## 31.4 生产者/消费者（有界缓冲区）问题

本章的下一个问题是生产者/消费者（producer/consumer）问题，有时称为有界缓冲区问题[D72]。第 30 章讲条件变量时已经详细描述了这一问题，细节请参考相应内容。

### 第一次尝试

第一次尝试解决该问题时，我们用两个信号量 empty 和 full 分别表示缓冲区空或者满。图 31.5 是 put()和 get()函数，图 31.6 是我们尝试解决生产者/消费者问题的代码。

```
1    int buffer[MAX];
2    int fill = 0;
3    int use  = 0;
4
5    void put(int value) {
6        buffer[fill] = value;    // line f1
7        fill = (fill + 1) % MAX; // line f2
8    }
9
10   int get() {
11       int tmp = buffer[use];    // line g1
12       use = (use + 1) % MAX;    // line g2
13       return tmp;
14   }
```

图 31.5 put()和 get()函数

```
1    sem_t empty;
2    sem_t full;
3
4    void *producer(void *arg) {
5        int i;
6        for (i = 0; i < loops; i++) {
7            sem_wait(&empty);           // line P1
8            put(i);                     // line P2
9            sem_post(&full);            // line P3
10       }
11   }
12
13   void *consumer(void *arg) {
14       int i, tmp = 0;
15       while (tmp != -1) {
16           sem_wait(&full);            // line C1
17           tmp = get();                // line C2
18           sem_post(&empty);           // line C3
19           printf("%d\n", tmp);
20       }
```

```
21  }
22
23  int main(int argc, char *argv[]) {
24      // ...
25      sem_init(&empty, 0, MAX); // MAX buffers are empty to begin with...
26      sem_init(&full, 0, 0);    // ... and 0 are full
27      // ...
28  }
```

图 31.6 增加 full 和 empty 条件

本例中，生产者等待缓冲区为空，然后加入数据。类似地，消费者等待缓冲区变成有数据的状态，然后取走数据。我们先假设 MAX=1（数组中只有一个缓冲区），验证程序是否有效。

假设有两个线程，一个生产者和一个消费者。我们来看在一个 CPU 上的具体场景。消费者先运行，执行到 C1 行，调用 sem_wait(&full)。因为 full 初始值为 0，wait 调用会将 full 减为−1，导致消费者睡眠，等待另一个线程调用 sem_post(&full)，符合预期。

假设生产者然后运行。执行到 P1 行，调用 sem_wait(&empty)。不像消费者，生产者将继续执行，因为 empty 被初始化为 MAX（在这里是 1）。因此，empty 被减为 0，生产者向缓冲区中加入数据，然后执行 P3 行，调用 sem_post(&full)，把 full 从−1 变成 0，唤醒消费者（即将它从阻塞变成就续）。

在这种情况下，可能会有两种情况。如果生产者继续执行，再次循环到 P1 行，由于 empty 值为 0，它会阻塞。如果生产者被中断，而消费者开始执行，调用 sem_wait(&full)（c1 行），发现缓冲区确实满了，消费它。这两种情况都是符合预期的。

你可以用更多的线程来尝试这个例子（即多个生产者和多个消费者）。它应该仍然正常运行。

我们现在假设 MAX 大于 1（比如 MAX=10）。对于这个例子，假定有多个生产者，多个消费者。现在就有问题了：竞态条件。你能够发现是哪里产生的吗？（花点时间找一下）如果没有发现，不妨仔细观察 put()和 get()的代码。

好，我们来理解该问题。假设两个生产者（Pa 和 Pb）几乎同时调用 put()。当 Pa 先运行，在 f1 行先加入第一条数据（fill=0），假设 Pa 在将 fill 计数器更新为 1 之前被中断，Pb 开始运行，也在 f1 行给缓冲区的 0 位置加入一条数据，这意味着那里的老数据被覆盖！这可不行，我们不能让生产者的数据丢失。

