基于最大秩距离码的Stern方案*

杜伟章, 王新梅

(西安电子科技大学 综合业务网国家重点实验室,陕西 西安 710071)

E-mail: duweizhang@yahoo.com.cn

http://www.xidian.edu.cn

摘要: 基于最大秩距离码,提出了一种新的Stern方案,讨论了它的安全性,证明了通过参数的适当选取,此基于最大秩距离码的Stern方案是安全的.

关键词: 秩距离码;纠错码;协议;安全性

中图法分类号: TP309 **文献标识码**: A

文献[1]提出了秩距离码及最大秩距离码的理论.文献[2]基于纠错码提出了一种协议,称为Stern方案.本文基于最大秩距离码提出一种新的Stern方案,由于秩及秩距离的特点,可以证明通过参数的适当选取,此基于最大秩距离码的Stern方案是安全的.

1 有关的定义及定理

令 X^n 表示域 $GF(q^N)$ 上的 n 维向量空间,这里,q 为素数或素数的幂.设 $u_1,u_2,...,u_N$ 是域 $GF(q^N)$ 的基底,则任意元素 $x_i\in GF(q^N)$ 可惟一地表示为

$$x_i=a_{1i}u_1+a_{2i}u_2+...+a_{Ni}u_N.$$

令 $M_{N\times n}(q)$ 表示元素取自域 $GF(q)$ 的所有 $N\times n$ 阶矩阵全体.对任意向量 $x=(x_1,x_2,...,x_n)\in X^n$,指定映射 $A:X^n\to M_{N\times n}(q)$ 如下:

$$A(X)=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{N1} & a_{N2} & \cdots & a_{Nn} \end{bmatrix}.$$

定义1. (1) 矩阵 $A(X)$ 的秩称为 X^n 的元素 X 在 $GF(q)$ 上的秩,表示为 $r(X)$;

(2) 两个元素 $X,Y\in X^n$ 之间的秩距离 $d(X;Y)$ 定义为 $d(X;Y):=r(X-Y)$;

(3) 元素属于 $GF(q^N)$ 的 $r\times n$ 阶矩阵 H 在 $GF(q)$ 上的极大线性无关的列数称为该矩阵在 $GF(q)$ 上的秩,记为 $r(H;q)$;矩阵 H 在 $GF(q_N)$ 上的极大线性无关的列数称为该矩阵在 $GF(q^N)$ 上的秩,记为 $r(H;q^N)$.

(4) X^n 的子集 $C\neq 0$ 称作码长为 n 的码,如果 C 是 X^n 的 k 维线性子空间,则称 C 是 (n,k) 线性码;$d=d_r(C):=\min\limits_{X\neq Y}\{d(X;Y)\mid X,Y\in C\}$ 称为 C 的最小秩距离.

码长为 n,维数为 k,最小秩距离为 d 的线性码称作秩距离 $[n,k,d]$ 码.

引理1. 令 $X=(x_1,x_2,...,x_n)$ 是域 $GF(q^N)$ 上的 n 维向量,λ 是 $GF(q^N)$ 上的非零元素,P 为

* 收稿日期: 2000-03-06; 修改日期: 2000-06-12

基金项目: 高等学校博士学科点专项科研基金资助项目(98070104)

作者简介: 杜伟章(1965-),女,湖南长沙人,博士,讲师,主要研究领域为通信与密码学;王新梅(1937-),男,浙江浦江人,教授,博士生导师,主要研究领域为信道编码,密码学,通信网络安全.

$GF(q)$上的 $n\times n$ 阶非奇异矩阵,则 $r(\lambda_X P)=r(x)$成立.

引理 2[1]. 对任意线性秩距离$[n,k,d]$码,秩距离满足不等式 $d\leqslant n-k+1$.

定义 2[1]. 满足 $d=n-k+1$ 的秩距离$[n,k,d]$码称为最大秩距离码.

引理 3[1]. 设 H 为码 M 的校验矩阵,则码 M 的最小秩距离为 d 的充要条件是:对任意元素属于 $GF(q)$,秩为 $d-1$ 的$(d-1)\times n$ 阶矩阵 Y,有 $r(YH^T;q^N)=d-1$;且存在元素属于 $GF(q)$,秩为 d 的 $d\times n$ 阶矩阵 Y_0,使得 $r(Y_0H^T;q^N)<d$.

下面,为了简化书写,引入符号$[i]=q^i,i=0,\pm 1,\dots$

令 $h_i\in GF(q^N)(i=1,2,\dots,n)$是在 $GF(q)$上线性无关的元素.指定整数 $d,d\leqslant n$,构造矩阵:

$$H=\begin{pmatrix} h_1 & h_2 & \dots & h_n \\ h_1^{[1]} & h_2^{[1]} & \dots & h_n^{[1]} \\ \vdots & \vdots & \vdots & \vdots \\ h_1^{[d-2]} & h_2^{[d-2]} & \dots & h_n^{[d-2]} \end{pmatrix}. \tag{1}$$

引理 4[1]. 校验矩阵如式(1)所示的码 M 是长度为 n,最小秩距离为 d 的最大秩距离码.

