多米诺效应的解决策略研究*

刘云龙 陈俊亮

(北京邮电大学程控交换技术与通信网国家重点实验室 北京 100876)

E-mail: ylliu@technologist.com chjl@bupt.edu.cn

摘要 定义了备查点间隔之间的先于关系,并对分布式系统执行的语义正确性进行了约束,证明了逆时先于现象是产生多米诺效应的本质,提出了多米诺避免、多米诺检测与消除、多米诺容忍三大解决策略.

关键词 分布式系统,容错,备查点与卷回恢复,多米诺效应.

中图法分类号 TP391

在分布式系统中,备查点与卷回恢复CRR(checkpointing and rollback recovery)机制是最常用的一种容错技术.它阶段性地把进程执行的中间状态保存到可靠存储器中,此动作称为备查点操作,被保存的状态称为备查点CP(checkpoint),从而在检测到故障时可以令进程从先前保存的状态上重新执行,此动作被称为卷回,程序从最近的备查点到故障点之间的重复计算被称为恢复.在分布式系统中的卷回恢复中,如何防护多米诺效应[1]是一个极其关键的问题.

现有文献中所提出的备查点机制可归纳为协同算法与独立算法两类.[3~5,7]协同算法要求系统中各进程协同地进行备查点操作,使所建立的全局备查点都能保持一致性,这使出错后的卷回操作较易实现,且不存在多米诺效应;在独立算法中,进程间异步地进行备查点操作,因此,附加时间开销比协同算法小得多,但系统出错后要从各进程的本地备查点中构造出一致性全局备查点,而多米诺效应的防护则不容忽视.本文将以备查点间隔的先于关系对多米诺效应的本质作形式化的分析与描述,并系统地给出其一般的解决方法.

1 理论基础

本文论述针对不存在共享内存或公共时钟的异步消息传递系统,此系统可以被抽象为 n 个有通信关系的并发进程的集合 P 与通信信道的集合 C 所组成的二元对 $\langle P,C\rangle$,进程之间通过对应的信道收发消息进行异步通信.系统中的处理机是"失效-停止"型的[2],拥有一个可靠存储器,消息的传输时延不可预期但为有限,且通信网络不会被隔离.

以 $CP_i^x(0\leqslant i<n,0\leqslant x)$ 表示进程 p_i 保存的第 x 个备查点,其中 n 为系统中的进程数,而进程 P_i 中相临两个备查点 CP_i^x 与 CP_i^{x+1} 之间的备查点间隔记为 CI_i^x.类似于 Lamport 的"Happened-Before"[3],我们定义如下.

定义 1. 对于分布式系统 $System::=\langle P,C\rangle$ 中的任意两个备查点间隔 CI_i^x 和 CI_j^y,当且仅当

(1) $(i=j)\wedge(x<y)$,或者

(2) $i\neq j$,且有一条计算消息 $m_{i,j}$ 由进程 P_i 在 CI_i^x 内发出,由进程 P_j 在 CI_j^y 内接收;或者

(3) $\exists\, CI_k^z,(CI_i^x\prec CI_k^z)\wedge(CI_k^z\prec CI_j^y)$

3 个条件之一成立时,我们称 CI_i^x 先于(Precedes)CI_j^y,记为 $CI_i^x\prec CI_j^y$.

定义 2. 如果一个分布式系统的某次执行服从以下约束条件:

(1) 同一进程上的所有动作(如状态转移)按时间先后能够被完全排序;

(2) 在任一时刻一条消息的发送动作必须发生在该消息的接收动作之前,

则称这次执行是语义正确的.

定义 3. 对于失效前语义正确的某次分布式系统执行,如果它卷回到某个全局备查点后的执行仍为语义正确,则称此全局备查点为一致性全局备查点.相应地,称本次卷回为一致性全局卷回.