## 解决方案：增加互斥

你可以看到，这里忘了互斥。向缓冲区加入元素和增加缓冲区的索引是临界区，需要小心保护起来。所以，我们使用二值信号量来增加锁。图 31.7 是对应的代码。

```
1   sem_t empty;
2   sem_t full;
3   sem_t mutex;
4
5   void *producer(void *arg) {
6       int i;
```

```
7       for (i = 0; i < loops; i++) {
8           sem_wait(&mutex);           // line p0 (NEW LINE)
9           sem_wait(&empty);           // line p1
10          put(i);                     // line p2
11          sem_post(&full);            // line p3
12          sem_post(&mutex);           // line p4 (NEW LINE)
13      }
14  }
15
16  void *consumer(void *arg) {
17      int i;
18      for (i = 0; i < loops; i++) {
19          sem_wait(&mutex);           // line c0 (NEW LINE)
20          sem_wait(&full);            // line c1
21          int tmp = get();            // line c2
22          sem_post(&empty);           // line c3
23          sem_post(&mutex);           // line c4 (NEW LINE)
24          printf("%d\n", tmp);
25      }
26  }
27
28  int main(int argc, char *argv[]) {
29      // ...
30      sem_init(&empty, 0, MAX); // MAX buffers are empty to begin with...
31      sem_init(&full, 0, 0);    // ... and 0 are full
32      sem_init(&mutex, 0, 1);    // mutex=1 because it is a lock (NEW LINE)
33      // ...
34  }
```

图 31.7 增加互斥量（不正确的）

现在我们给整个 put()/get()部分都增加了锁，注释中有 NEW LINE 的几行就是。这似乎是正确的思路，但仍然有问题。为什么？死锁。为什么会发生死锁？考虑一下，尝试找出一个死锁的场景。必须以怎样的步骤执行，会导致程序死锁？

## 避免死锁

好，既然你想出来了，下面是答案。假设有两个线程，一个生产者和一个消费者。消费者首先运行，获得锁（c0 行），然后对 full 信号量执行 sem_wait() （c1 行）。因为还没有数据，所以消费者阻塞，让出 CPU。但是，重要的是，此时消费者仍然持有锁。

然后生产者运行。假如生产者能够运行，它就能生产数据并唤醒消费者线程。遗憾的是，它首先对二值互斥信号量调用 sem_wait()（p0 行）。锁已经被持有，因此生产者也被卡住。

这里出现了一个循环等待。消费者持有互斥量，等待在 full 信号量上。生产者可以发送 full 信号，却在等待互斥量。因此，生产者和消费者互相等待对方——典型的死锁。

## 最后，可行的方案

要解决这个问题，只需减少锁的作用域。图 31.8 是最终的可行方案。可以看到，我们

把获取和释放互斥量的操作调整为紧挨着临界区，把 full、empty 的唤醒和等待操作调整到锁外面。结果得到了简单而有效的有界缓冲区，多线程程序的常用模式。现在理解，将来使用。未来的岁月中，你会感谢我们的。至少在期末考试遇到这个问题时，你会感谢我们。

```
1   sem_t empty;
2   sem_t full;
3   sem_t mutex;
4
5   void *producer(void *arg) {
6       int i;
7       for (i = 0; i < loops; i++) {
8           sem_wait(&empty);           // line p1
9           sem_wait(&mutex);           // line p1.5 (MOVED MUTEX HERE...)
10          put(i);                     // line p2
11          sem_post(&mutex);           // line p2.5 (... AND HERE)
12          sem_post(&full);            // line p3
13      }
14  }
15
16  void *consumer(void *arg) {
17      int i;
18      for (i = 0; i < loops; i++) {
19          sem_wait(&full);            // line c1
20          sem_wait(&mutex);           // line c1.5 (MOVED MUTEX HERE...)
21          int tmp = get();            // line c2
22          sem_post(&mutex);           // line c2.5 (... AND HERE)
23          sem_post(&empty);           // line c3
24          printf("%d\n", tmp);
25      }
26  }
27
28  int main(int argc, char *argv[]) {
29      // ...
30      sem_init(&empty, 0, MAX);  // MAX buffers are empty to begin with...
31      sem_init(&full, 0, 0);     // ... and 0 are full
32      sem_init(&mutex, 0, 1);    // mutex=1 because it is a lock
33      // ...
34  }
```