引理 5[3]. $GF(q)$上秩为 r 的 $m\times r$ 阶矩阵的数目为 $q^{\frac{r(r-1)}{2}}\prod_{i=0}^{r-1}(q^{m-i}-1)$.

推论 1. $GF(q)$上 $r\times r$ 阶非奇异矩阵的数目为 $q^{\frac{r(r-1)}{2}}\prod_{i=1}^{r}(q^i-1)$.

引理 6[1]. 设 H 为一个最大秩距离(n,k)码 M 的校验矩阵,该码的最小秩距离为 d.如果 Z^T 是 $GF(q)$上秩为 s 的 $n\times s$ 阶矩阵,其中 $s\geqslant d=n-k+1$,则矩阵 $\tilde{H}=HZ^T$ 为具有相同最小秩距离的最大秩距离$(s,k+s-n)$码 $\tilde{M}$ 的校验矩阵.

推论 2[1]. 如果 H 为最大秩距离$[n,k,d]$码的校验矩阵,Z 为 $GF(q)$上的 $n\times n$ 阶非奇异矩阵,则矩阵 $\tilde{H}=HZ^T$ 为同一最大秩距离$[n,k,d]$码的校验矩阵.

2 方案的构造

下面,我们基于最大秩距离码,提出一种新的 Stern 方案.

令 H 为 $GF(q^N)$上秩为$(n-k)$的一个随机$(n-k)\times n$ 阶矩阵.每个用户 U 选择秩为 r 的向量 $y_U\in GF(q^N)^n$,且计算 $s_U=y_UH^T$.

公钥:用户 U 的公钥由值 r,矩阵 H 和向量 s_U 组成.

私钥:用户 U 的私钥为向量 y_U.

3 协议的安全性分析

此协议的安全基于下述问题:给定矩阵 H,值 r 和向量 s,找一个秩为 r 的向量 y 满足 $s=yH^T$.随机矩阵 H 可看做是一个随机秩距离线性$[n,k,d]$码的校验矩阵,其中 d 为未知的.

可以从下面几方面考虑协议的安全性:(1) 由文献[4]可知,线性码的一般译码问题是 NP 完全的,建议的协议基于秩距离码的伴随式译码问题,由于对一般纠错码的各种译码方法不适用于秩距离码,所以基于秩距离码的伴随式译码问题看起来更难.另外,由于秩距离与秩距离码的特点,对基于一般纠错码的 Stern 方案的已知的各种攻击方法也不适合于此协议.(2) $GF(q^N)$上汉明重量为 w 的 n 维向量的总数为 $\binom{n}{w}(q^N-1)$,而 $GF(q^N)$上秩为 r 的 n 维向量的总数为 $\prod_{i=1}^{r}\frac{(q^n-q^{i-1})(q^N-q^{i-1})}{q^r-q^{i-1}}\approx q^{r(n+N)-r^2}$,当取 $r=w$ 时,此数比$\binom{n}{r}(q^N-1)$大得多,这样,对于充分大

的参数,通过穷搜索获得私钥更难.(3) 对于一般纠错码,当假设陪集中重量为 w 的向量服从均匀分布时,具有相同伴随式的重量为 w 的向量的平均数为 $\binom{n}{w}(q^N-1)/(q^N)^{n-k}$. 而对秩距离码,如果假设陪集中秩为 r 的向量服从均匀分布,则具有相同伴随式的秩为 r 的向量的平均数为 $\frac{1}{(q^N)^{n-k}}\prod_{i=1}^{r}\frac{(q^n-q^{i-1})(q^N-q^{i-1})}{q^r-q^{i-1}}$,当取 $r=w$ 时,此数比 $\binom{n}{w}(q^N-1)/(q^N)^{n-k}$ 要大. 因此基于秩距离码的 Stern 方案的密钥碰撞数比文献[2]所提出协议的密钥碰撞数大,但当 r 取得比较小而 n、N 取得比较大时,$\frac{1}{(q^N)^{n-k}}\prod_{i=1}^{r}\frac{(q^n-q^{i-1})(q^N-q^{i-1})}{q^r-q^{i-1}}$ 仍很小,而当 $r\leqslant[(d-1)/2]$ 时密钥无碰撞. 因此,总的来说,基于秩距离码的 Stern 方案是安全的.

作为一个数值例子,考虑 $n=32,k=N=16,r=6,q=2$ 的情形. 对此方案有两类攻击需要考虑:(1) 从 $s_U=y_UH^T$,寻找秩为 r 的解. 由文献[3]可知,对秩距离码的一般译码问题,需要 $O((nr+N)^3\cdot q^{(N-r)(r-1)})$ 次初等运算,对给定的数值,约需 2^{73} 次初等运算,在计算上这是不可行的. 而如果直接求解方程 $s_U=y_UH^T$,寻找秩为 r 的解,这时方程 $s_U=y_UH^T$ 有 $(q^N)^k=2^{256}$ 个解,对解进行穷搜索在计算上是不可行的.(2) 测试所有秩为 r 的向量. 大约有 $q^{r(n+N)-r^2}=2^{252}$ 个那样的向量,因此对所有这样的向量进行测试在计算上是不可行的.

