填入，或用工具自动扫描所有坏道。低格过程中，低格程序对所有磁道按一定的规律进行编号，同时将前面记录或扫描到

的坏道排除在外，即“跳过”（Skipped）那些位置，这对用户来说算是“修好”了“坏道”。而如果哪个用户轻易对硬盘进行低格，却没有登记坏道，那么低格会令以前曾“跳过”的坏道重新显现，这就是当时人们常说“低格会令硬盘增加坏道”的原因。

那么，现在为什么不用“坏道”的概念，而用“缺陷”的概念呢？以前的硬盘，通过低格来修复，只要某磁道中出现一个坏扇区，该磁道就算“坏磁道”（Bad Track），修复时将整个磁道所有扇区一起“跳过”。所以，坏磁道和坏扇区没有区别开来，一起称作“坏道”还算贴切。而现在的硬盘，每个磁道划分为数百上千个扇区，不能因为有一个坏扇区就丢掉整个磁道。而且，有些硬盘在出厂前 P-List 中就记录数千个坏扇区，如果丢掉数千个磁道（意味着要丢掉数 GB 的空间）就太浪费了。现在的硬盘，不同的缺陷有不同的表现，不同的原因修复方法也各不相同。如果继续用“坏磁道”或“坏道”来概括多种缺陷，明显词不达意。