图 31.8 增加互斥量（正确的）

## 31.5 读者—写者锁

另一个经典问题源于对更加灵活的锁定原语的渴望，它承认不同的数据结构访问可能需要不同类型的锁。例如，一个并发链表有很多插入和查找操作。插入操作会修改链表的状态（因此传统的临界区有用），而查找操作只是读取该结构，只要没有进行插入操作，我们可以并发的执行多个查找操作。读者—写者锁（reader-writer lock）就是用来完成这种操

作的[CHP71]。图 31.9 是这种锁的代码。

代码很简单。如果某个线程要更新数据结构，需要调用 rwlock_acquire_lock()获得写锁，调用 rwlock_release_writelock()释放锁。内部通过一个 writelock 的信号量保证只有一个写者能获得锁进入临界区，从而更新数据结构。

```
1   typedef struct _rwlock_t {
2     sem_t lock;      // binary semaphore (basic lock)
3     sem_t writelock; // used to allow ONE writer or MANY readers
4     int    readers;  // count of readers reading in critical section
5   } rwlock_t;
6
7   void rwlock_init(rwlock_t *rw) {
8     rw->readers = 0;
9     sem_init(&rw->lock, 0, 1);
10    sem_init(&rw->writelock, 0, 1);
11  }
12
13  void rwlock_acquire_readlock(rwlock_t *rw) {
14    sem_wait(&rw->lock);
15    rw->readers++;
16    if (rw->readers == 1)
17      sem_wait(&rw->writelock); // first reader acquires writelock
18    sem_post(&rw->lock);
19  }
20
21  void rwlock_release_readlock(rwlock_t *rw) {
22    sem_wait(&rw->lock);
23    rw->readers--;
24    if (rw->readers == 0)
25      sem_post(&rw->writelock); // last reader releases writelock
26    sem_post(&rw->lock);
27  }
28
29  void rwlock_acquire_writelock(rwlock_t *rw) {
30    sem_wait(&rw->writelock);
31  }
32
33  void rwlock_release_writelock(rwlock_t *rw) {
34    sem_post(&rw->writelock);
35  }
```

图 31.9 一个简单的读者-写者锁

读锁的获取和释放操作更加吸引人。获取读锁时，读者首先要获取 lock，然后增加 reader 变量，追踪目前有多少个读者在访问该数据结构。重要的步骤然后在 rwlock_acquire_readlock()内发生，当第一个读者获取该锁时。在这种情况下，读者也会获取写锁，即在 writelock 信号量上调用 sem_wait()，最后调用 sem_post()释放 lock。

一旦一个读者获得了读锁，其他的读者也可以获取这个读锁。但是，想要获取写锁的线程，就必须等到所有的读者都结束。最后一个退出的写者在“writelock”信号量上调用

sem_post()，从而让等待的写者能够获取该锁。

**提示：简单的笨办法可能更好（Hill 定律）**

我们不能小看一个概念，即简单的笨办法可能最好。某些时候简单的自旋锁反而是最有效的，因为它容易实现而且高效。虽然读者—写者锁听起来很酷，但是却很复杂，复杂可能意味着慢。因此，总是优先尝试简单的笨办法。

这种受简单吸引的思想，在多个地方都能发现。一个早期来源是 Mark Hill 的学位论文[H87]，研究如何为 CPU 设计缓存。Hill 发现简单的直接映射缓存比花哨的集合关联性设计更加有效（一个原因是在缓存中，越简单的设计，越能够更快地查找）。Hill 简洁地总结了他的工作："大而笨更好。"因此我们将这种类似的建议叫作 Hill 定律（Hill's Law）。

这一方案可行（符合预期），但有一些缺陷，尤其是公平性。读者很容易饿死写者。存在复杂一些的解决方案，也许你可以想到更好的实现？提示：有写者等待时，如何能够避免更多的读者进入并持有锁。