References:

[1] Gabidulin, E. M. Theory of code with maximum rank distance. Problems of Information Transmission, 1985,21(1):1~12.

[2] Stern, J. A new identification scheme based on syndrome decoding. In: Stinson, D. R., ed. Advances in Cryptology—Proceedings of the Crypto'93. Lecture Notes in Computer Science, Vol773. Berlin, Heidelberg, New York: Springer-Verlag, 1994. 13~21.

[3] Chabaud, F., Stern, J. The cryptographic security of the syndrome decoding problem for rank distance codes. In: Kim, K., Matsumoto, T., eds. Advances in Cryptology—Asiacrypt'96. Lecture Notes in Computer Science, Vol1163. Berlin: Springer-Verlag, 1996. 368~381.

[4] Berlekamp, E. R., McEliece, R. J., Van, Tilborg, H. C. A. On the inherent intractability of certain coding problems. IEEE Transactions on Information Theory, 1978,24(3):384~386.

A Stern Scheme Based on Maximum Rank Distance Codes*

DU Wei-zhang, WANG Xin-mei

(*National Key Laboratory of Integrated Service Networks, Xidian University, Xi'an* 710071, *China*)

E-mail: duweizhang@yahoo.com.cn

http://www.xidian.edu.cn

Abstract: Based on maximum rank distance codes, a new kind of Stern scheme is proposed in this paper, security of this scheme is discussed and it is proved that this scheme is secure when the parameters are selected properly.

Key words: rank distance code; error-correcting code; protocol; security

---

* Received March 6, 2000; accepted June 12, 2000

Supported by the National Research Foundation for the Doctoral Program of Higher Education of China under Grant No. 98070104

1000-9825/2001/12(10)1555-07 ©2001 Journal of Software 软件学报 Vol.12, No.10

动态优先系统及其应用*

李文军[1,2]，周晓聪[1]，李师贤[1]

[1](中山大学 计算机科学系,广东 广州 510275);

[2](南京大学 计算机软件新技术国家重点实验室,江苏 南京 210093)

E-mail: lnslwj@zsu.edu.cn

http://www.selab.zsu.edu.cn

摘要：优先关系是并发系统控制的重要手段，常用于解决并发系统设计中的冲突问题.在有界P/T系统的基础上提出一种动态优先系统，并分别给出它们的交错语义与真并发语义.动态优先系统既可以作为并发与分布式系统的建模工具，也可以作为定义程序设计语言中优先算子的语义基础.最后，基于动态优先系统的概念，为Occam语言扩充了一种动态优先选择算子.

关键词：并发模型;Petri网;优先关系

中图法分类号：TP311 **文献标识码**：A

控制是并发系统研究的核心问题之一，诸如冲突解析、任务调度、进程同步等本质上均表现为控制问题.优先关系是一种常见的控制方式，为解决并发系统设计中的冲突问题提供了一种方便而实用的途径.本文提出的动态优先系统是一种带有动态优先结构的Petri网系统(Σ,D)，其中Σ是有界Petri网，D是描述Σ的变迁之间优先关系的动态优先结构.本文分别给出Σ为安全网和Σ为有界网时(Σ,D)的Petri网语义，讨论了动态优先系统的两个应用方向，并为Occam语言扩充了一种动态优先选择算子.

1 并发模型与优先关系

优先关系是现实生活中常见的行为关系，用于解决因资源竞争产生的不确定性.许多并发系统运行时要求行为间的优先关系可以动态改变，即在状态S_1，动作a优先于b，但在S_2，可能b优先于a.有许多实例说明，并发模型中优先关系应具备灵活的动态特征.例如，女士优先原则规定男女相遇时女士先行，然而灯光暗淡或路面难行时还遵循该规则会被视为过腐或缺乏绅士风度.古罗马帝国在和平时期执政官权力很小，主要决策由元老院作出，但出现战争、灾难等危机时权力移交给执政官，此时更需要快速反应决策而不是民主.

鉴于优先关系在并发与分布式系统中的作用，对并发模型中优先关系的研究进行了许多有益的尝试.部分工作建立在以Petri网为代表的真并发模型上.Hack最早为Petri网扩充优先关系[1]，Best和Koutny提出优先系统(Σ,ρ)[2]，其中ρ是Σ变迁集上的二元优先关系，但该模型只能描述静态优先关系.本文工作建立在文献[2]的基础上，不同的是，优先结构具有良好的动态特征，并且优先关系动态调整可在规格说明中显式地表达出来.