---

* 本文研究得到国家教委博士点专项科研基金资助.作者刘云龙,1972 年生,博士,主要研究领域为智能网络,容错计算,分布式计算.陈俊亮,1933 年生,博士,教授,博导,中国科学院院士,中国工程院院士,主要研究领域为智能通信网,通信软件,容错计算.

本文通讯联系人:刘云龙,北京 100080,海淀南路 30 号航天长城大厦 15 层贝尔实验室

本文 1997-09-24 收到原稿,1997-11-20 收到修改稿

定理 1. 如果有某个备查点间隔被卷回，则为了维护卷回恢复的一致性，此备查点间隔所先于的其他所有备查点间隔均必须被卷回.

证明：由定义 1、定义 2 和定义 3 易证(略).

2 多米诺效应的分析

在本文中，同一进程中，晚发生的备查点间隔"先于"早发生的备查点间隔的异常现象被称为"逆时先于"现象.

定理 2. 多米诺效应本质定理：分布式系统中潜在多米诺效应的充要条件是在其执行过程形成了"逆时先于".

证明：(充分性)若分布式系统的某次执行中存在"逆时先于"现象，那么，当形成此现象的两个备查点间隔中序号较大的一个被卷回时，因为逆时先于现象导致了序号较大的一个先于较小的一个，由定理 1 可知，此时为了维护卷回恢复的一致性，序号较小的也必须被卷回，多米诺效应由此产生.

(必要性)若分布式系统中存在多米诺效应，则意味着某个进程，如 p_i 卷回到某个备查点 CP_i^x 引起语义正确性约束(2)的违背，从而导致另一进程，如 p_j 卷回到某个备查点 CP_j^y 以恢复一致性，由约束条件(2)的含义可知，此时必存在一条消息 $\exists\ m$：$(sending(m)\propto CI_i^x) \wedge (Receiving(m)\propto CI_j^y)$，进而有 $CI_i^x \prec CI_j^y$；p_j 卷回到 CP_j^y 将进一步引起其他进程的卷回，并最终导致 p_i 卷回到某个更前面的备查点 $CI_i^r(0\leqslant r<x)$，此时必存在一条消息链 $\exists\ (m_0, m_1, \ldots, m_k)$：$(sending(m_0)\propto CI_j^y) \wedge (Receiving(m_k)\propto CI_i^r)$，由于关系的传递性有 $CI_j^y \prec CI_i^r$，这样，$(CI_i^x \prec CI_j^y) \wedge (CI_j^y \prec CI_i^r) \Rightarrow (CI_i^x \prec CI_i^r) \wedge (r<x)$，所以存在"逆时先于"现象. □

图 1 给出了一个多米诺效应的例子. 其中由四条消息产生下面两条先于链：$CI_2^2 \prec CI_1^0 \prec CI_0^0 \prec CI_0^1 \prec CI_2^2$ 和 $CI_2^2 \prec CI_1^1 \prec CI_0^1 \prec CI_0^2 \prec CI_2^2$，这两条链均在 CI_2^2 封闭成回路(称为逆时先于回路*)，导致 p_0 和 p_1 中都出现了"逆时先于"：$CI_0^1 \prec CI_0^0$ 和 $CI_1^2 \prec CI_0^2$. 此外，本例还表明多米诺效应并非缘于差错的传播[4]，而是由各进程备查点设置与其通信结构不协调引起"逆时先于"所致.

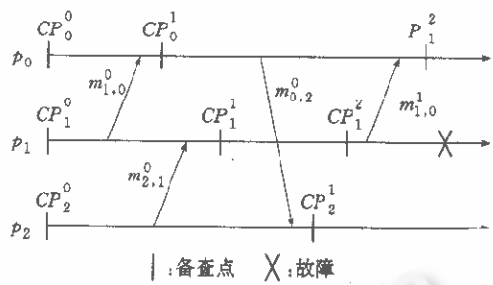

图1　一个多米诺效应敏感度为2的CRR算法

定义 4. 若一个 CRR 算法不会导致多米诺效应，则被称为是多米诺安全的；否则，被称为多米诺危险的.