最后，应该指出，读者-写者锁还有一些注意点。它们通常加入了更多开锁（尤其是更复杂的实现），因此和其他一些简单快速的锁相比，读者写者锁在性能方面没有优势[CB08]。无论哪种方式，它们都再次展示了如何以有趣、有用的方式来使用信号量。

## 31.6 哲学家就餐问题

哲学家就餐问题（dining philosopher's problem）是一个著名的并发问题，它由 Dijkstra 提出来并解决[DHO71]。这个问题之所以出名，是因为它很有趣，引人入胜，但其实用性却不强。可是，它的名气让我们在这里必须讲。实际上，你可能会在面试中遇到这一问题，假如老师没有提过，导致你们没有通过面试，你们会责怪操作系统老师的。因此，我们这里会讨论这一问题。假如你们因为这个问题得到工作，可以向操作系统老师发感谢信，或者发一些股票期权。

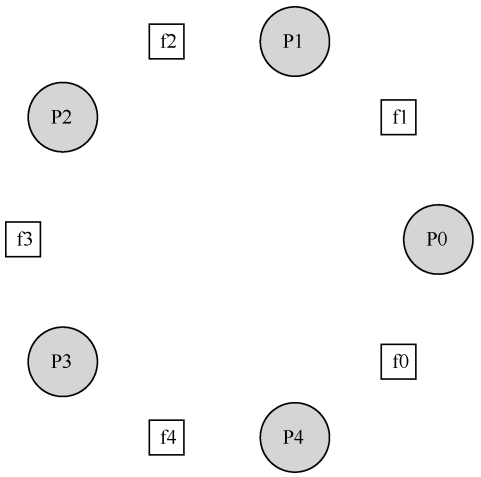

图 31.10 哲学家就餐问题

这个问题的基本情况是（见图 31.10）：假定有 5 位"哲学家"围着一个圆桌。每两位哲学家之间有一把餐叉（一共 5 把）。哲学家有时要思考一会，不需要餐叉；有时又要就餐。而一位哲学家只有同时拿到了左手边和右手边的两把餐叉，才能吃到东西。关于餐叉的竞争以及随之而来的同步问题，就是我们在并发编程中研究它的原因。

下面是每个哲学家的基本循环：

```
while (1) {
  think();
```

```
    getforks();
    eat();
    putforks();
}
```

关键的挑战就是如何实现 getforks()和 putforks()函数，保证没有死锁，没有哲学家饿死，并且并发度更高（尽可能让更多哲学家同时吃东西）。

根据 Downey 的解决方案[D08]，我们会用一些辅助函数，帮助构建解决方案。它们是：

```
int left(int p)  { return p; }
int right(int p) { return (p + 1) % 5; }
```

如果哲学家 p 希望用左手边的叉子，他们就调用 left(p)。类似地，右手边的叉子就用 right(p)。模运算解决了最后一个哲学家（p = 4）右手边叉子的编号问题，就是餐叉 0。

我们需要一些信号量来解决这个问题。假设需要 5 个，每个餐叉一个：sem_t forks[5]。

### 有问题的解决方案

我们开始第一次尝试。假设我们把每个信号量（在 fork 数组中）都用 1 初始化。同时假设每个哲学家知道自己的编号（p）。我们可以写出 getforks()和 putforks()函数，如图 31.11 所示。

```
1    void getforks() {
2      sem_wait(forks[left(p)]);
3      sem_wait(forks[right(p)]);
4    }
5
6    void putforks() {
7      sem_post(forks[left(p)]);
8      sem_post(forks[right(p)]);
9  }
```

图 31.11 getforks()和 putforks()函数

这个（有问题的）解决方案背后的思路如下。为了拿到餐叉，我们依次获取每把餐叉的锁——先是左手边的，然后是右手边的。结束就餐时，释放掉锁。很简单，不是吗？但是，在这个例子中，简单是有问题的。你能看到问题吗？想一想。