---

* **收稿日期**：2000-03-06；**修改日期**：2000-06-13

基金项目：高等学校博士点基金资助项目(99-018-411703)

作者简介：李文军(1966－)，男，广东从化人，副教授，主要研究领域为并行与分布式计算，软件工程；周晓聪(1971－)，男，湖南常宁人，讲师，主要研究领域为软件工程，类型系统理论；李师贤(1944－)，男，江西于都人，教授，博士生导师，主要研究领域为形式语义学，软件工程.

由于并发与优先关系结合而产生的语义问题,更多的工作建立在交错模型上.例如,$CCS^{+>}$模型为 CCS 扩充了优先选择算子[3];$PCCS_\xi$ 模型为概率 CCS 扩充了 0 概率变迁,将优先关系看做是概率的极端[4];CCS^{prio}模型为 CCS 引入优先关系,并研究了进程的等价性与等效性[5].

2 动态优先系统

动态优先系统建立在有界 P/T 系统基础上,Petri 网的基本定义参见文献[6].任给变迁集合 X,X 上的优先关系 $\rho\subseteq X\times X$ 满足反自反性和反对称性,除此之外不强加 ρ 任何约束.$(x,y)\in\rho$ 表示 x 的优先级高于 y,记为 $x\prec_\rho y$ 或 $y\succ_\rho x$,上下文无二义时省略下标 ρ.

定义 1. 动态优先结构是四元组 $D=(T,P,\delta,\rho_0)$,其中 T 是有穷变迁集,T 上的二元关系 ρ 称为 D 的一个优先格局当且仅当 ρ 是反自反和反对称的,D 的所有优先格局的集合记为 $prior(D)$,$\rho_0\in prior(D)$是初始优先格局;优先变迁集 P 是对目标系统中可调整优先关系的所有行为的抽象;偏函数 $\delta:T\times T\times P\rightarrow T\times T$ 是优先关系调整函数,对任意 $x,y\in T$ 和 $t\in P$,δ 定义为

$$\delta(x\prec y,t)=\begin{cases}y\prec x, & \delta\text{ 有定义,则改变优先关系方向}\\ \perp, & \text{否则},\delta\text{ 无定义}\end{cases},$$

并且满足如下的惟一性约束:

(1) $\forall x_1,x_2,y_1,y_2\in T.\ (x_1,y_1)\neq(x_2,y_2)\wedge\delta(x_1\prec y_1,t_1)\neq\perp\wedge(x_2\prec y_2,t_2)\neq\perp\Rightarrow t_1\neq t_2$

(2) $\forall x,y\in T.\ \delta(x\prec y,t_1)\neq\perp\wedge\delta(x\prec y,t_2)\neq\perp\Rightarrow t_1=t_2$.

直观上理解,$\delta(x\prec y,t)=\perp$ 表示 t 发生对优先关系 $x\prec y$ 不产生影响,否则将改变 x 和 y 的优先关系.约束(1)规定一个优先变迁只可作用在一对优先关系上,约束(2)规定一对优先关系只能由一个优先变迁改变.注意,$\delta(x\prec y,t)=y\prec x$ 并不蕴含 $\delta(y\prec x,t)=x\prec y$.

δ 可进一步重载为优先格局的函数 $\delta:prior(D)\times P\rightarrow prior(D)$.对任意 $\rho\in prior(D)$和 $t\in P$,定义 $\rho'=\delta(\rho,t)=\{y\prec_{\rho'}x\mid x\prec_\rho y\wedge\delta(x\prec y,t)\neq\perp\}\cup\{x\prec_{\rho'}y\mid x\prec_\rho y\wedge\delta(x\prec y,t)=\perp\}$,表示在优先格局 ρ 发生变迁 t 而产生新的优先格局 ρ',记为 $\rho(t)\rho'$.这种记号还可推广到变迁串:记 ε 为空变迁串,任给变迁串 $s\in P^*$,定义 $\delta(\rho,\varepsilon)=\rho$ 且 $\delta(\rho,ts)=\delta(\delta(\rho,t),s)$.

定义 2. 动态优先结构 $D=(T,P,\delta,\rho_0)$的可达优先格局集$\langle\rho_0\rangle$是从 ρ_0 出发可到达的所有优先格局集,定义为满足 $\rho_0\in\langle\rho_0\rangle$且 $\rho'\in\langle\rho_0\rangle\wedge\exists\, t\in P.\ \rho'(t)\rho''\Rightarrow\rho''\in\langle\rho_0\rangle$的最小集合.

定义 3. 动态优先系统(Σ,D)由网系统 $\Sigma=(S,T;F,K,W,M_0)$和动态优先结构 $D=(T,P,\delta,\rho_0)$组成,满足 $S\cap P=\varnothing$.注意,并未约束 $P\cap T=\varnothing$,因为 Σ 中建模的行为也可能动态改变某些优先关系,而那些仅对优先结构动态调整起作用的优先变迁在 Σ 中不需要建模,它们由集合 P-T 加以描述.