定义 5. 若一个 CRR 算法无法避免"逆时先于"现象，形式化地

$$\exists\ p_i \in P: (CI_i^t \prec CI_i^r) \wedge (t>r),$$

则被称为是多米诺敏感的；否则，被称为是多米诺迟钝的.

定义 6. 在一个多米诺敏感的 CCR 算法的执行中，若存在某个正整数 $\alpha>0$，使

$$\forall\ p_i \in P: (r<t) \wedge (CI_i^t \prec CI_i^r) \Rightarrow t-r \leqslant \alpha,$$

则此备查点算法就被称为是 α 级多米诺敏感的，而 α 被称为此备查点算法的多米诺敏感度.

定义 7. 在一个多米诺敏感的备查点算法的执行中，如果某个备查点 $CP_i^x(0\leqslant i<n)$ 满足以下条件：

$$\exists\ r<x, \exists\ t\geqslant x: (CI_i^t \prec CI_i^r),$$

那么，此备查点就被称为是无效备查点(Invalid Checkpoint).

3 多米诺效应的解决

满足某种公共约束或具有某种共同特性的一类备查点与通信方式被称为备查点与通信模型 CCM(checkpoint and communication model).[5]这里，我们提出以下 3 种基本策略可以保证备查点算法的安全性：多米诺效应的避免、多米诺效应的检测与消除和多米诺效应的容忍.

3.1 多米诺效应的避免

定理 3. 多米诺效应避免的条件：如果一个备查点与通信模型能够保证所有备查点间隔内消息的接收事件都处在消息的事件之前，那么，此模型必是多米诺迟钝的.

---

* 一个"逆时先于回路"中至少要包含某个进程的两个备查点间隔，否则只构成一个回路，而非逆时先于回路.

证明：由反证法易证(略).

以上条件虽对多米诺效应的避免是充分的，但要求过于严格.如果在计算消息的发送事件之后紧跟有计算消息的接受事件时，那么在接收此消息前必须先插入一个备查点，从而使无错运行的附加时间开销过大，同时，这样插入的备查点不允许随意移动，也给备查点算法的优化带来难度.[6]为了防止多米诺效应的发生而被额外插入的备查点称为临界备查点(Critical-Checkpoints，C-CPs).文献[5]所归纳的6类备查点与通信模型均可作为多米诺避免的实施技术，即NRAS(no-receive-after-send)模型、CAS(checkpointing-after-send)模型、CBR(checkpointing-before-receiving)模型、CASBR(checkpointing-after-send-before-receive)模型、FDAS(fixed-dependency-after-send)模型及FDI(fixed-dependency-interval)模型.

3.2 多米诺效应的检测与消除

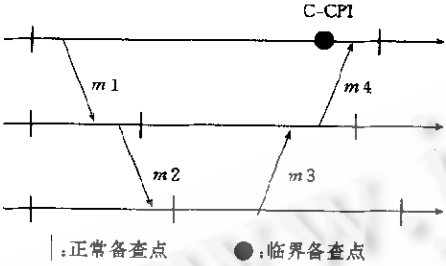

图2 FDAS−模型的实施举例

多米诺效应避免条件的要求存在冗余，多米诺效应的检测与消除策略就是为了减少这种超出必要的冗余而提出的.其主要思想是：当一个进程检测到某个消息的接收事件将导致本进程的当前备查点间隔先于同一进程的某个备查点间隔(包括当前备查点间隔自身)时，就在处理此消息之前先插入一个备查点，以切断"逆时先于"回路，消除多米诺效应的隐患.如果我们对FDAS模型进行如下优化，则可得到多米诺效应的检测与消除模型：FDAS+模型.

FDAS+模型规定任何备查点间隔内，在第1次计算消息的发送事件后、接收到将导致逆时先于回路的计算消息之前，都要先插入一个备查点.如图2所示，只需插入一个临界备查点C-CP1，就足以切断由计算消息$m1$，$m2$，$m3$和$m4$的发送与接收将产生的逆时先于回路.