问题是死锁（deadlock）。假设每个哲学家都拿到了左手边的餐叉，他们每个都会阻塞住，并且一直等待另一个餐叉。具体来说，哲学家 0 拿到了餐叉 0，哲学家 1 拿到了餐叉 1，哲学家 2 拿到餐叉 2，哲学家 3 拿到餐叉 3，哲学家 4 拿到餐叉 4。所有的餐叉都被占有了，所有的哲学家都阻塞着，并且等待另一个哲学家占有的餐叉。我们在后续章节会深入学习死锁，这里只要知道这个方案行不通就可以了。

### 一种方案：破除依赖

解决上述问题最简单的方法，就是修改某个或者某些哲学家的取餐叉顺序。事实上，Dijkstra 自己也是这样解决的。具体来说，假定哲学家 4（编写最大的一个）取餐叉的顺序

不同。相应的代码如下：

```
1    void getforks() {
2      if (p == 4) {
3        sem_wait(forks[right(p)]);
4        sem_wait(forks[left(p)]);
5      } else {
6        sem_wait(forks[left(p)]);
7        sem_wait(forks[right(p)]);
8      }
9    }
```

因为最后一个哲学家会尝试先拿右手边的餐叉，然后拿左手边，所以不会出现每个哲学家都拿着一个餐叉，卡住等待另一个的情况，等待循环被打破了。想想这个方案的后果，让你自己相信它有效。

还有其他一些类似的“著名”问题，比如吸烟者问题（cigarette smoker’s problem），理发师问题（sleeping barber problem）。大多数问题只是让我们去理解并发，某些问题的名字很吸引人。感兴趣的读者可以去查阅相关资料，或者通过一些更实际的思考去理解并发行为[D08]。

## 31.7 如何实现信号量

最后，我们用底层的同步原语（锁和条件变量），来实现自己的信号量，名字叫作Zemaphore。这个任务相当简单，如图 31.12 所示。

```
1    typedef struct   _Zem_t {
2        int value;
3        pthread_cond_t cond;
4        pthread_mutex_t lock;
5    } Zem_t;
6
7    // only one thread can call this
8    void Zem_init(Zem_t *s, int value) {
9        s->value = value;
10       Cond_init(&s->cond);
11       Mutex_init(&s->lock);
12   }
13
14   void Zem_wait(Zem_t *s) {
15       Mutex_lock(&s->lock);
16       while (s->value <= 0)
17           Cond_wait(&s->cond, &s->lock);
18       s->value--;
19       Mutex_unlock(&s->lock);
20   }
21
22   void Zem_post(Zem_t *s) {
```

```
23        Mutex_lock(&s->lock);
24        s->value++;
25        Cond_signal(&s->cond);
26        Mutex_unlock(&s->lock);
27    }
```

图 31.12 用锁和条件变量实现 Zemahpore

可以看到，我们只用了一把锁、一个条件变量和一个状态的变量来记录信号量的值。请自己研究这些代码，直到真正理解它。去做吧！

我们实现的 Zemaphore 和 Dijkstra 定义的信号量有一点细微区别，就是我们没有保持当信号量的值为负数时，让它反映出等待的线程数。事实上，该值永远不会小于 0。这一行为更容易实现，并符合现有的 Linux 实现。

**提示：小心泛化**

在系统设计中，泛化的抽象技术是很有用处的。一个好的想法稍微扩展之后，就可以解决更大一类问题。然而，泛化时要小心，正如 Lampson 提醒我们的“不要泛化。泛化通常都是错的。”[L83]

我们可以把信号量当作锁和条件变量的泛化。但这种泛化有必要吗？考虑基于信号量去实现条件变量的难度，可能这种泛化并没有你想的那么通用。

很奇怪，利用信号量来实现锁和条件变量，是棘手得多的问题。某些富有经验的并发程序员曾经在 Windows 环境下尝试过，随之而来的是很多缺陷[B04]。你自己试一下，看看是否能明白为什么使用信号量实现条件变量比看起来更困难。

## 31.8 小结

信号量是编写并发程序的强大而灵活的原语。有程序员会因为简单实用，只用信号量，不用锁和条件变量。

本章展示了几个经典问题和解决方案。如果你有兴趣了解更多，有许多资料可以参考。Allen Downey 关于并发和使用信号量编程的书[D08]就很好（免费的参考资料）。该书包括了许多谜题，你可以研究它们，从而深入理解具体的信号量和一般的并发。成为一个并发专家需要多年的努力，学习本课程之外的内容，无疑是掌握这个领域的关键。