动态优先系统为并发模型引入了优先关系,而且显式表达了优先关系在运行过程中的动态调整.例如,古罗马帝国决策体制可用如图 1 所示的动态优先系统建模,其中 power 选择结构防止同时有两个统治者发号施令,senate 与 consul 是否有决策权不像 P/T 系统那样不确定,而是由两者的优先关系决定,这种关系会因 war 或 peace 改变.注意,动态调整优先关系的动作 war 和 peace 并没有在 P/T 系统中出现,这种表达使模型核心内容更清晰.

动态优先系统(Σ,D)的动态性特征是 Σ 变迁间的优先关系在由 ρ_0 确定之后,δ 不允许创建 ρ_0 之外的两个变迁间的优先关系,也不允许取消 ρ_0 中已有的优先关系,而只能动态调整已有的优先关系的方向.其直觉理解是任何优先关系都有明确的初始状态,且两个变迁一旦存在优先关系就不可取消,尽管它们之间的优先权可能交换.

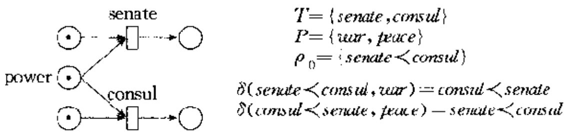


Fig. 1 Governing power distribution in the Rome empire
图1 古罗马帝国的统治权分配机制

3 动态优先系统的语义

3.1 交错语义与真并发语义

利用扩展变迁序列可直接给出动态优先系统的交错语义.由于增加了优先关系约束,则须规定在标识M变迁t不存在优先权更高的变迁t'受权发生时,t才可能受权发生.变迁$t\in T\cup P$,在状态(M,ρ)受权发生的条件是$(t\in P-T\Rightarrow def(\rho,t))\wedge(t\in T-P\Rightarrow M[t\rangle\wedge pri(M,\rho,t))\wedge(t\in T\cap P\Rightarrow def(\rho,t)\wedge M[t\rangle\wedge pri(M,\rho,t))$,其中$def(\rho,t)\Leftrightarrow\exists\ x,y\in T.\ x\prec_{\rho}y\wedge\delta(x\prec y,t)\neq\perp$;$pri(M,\rho,t)\Leftrightarrow\neg\exists\ t'\in T.\ t'\prec_{\rho}t\wedge M[t'\rangle$.

t发生后产生新标识M'与新优先格局ρ',记为$(M,\rho)[t\rangle(M',\rho')$,新状态定义为$(t\in P-T\wedge\rho(t)\rho'\Rightarrow(M,\rho)[t\rangle(M,\rho'))\wedge(t\in T-P\wedge M[t\rangle M'\Rightarrow(M,\rho)[t\rangle(M',\rho))\wedge(t\in T\cap P\wedge\rho(t)\rho'\wedge M[t\rangle M'\Rightarrow(M,\rho)[t\rangle(M',\rho'))$.记$[M_0,\rho_0\rangle$为满足$(M_0,\rho_0)\in[M_0,\rho_0\rangle$且$(M',\rho')\in[M_0,\rho_0\rangle\wedge\exists\ t\in T\cup P.\ (M',\rho')[t\rangle(M'',\rho'')\Rightarrow(M'',\rho'')\in[M_0,\rho_0\rangle$的最小集合.

扩展变迁序列$\sigma=t_1\ldots t_n(n\geqslant 0)$是$T\cup P$中变迁的有穷序列,满足$\exists\ (M_1,\rho_1),\ldots,(M_n,\rho_n)\in[M_0,\rho_0\rangle.\ (M_{i-1},\rho_{i-1})[t_i\rangle(M_i,\rho_i)(i=1,\ldots,n)$,$(\Sigma,D)$所有扩展变迁序列的集合记为$seq(\Sigma,D)$.用$seq(\Sigma,D)$描述$(\Sigma,D)$的行为即给出动态优先系统的交错语义.

然而,在定义真并发语义时情况变得复杂化.由于Petri网是真并发模型,优先关系与并发关系这两种规格说明交互作用导致优先关系难以形式化,例如,一对变迁间的优先关系可能与另一对变迁间的并发关系产生冲突[2].

我们采用变换方法给出真并发语义,将(Σ,D)变换为不带任何优先结构的P/T系统Σ_D.记(Σ,D)所有步序列[7]的集合为$steps(\Sigma,D)$,记$steps(\Sigma,D)$关于线性化运算封闭的最大子集为$kernel(\Sigma,D)$,借助步序列语义可以证明$steps(\Sigma_D)$与$steps(\Sigma,D)$的差别最小,即$steps(\Sigma_D)=kernel(\Sigma,D)$[8].直观上看,$(\Sigma,D)$的语义由$\Sigma_D$的行为刻画,这些行为满足动态优先结构$D$的规格说明约束,并尽可能保持了$\Sigma$的并发性.下面,我们假设$\Sigma$是无冲撞的,实际应用时可通过添加补位置消除可能出现的冲撞现象.

3.2 针对安全系统的变换技术

广义补位置是位置子集的补位置,允许补位置的标记数与关联的弧数放大,并可扩大容量以添加冗余标记.广义补位置在Σ_D的构造过程中起着重要作用.