FDAS+模型中，只有在检测到将出现逆时先于时，才插入一个临界备查点，使临界备查点数目降为最低，进而使为防止多米诺效应而在无错运行时引入的额外开销降为最低.

3.3 多米诺效应的容忍

3.3.1 一次性卷回

有一些算法乐观地把进程失效与多米诺效应同时发生视为小概率事件，因而未采取任何多米诺效应的避免或消除技术，但这种小概率事件一旦发生，将造成大量的时间损耗，一次性卷回技术可作为一种补救措施.如果去除分布式系统执行中的所有无效备查点，那么就可以通过把多米诺敏感度α强置为0来消除可能的连锁卷回.一次性卷回技术对备查点算法的要求较松，但需要在正常运行时或出错后采取适当的措施去除已建立的无效备查点.前者将影响进程无错运行的时间性能，后者将影响恢复操作的时间性能.一次性卷回技术并不能减少多米诺效应所造成的计算损失，但却可以消除因连锁卷回而造成的大量的时间损耗，这一显著特点对于采用上述乐观假设的应用(如大型科学计算)具有现实意义.

3.3.2 消息日志

在独立备查点机制中，为了使全局卷回恢复所损失的计算量降为最低，可采取消息日志机制.[7]在消息日志机制中，进程随机地进行备查点操作，并对所接收到的消息做日志，这样，一个进程就可以失效后卷回到某个备查点，并对那个备查点之后接收到的消息按原顺序进行重演，从而使进程恢复到失效前的任意状态.基于消息日志的恢复策略中不必消除"逆时先于"现象，而是通过对孤儿消息做日志并在恢复过程中进行重演来抑制连锁卷回，从而避免多米诺效应的发生.

4 结束语

本文对多米诺效应的产生机理及解决途径均做了系统的论述，证明了"逆时先于现象是多米诺效应产生的本质"的结论，并给出了必要的形式化描述与分析，然后系统地阐述了多米诺效应的解决策略，提出了多米诺效应的避免、在线检测与消除及在线容忍三大解决策略，为分布式系统的卷回恢复的研究提供了有力的理论与技术支持.

参考文献

1 Randell B. System structure for software fault tolerance. IEEE Transactions on Software Engineering, 1975,1(2):220～232

2 Schlichting R D, Schneider F B. Fail-stop processors: an approach to designing fault-tolerant systems. ACM Transactions on Computing System, 1983,1(3):222～238

3 Lamport L. Time, clocks, and the ordering of events in a distributed systems. Communication of the ACM, 1978,21(7):558～565

4 周笛，王鼎兴. 分布系统中多米诺效应的分析与消除. 计算机学报，1992,15(6):408～416
(Zhou Di, Wang Ding-xing. Analysis and elimination of Domino-effect in distributed systems. Chinese Journal of Computers, 1992,15(6):408～416)

5 Wang Yi-min. Consistent global checkpoints that contain a given set of local checkpoints. IEEE Transactions on Computers, 1997,46(4):456～468

6 Lecuyer P, Malenfant J. Computing optimal checkpointing for rollback and recovery systems. IEEE Transactions on Computers, 1988,37(4):491～496

7 Strom R E, Yemini S. Optimistic recovery in distributed systems. ACM Transactions on Computer System, 1985,3(3):204～226

Study on Resolutions of Domino Effect

LIU Yun-long　CHEN Jun-liang

(National Laboratory of Switching Technology and Telecommunication Networks
Beijing University of Posts and Telecommunications　Beijing　100876)

Abstract　In this paper, the preceding relationship between the checkpointing intervals is defined, and the "reverse-precedence" phenomenon is proved to be the essential cause of Domino effect, and three main resolving strategies for Domino effect are presented which are off-line or on-line Domino avoidance, on-line Domino detection and elimination, and on-line Domino tolerance.

Key words　Distributed system, fault tolerance, checkpointing and rollback recovery, Domino effect