## 参考资料

[B04]“Implementing Condition Variables with Semaphores”Andrew Birrell

December 2004

一本关于在信号量上实现条件变量有多困难，以及作者和同事在此过程中犯的错误的有趣读物。因为该小组进行了大量的并发编程，所以讲述特别中肯。例如，Birrell 以编写各种线程编程指南而闻名。

[CB08]“Real-world Concurrency”Bryan Cantrill and Jeff Bonwick
ACM Queue. Volume 6, No. 5. September 2008
一篇很好的文章，来自一家以前名为 Sun 的公司的一些内核黑客，讨论了并发代码中面临的实际问题。

[CHP71]“Concurrent Control with Readers and Writers”
P.J. Courtois, F. Heymans, D.L. Parnas Communications of the ACM, 14:10, October 1971
读者—写者问题的介绍以及一个简单的解决方案。后来的工作引入了更复杂的解决方案，这里跳过了，因为它们非常复杂。

[D59]“A Note on Two Problems in Connexion with Graphs”
E. W. Dijkstra
Numerische Mathematik 1, 269271, 1959
你能相信人们在 1959 年从事算法工作吗？我们很难相信。即使在计算机用起来有趣之前，这些人都感觉到他们会改变世界……

[D68a]“Go-to Statement Considered Harmful”
E.W. Dijkstra
Communications of the ACM, volume 11(3): pages 147148, March 1968
有时被认为是软件工程领域的开始。

[D68b]“The Structure of the THE Multiprogramming System”
E.W. Dijkstra
Communications of the ACM, volume 11(5), pages 341346, 1968
最早的论文之一，指出计算机科学中的系统工作是一项引人入胜的智力活动，也为分层系统式的模块化进行了强烈辩护。

[D72]“Information Streams Sharing a Finite Buffer”
E.W. Dijkstra
Information Processing Letters 1: 179180, 1972
Dijkstra 创造了一切吗？不，但可能差不多。他当然是第一位明确写下并发代码中的问题的人。然而，操作系统设计的从业者确实知道 Dijkstra 所描述的许多问题，所以将太多东西归功于他也许是对历史的误传。

[D08]“The Little Book of Semaphores”
A.B. Downey
一本关于信号量的好书（而且免费!）。如果你喜欢这样的事情，有很多有趣的问题等待解决。

[DHO71]“Hierarchical ordering of sequential processes”
E.W. Dijkstra
介绍了许多并发问题，包括哲学家就餐问题。关于这个问题，维基百科也给出了很丰富的内容。

[GR92]“Transaction Processing: Concepts and Techniques”Jim Gray and Andreas Reuter
Morgan Kaufmann, September 1992

我们发现特别幽默的引用就在第 485 页，第 8.8 节开始处：“第一个多处理器，大约在 1960 年，就有测试并设置指令……大概是 OS 的实现者想出了正确的算法，尽管通常认为 Dijkstra 在多年后发明信号量。”

[H87]“Aspects of Cache Memory and Instruction Buffer Performance”Mark D. Hill
Ph.D. Dissertation, U.C. Berkeley, 1987
Hill 的学位论文工作，给那些痴迷于早期系统缓存的人。量化论文的一个很好的例子。

[L83]“Hints for Computer Systems Design”Butler Lampson
ACM Operating Systems Review, 15:5, October 1983
著名系统研究员 Lampson 喜欢在设计计算机系统时使用暗示。暗示经常是正确的，但可能是错误的。在这种用法中，signal()告诉等待线程它改变了等待的条件，但不要相信当等待线程唤醒时条件将处于期望的状态。在这篇关于系统设计的暗示的文章中， Lampson 的一般暗示是你应该使用暗示。这并不像听上去那么令人困惑。