如果Σ是安全的,则动态优先系统(Σ,D)称为安全的.此时,构造Σ_D的基本思路是对任意变迁t,如果有变迁u优先权高于t,则利用一个广义补位置跟踪u的所有输入位置中的标记数,从而保证当u受权发生时t无法受权发生,仅当u未受权发生时t才可能受权发生.优先结构的动态性通过往广义补位置添加若干表示优先权的标记实现,优先关系调整相当于优先变迁将这些标记从一个广义补位置移到另一个广义补位置.

我们分3步来构造Σ_D.

(1) 首先为每对 $t_i \prec_{\rho_0} t_j$ 添加 t_i 和 t_j 的输入集的广义补位置 γ_{ij}和 γ_{ji},放大容量以容纳表示优先权的标记,并在 γ_{ji} 中多放若干标记表示优先权可由 t_i 使用.

(2) 然后构造 t_i 到 γ_{ji}和 t_j 到 γ_{ij}的两条优先权检测回路,当 $t_i \prec t_j$ 时,t_i 到 γ_{ji}的检测总成功,而 t_j 到 γ_{ij}的检测是否成功取决于 t_i 是否受权发生;如果 γ_{ji}到 t_i 或 γ_{ij}到 t_j 已存在弧,则这些弧本身已具备检测功能,因而不必添加新弧.

(3) 最后处理优先关系的动态调整. 如果 $\delta(t_i \prec t_j, p) \neq \bot$,则添加 p 与相关的弧.

利用步序列语义可以证明 Σ_D 具有良好的语义性质[8]:$steps(\Sigma_D)=kernel(\Sigma,D)$,即 $steps(\Sigma_D)$ 是 $steps(\Sigma,D)$关于线性化运算封闭的最大子集,表明 $steps(\Sigma_D)$与 $steps(\Sigma,D)$的差别尽量最小.

3.3 针对有界系统的变换技术

如果 Σ 有界,则分 5 步构造 Σ_D.

(1) 首先为 D 中每对 $t_i \prec_{\rho_0} t_j$ 分别添加 t_i 和 t_j 的每个输入位置 s_{ik}和 s_{jk}的补位置 γ_{ijk}和 γ_{jik},所有 γ_{ijk}均放大容量以容纳表示优先权的若干标记,并在 γ_{jik}中多放若干标记表示当前优先格局下优先权由 t_i 使用.

(2) 然后为每对 $t_i \prec_{\rho_0} t_j$ 分别分解 t_i 和 t_j,所得副本保持原变迁的弧连接关系,t_i 的副本数是与 t_i 有优先关系的变迁的输入位置间的组合数,以便对这些输入位置作组合检测.

(3) 根据变迁的最大自并发数复制变迁及相关补位置,从而支持变迁在 Σ_D 的自并发.

(4) 添加一组用于检测是否具有优先权的回路,$t_{ij_1k_1\ldots j_mk_ml}$组合检测变迁 t_{j_1} 的输入位置 s_{k_1} 的补位置 $\gamma_{j_1ik_1l},\ldots$,变迁 t_{j_m} 的输入位置 s_{k_m} 的补位置 $\gamma_{j_mik_ml}$等.

(5) 最后处理优先变迁对优先关系的动态调整.

由于上述构造过程对变迁进行了分解,讨论 Σ_D 与(Σ,D)之间的语义关系必须对 Σ_D 变迁重标号. 重标号函数 *ancestor* 和 *merge* 将分解变迁副本映射回 Σ 中的原变迁,并在变迁袋集中对这些变迁进行合并. 可以证明 $merge(steps(\Sigma_D))\subseteq kernel(\Sigma,D)$,同时有反例说明反向包含关系不一定成立. 这一定理刻画了 Σ_D 的语义性质,表明 Σ_D 的构造过程丢失了部分并发性. 反向包含关系仅当满足某些条件时才成立,我们进一步给出了使 $merge(steps(\Sigma_D))=kernel(\Sigma,D)$成立的一个充分条件[8].

4 动态优先系统的应用

动态优先系统可作为一种适合处理并发性与分布性的建模工具. 动态优先系统为 Petri 网引入优先关系,并允许在规格说明中显式地描述优先关系的动态变化,从而提供了一种简便而有效的控制手段,以减少并发与分布式系统规格说明中不必要的不确定性.

许多并发与分布式应用都可将优先关系作为一种有效的控制方式,例如,经典的读/写问题[9]也可用动态优先系统建模. 文献[9]的 Petri 网模型解决了最多 n 个进程同时读的读/写问题,可保证读写互斥原则并避免死锁. 利用优先关系作为控制手段可以给出该问题的更简单模型,如图 2(a)所示. 该模型节省了用于同步与互斥的位置 s_1,代之以两个优先关系约束:$r_2 \prec w_1$ 和 $w_2 \prec r_1$. $r_2 \prec w_1$可理解为当 r_2 与 w_1 同时受权发生时 w_1 不会真正发生,从而避免了有进程正在读时任何写进程的进入;$w_2 \prec r_1$ 则避免了有进程正在写时读进程的进入.

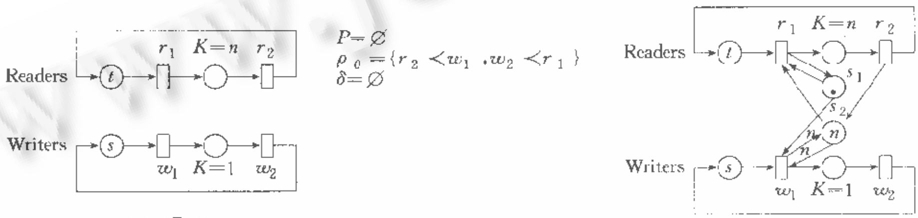
该模型是有界的而不是安全的,可用第 3.3 节中的变换技术转换为如图 2(b)所示的 Petri 网. 变换前先用补位置消除 Σ 可能出现的冲撞现象,并在变换后删除无用的补位置及优先权检测回

路. 虽然变换结果与原 Petri 网模型不同,但同样解决了互斥与死锁问题. 可见动态优先系统建立的模型比 Petri 网更简洁(不必考虑变换后的结果,正如高级语言程序员不必考虑编译的目标代码一样),这样,开发人员可将精力集中到模型的核心,而一些互斥与同步等控制则借助优先关系来完成.

动态优先系统的另一应用是为并发与分布式语言提供形式语义,特别是其中的优先算子. 例如,Occam 语言的优先选择算子 PRIALT 的典型形式是:

$$\begin{array}{c}\text{PRIALT}\\ a_1?\ X_1\rightarrow P_1\\ \vdots\\ a_k?\ X_k\rightarrow P_k\end{array}$$

表示进程从信道 $a_1,\ldots,a_k$ 接收数据,排列越前的信道则具有越高的通信优先权,仅当 a_i 就绪而 $a_1,\ldots,a_{i-1}$ 均未就绪时才会从 a_i 接收数据.



(a) (Σ,D) (b) Σ_D

Fig. 2 The dynamic priority system model for the readers/writers problem and the translated Petri net
图2 读/写问题的动态优先系统模型及其变换得到的Petri网

为了给出 Occam 语言的 Petri 网语义,通常先定义 Occam 程序的抽象语法,然后再用 Petri 网给出抽象程序的语义. 例如,在抽象程序 $P_1=(a;c?)\parallel(b;c!\ \square d)$ 中,事件 $c?$ 和 $c!$ 分别表示从信道 c 输入和输出信息,$P;Q$ 表示进程 P 和 Q 的顺序执行,$\square$ 和 $\parallel$ 分别对应 CSP 的不确定选择和同步并行复合,本例中事件 $c?$ 和 $c!$ 必须同步. 该程序的语义如图 3 所示.

P_1 中 $c!\ \square d$ 表示事件 $c!$ 和 d 的发生是不确定的,如果程序员要控制它们发生的优先次序,可用优先选择算子 $\square\!<$ 将 P_1 改写为 $P_2=(a;c?)\parallel(b;c!\ \square\!< d)$,其中 $P\square\!< Q$ 表示只要 P 的初始事件就绪,则 Q 的初始事件不会发生,否则 $P\square\!< Q$ 的行为与 $P\square Q$ 相同. 利用本文提出的动态优先系统,可根据图 3 直接得到该程序的语义,如图 4 所示.

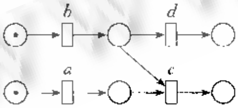


Fig. 3 The Petri net corresponding to P_1
图3 P_1 对应的Petri网

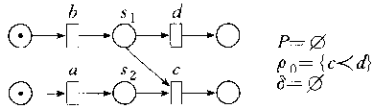


Fig. 4 The dynamic priority system corresponding to P_2
图4 P_2 对应的动态优先系统

$c!\ \square\!< d$ 中优先选择算子不仅与另一子程序中的事件 $c?$ 有关联,而且与该子程序中的事件 a 也关联,因为 a 的发生使信道 c 上的通信受权发生. 根据前述从 (Σ,D) 到 Σ_D 的变换过程,这反映在位置 s_1 和 s_2 的广义补位置将变迁 a 关联到 c 和 d. 由于当不涉及优先算子时根据 Occam 抽象程序构造的 Petri 网均为有界的,所以用动态优先系统可有效地刻画其真并发语义.

优先算子通常只表达了事件间的静态优先关系,程序员无法显式地刻画优先关系在系统演化过程中的动态变化,处理这类算子只需在动态优先系统中令 $P=\varnothing\wedge\delta=\varnothing$ 即可. 本节尝试为

Occam引入一种新的动态优先选择算子,利用动态优先系统可以直接给出它的形式语义.在抽象语法中定义优先关系表达式为两个事件之间加上优先关系比较算子$\prec$,例如$e_1 \prec e_2$表示事件e_1优先级高于e_2.如果事件e之后紧接方括号括住优先关系表达式,如$e[e_1 \prec e_2]$,则表明e是一个优先关系调整事件,其直观语义是仅当e_2优先级高于e_1时e才会发生,发生结果至少保证e_1的优先级高于e_2.为了避免递归定义所带来的问题,规定优先关系调整事件e不出现在任何优先关系表达式中.此外,对e不作任何限制,从而允许e既可兼作普通事件,也可仅用于动态调整其他事件间的优先关系.