# 第 32 章　常见并发问题

多年来，研究人员花了大量的时间和精力研究并发编程的缺陷。很多早期的工作是关于死锁的，之前的章节也有提及，本章会深入学习[C+71]。最近的研究集中在一些其他类型的常见并发缺陷（即非死锁缺陷）。在本章中，我们会简要了解一些并发问题的例子，以便更好地理解要注意什么问题。因此，本章的关键问题就是：

**关键问题：如何处理常见的并发缺陷**

并发缺陷会有很多常见的模式。了解这些模式是写出健壮、正确程序的第一步。

## 32.1　有哪些类型的缺陷

第一个最明显的问题就是：在复杂并发程序中，有哪些类型的缺陷呢？一般来说，这个问题很难回答，好在其他人已经做过相关的工作。具体来说，Lu 等人[L+08]详细分析了一些流行的并发应用，以理解实践中有哪些类型的缺陷。

研究集中在 4 个重要的开源应用：MySQL（流行的数据库管理系统）、Apache（著名的 Web 服务器）、Mozilla（著名的 Web 浏览器）和 OpenOffice（微软办公套件的开源版本）。研究人员通过检查这几个代码库已修复的并发缺陷，将开发者的工作变成量化的缺陷分析。理解这些结果，有助于我们了解在成熟的代码库中，实际出现过哪些类型的并发问题。

表 32.1 是 Lu 及其同事的研究结论。可以看出，共有 105 个缺陷，其中大多数是非死锁相关的（74 个），剩余 31 个是死锁缺陷。另外，可以看出每个应用的缺陷数目，OpenOffice 只有 8 个，而 Mozilla 有接近 60 个。

**表 32.1　现代应用程序的缺陷统计**

| 应用名称 | 用途 | 非死锁 | 死锁 |
|---|---|---|---|
| MySQL | 数据库服务 | 14 | 9 |
| Apache | Web 服务器 | 13 | 4 |
| Mozilla | Web 浏览器 | 41 | 16 |
| OpenOffice | 办公套件 | 6 | 2 |
| 总计 | | 74 | 31 |

我们现在来深入分析这两种类型的缺陷。对于第一类非死锁的缺陷，我们通过该研究的例子来讨论。对于第二类死锁缺陷，我们讨论人们在阻止、避免和处理死锁上完成的大量工作。

## 32.2 非死锁缺陷

Lu 的研究表明，非死锁问题占了并发问题的大多数。它们是怎么发生的？我们如何修复？我们现在主要讨论其中两种：违反原子性（atomicity violation）缺陷和错误顺序（order violation）缺陷。

### 违反原子性缺陷

第一种类型的问题叫作违反原子性。这是一个 MySQL 中出现的例子。读者可以先自行找出其中问题所在。

```
1    Thread 1::
2    if (thd->proc_info) {
3      ...
4      fputs(thd->proc_info, ...);
5      ...
6    }
7
8    Thread 2::
9    thd->proc_info = NULL;
```

这个例子中，两个线程都要访问 thd 结构中的成员 proc_info。第一个线程检查 proc_info 非空，然后打印出值；第二个线程设置其为空。显然，当第一个线程检查之后，在 fputs()调用之前被中断，第二个线程把指针置为空；当第一个线程恢复执行时，由于引用空指针，导致程序奔溃。

根据 Lu 等人，更正式的违反原子性的定义是：“违反了多次内存访问中预期的可串行性（即代码段本意是原子的，但在执行中并没有强制实现原子性）”。在我们的例子中，proc_info 的非空检查和 fputs()调用打印 proc_info 是假设原子的，当假设不成立时，代码就出问题了。

这种问题的修复通常（但不总是）很简单。你能想到如何修复吗？

在这个方案中，我们只要给共享变量的访问加锁，确保每个线程访问 proc_info 字段时，都持有锁（proc_info_lock）。当然，访问这个结构的所有其他代码，也应该先获取锁。

```
1    pthread_mutex_t proc_info_lock = PTHREAD_MUTEX_INITIALIZER;
2
3    Thread 1::
4    pthread_mutex_lock(&proc_info_lock);
5    if (thd->proc_info) {
6      ...
7      fputs(thd->proc_info, ...);
8      ...
9    }
10    pthread_mutex_unlock(&proc_info_lock);
```

```
11
12   Thread 2::
13   pthread_mutex_lock(&proc_info_lock);
14   thd->proc_info = NULL;
15   pthread_mutex_unlock(&proc_info_lock);
```

### 违反顺序缺陷

Lu 等人提出的另一种常见的非死锁问题叫作违反顺序（order violation）。下面是一个简单的例子。同样，看看你是否能找出为什么下面的代码有缺陷。

```
1    Thread 1::
2    void init() {
3        ...
4        mThread = PR_CreateThread(mMain, ...);
5        ...
6    }
7
8    Thread 2::
9    void mMain(...) {
10       ...
11       mState = mThread->State;
12       ...
13   }
```

你可能已经发现，线程 2 的代码中似乎假定变量 mThread 已经被初始化了（不为空）。然而，如果线程 1 并没有首先执行，线程 2 就可能因为引用空指针奔溃（假设 mThread 初始值为空；否则，可能会产生更加奇怪的问题，因为线程 2 中会读到任意的内存位置并引用）。

违反顺序更正式的定义是：“两个内存访问的预期顺序被打破了（即 A 应该在 B 之前执行，但是实际运行中却不是这个顺序）”[L+08]。

我们通过强制顺序来修复这种缺陷。正如之前详细讨论的，条件变量（condition variables）就是一种简单可靠的方式，在现代代码集中加入这种同步。在上面的例子中，我们可以把代码修改成这样：

```
1    pthread_mutex_t mtLock = PTHREAD_MUTEX_INITIALIZER;
2    pthread_cond_t  mtCond = PTHREAD_COND_INITIALIZER;
3    int mtInit             = 0;
4
5    Thread 1::
6    void init() {
7        ...
8        mThread = PR_CreateThread(mMain, ...);
9
10       // signal that the thread has been created...
11       pthread_mutex_lock(&mtLock);
12       mtInit = 1;
13       pthread_cond_signal(&mtCond);
```

```
14      pthread_mutex_unlock(&mtLock);
15      ...
16  }
17
18  Thread 2::
19  void mMain(...) {
20      ...
21      // wait for the thread to be initialized...
22      pthread_mutex_lock(&mtLock);
23      while (mtInit == 0)
24          pthread_cond_wait(&mtCond,  &mtLock);
25      pthread_mutex_unlock(&mtLock);
26
27      mState = mThread->State;
28      ...
29  }
```

在这段修复的代码中，我们增加了一个锁（mtLock）、一个条件变量（mtCond）以及状态的变量（mtInit）。初始化代码运行时，会将 mtInit 设置为 1，并发出信号表明它已做了这件事。如果线程 2 先运行，就会一直等待信号和对应的状态变化；如果后运行，线程 2 会检查是否初始化（即 mtInit 被设置为 1），然后正常运行。请注意，我们可以用 mThread 本身作为状态变量，但为了简洁，我们没有这样做。当线程之间的顺序很重要时，条件变量（或信号量）能够解决问题。

### 非死锁缺陷：小结

Lu 等人的研究中，大部分（97%）的非死锁问题是违反原子性和违反顺序这两种。因此，程序员仔细研究这些错误模式，应该能够更好地避免它们。此外，随着更自动化的代码检查工具的发展，它们也应该关注这两种错误，因为开发中发现的非死锁问题大部分都是这两种。

然而，并不是所有的缺陷都像我们举的例子一样，这么容易修复。有些问题需要对应用程序的更深的了解，以及大量代码及数据结构的调整。阅读 Lu 等人的优秀（可读性强）的论文，了解更多细节。

## 32.3 死锁缺陷

除了上面提到的并发缺陷，死锁（deadlock）是一种在许多复杂并发系统中出现的经典问题。例如，当线程 1 持有锁 L1，正在等待另外一个锁 L2，而线程 2 持有锁 L2，却在等待锁 L1 释放时，死锁就产生了。以下的代码片段就可能出现这种死锁：

```
Thread 1:    Thread 2:
lock(L1);    lock(L2);
lock(L2);    lock(L1);
```