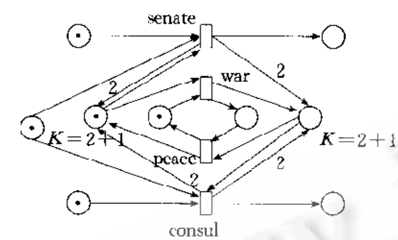


Fig. 5　The translated result of the dynamic priority system corresponding to P_3

图5　P_3对应动态优先系统的变换结果

此时,程序有一个全局状态描述优先关系格局.动态优先选择算子$P\succ\square\prec Q$规定了初始优先关系格局:P的初始事件优先级高于Q的初始事件,如果程序执行过程中这种格局未经任何优先关系调整事件改变,则$P\succ\square\prec Q$的语义与$P\square\prec Q$相同;如果经过调整,则$P\succ\square\prec Q$的语义既可能与$P\square\prec Q$相同,也可能与$Q\square\prec P$相同,这取决于当时的优先关系格局.

例如,抽象程序P_3=(war[consul$\prec$senate]$\sqcap$peace[senate$\prec$consul])|(senate$\succ\square\prec$consul)的语义如图1所示.由于该系统是安全的,可用第3.2节中的步骤变换为如图5所示的Petri网,并保证了结果尽可能保持原有的并发语义.对该例而言,两者的并发语义完全相同.

5　结束语

本文提出一种动态优先系统,并用变换技术给出其Petri网语义.动态优先系统显式地刻画了变迁间优先关系的动态调整,既可作为一种并发与分布系统的建模工具,也可用于定义优先算子的形式语义.基于动态优先系统的概念与思想,本文提出一种适于类Occam语言的动态优先选择算子.文中仅给出描述该算子语法与语义的基本思路,进一步的工作是完善这些定义并在机器上实现该算子.

References:

[1] Hack, M.H. Petri net languages. Technical Report, TR-159, Laboratory Computer Science, MIT, 1976.

[2] Best, E., Koutny, M. Petri net semantics of priority systems. Theoretical Computer Science, 1992,96(1):175~215.

[3] Camilleri, J., Winskel, G. CCS with priority choice. Information and Computation, 1995,116(1):26~37.

[4] Smolka, S.A., Steffen, B. Priority as extremal probability. In: Baeten, J.C., Klop, J.W., eds. Proceedings of the CONCUR'90. Lecture Notes in Computer Science 458. Berlin: Springer-Verlag, 1990. 456~466.

[5] Cleaveland, R., Hennessy, M. Priorities in process algebras. Information and Computation, 1990,87(1):58~77.

[6] Yuan, Chong-yi. Principles of Petri nets. Beijing: Electronics Industry Press, 1998. 1~75 (in Chinese).

[7] Janicki, R. A formal semantics of concurrent systems with a priority relation. Acta Informatica, 1987,24(1):33~55.

[8] Li, Wen-jun. Models for concurrency and dynamic priority systems [Ph.D. Thesis]. Beijing: Institute of Software, The Chinese Academy of Sciences, 2001 (in Chinese).

[9] Peterson, J.L. Petri Net Theory and the Modeling of Systems. Englewood Cliffs, NJ: Prentice Hall, 1981. 66~68.

附中文参考文献:

[6] 袁崇义.Petri网原理.北京:电子工业出版社,1998.1~75.

[8] 李文军.并发模型与动态优先系统[博士学位论文].北京:中国科学院软件研究所,2001.

Dynamic Priority Systems and Their Applications*

LI Wen-jun[1,2], ZHOU Xiao-cong[1], LI Shi-xian[1]

[1](*Department of Computer Science, Zhongshan University, Guangzhou* 510275, *China*);

[2](*State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing* 210093, *China*)

E-mail: lnslwj@zsu.edu.cn

http://www.selab.zsu.edu.cn

Abstract: Priority is an important approach to the control of concurrent systems. It is often applied to solve the conflict problems in the design of concurrent systems. In this paper, the concept of dynamic priority systems is developed based on bounded P/T systems and the interleaving and the true-concurrency semantics are provided for them respectively. Dynamic priority systems can be used as both modeling tools to build concurrent and distributed systems and semantic foundations to define prioritised operators in programming languages. Finally, the Occam language with a dynamic prioritised operator based on the concept of dynamic priority systems is extended.

Key words: model for concurrency; Petri nets; priority

---

* Received March 6, 2000; accepted June 13, 2000

Supported by the National Research Foundation for the Doctoral Program of Higher Education of China under Grant No. 99-018 411703