网上证券交易系统的时序 Petri 网描述及验证*

杜玉越[1,2,3], 蒋昌俊[1]

[1](同济大学 计算机科学与工程系,上海 200092);
[2](聊城师范学院 计算机科学系,山东 聊城 252059);
[3](中国科学院 软件研究所 计算机科学重点实验室,北京 100080)
E-mail: yydu001@163.com; cjjiang@online.sh.cn
http://www.tongji.edu.cn

摘要: 基于时序 Petri 网对我国现行网上静态和动态证券交易系统进行了模拟、形式描述及功能正确性验证.应用时序逻辑推理规则,从形式上严格证明了证券交易系统需求规范及其时序 Petri 网模型动态行为的一致性.结果表明,时序 Petri 网能够清楚而简单地描述事件间的因果关系和时序关系以及并发系统中某些与时间有关的重要性质,如最终性和公平性.因此,时序 Petri 网可作为并发系统形式化描述和分析的有力工具.

关 键 词: 模型检查;证券交易系统;时序逻辑;Petri 网;形式描述;正确性验证;电子商务
中图法分类号: TP311 文献标识码: A

网上证券交易具有公平性、速度快等特点,因此越来越受到众多券商和股民的青睐.它也是电子商务中最早实现电子数据交换的重要领域之一.但是与传统的证券交易方式相比,在线证券交易系统需要更高的安全性和可靠性.其安全性通过数据加密技术和数字签名技术来实现,可靠性反映了交易数据的有效性、公平性及交易撮合过程的正确性.在证券交易系统中,股民申报的交易数据,先由所委托的券商验证交易数据的有效性,再由券商处理系统将验证后的有效数据发送到相应的交易所,最后在交易所前置机中记录交易数据的到达时间,把它们按其所属股票进行分类,并输送到交易机进行撮合处理.

任何采用非形式化设计方法产生的交易协议,都需要进行分析和校验,以确保协议规范和其服务规范的一致性.因此,本文以上海交易所证券交易系统为基础,基于时序 Petri 网[1~3]对网上证券交易系统进行模拟、描述及其正确性验证.进一步表明,时序 Petri 网与 Petri 网[4]和时间 Petri 网[5,6]相比,能够较好地表达事件间的因果关系和时序关系以及并发系统中某些具有时间限制的基本性质,如最终性(某些事件必须最终发生,某些条件必须最终满足)和公平性(如果一个事件常常无限次地可以发生,则它必须常常无限次地发生).

1 基本概念

五元组 $PN=(P,T;F,W,M_0)$ 称为一个 Petri 网当且仅当 P 表示库所的有限集;T 表示变迁的有限集:$P\cap T=\varnothing, P\cup T\neq\varnothing$;且 $F\subseteq(P\times T)\cup(T\times P)$ 表示一个弧集(即流关系);$W:F\rightarrow\{1,2,\ldots\}$ 表示一个权函数;$M_0:P\rightarrow\{0,1,2,\ldots\}$ 是一个初始标识.当 Petri 网用有向图表示时,库所 p 表示成一个圆,变迁 t 表示成一个短线;库所 p 与变迁 t 之间的关系,由有向弧线表示,对任意库所 p,在它里边画 $M(p)$ 个圆点以表示当前标识 M.t 在 M 可引发当且仅当 $\forall p\in{}^{\cdot}t, M(p)\geq W(p,t)$,其中 ${}^{\cdot}t$ 表示 t 的所有输入库所构成的集合.若 t 在标识 M 可引发,则 t 可以引发,并产生一

* 收稿日期: 2001-07-10; 修改日期: 2001-11-26
基金项目: 国家自然科学基金资助项目(69973029,69933020);国家重点基础研究规划 973 资助项目(G1998030604);中国科学院软件研究所计算机科学重点实验室资助项目(SYSKF0205)
作者简介: 杜玉越(1960－),男,山东聊城人,博士生,教授,主要研究领域为模型检查,协议形式化验证,并发理论,Petri 网应用;蒋昌俊(1962－),男,安徽安庆人,博士,教授,博士生导师,主要研究领域为并发理论,并行处理,Petri 网,软件形式化验证.

个后继标识 M',记为 $M[t>M'$,其中$\forall p\in P:M'(p)=M(p)-W(p,t)+W(t,p)$.当 $W(p,t)$或 $W(t,p)$是一个整数型变量时,称其为可变权函数,通常由变量 N 表示,在给定的模拟系统中,这些可变权有一定的具体含义.

一个时序 Petri 网 TPN(temporal Petri net)由 PN 和 f 构成,$TPN=(PN,f)$,其中 PN 是一个 Petri 网,f 是一个公式且具有下列性质:

(1) 命题 p,t_{fir} 和 t 是原子命题,这里 $p\in P,t\in T$;

(2) 原子命题是公式;

(3) 若 f 和 g 是公式,则$\neg f,f+g,f\bullet g,f\Rightarrow g,\bigcirc f,\Diamond f,\Box f$ 和 f until g 也是公式.

在上述性质中,p 表示在库所 p 中至少有一个标志(token);t_{fir} 表示变迁 t 在当前标识下可引发;t 表示变迁 t 在当前标识下引发.符号¬,+,•和⇒是布尔(Boolean)连接符.公式$\bigcirc f$表示在当前标识的下一个可达标识,f为真;公式$\Diamond f$表示在当前标识下,存在一个可达标识,使得f为真;公式$\Box f$表示从当前标识开始(包括当前标识)的每一个可达标识,f总为真;公式 f until g 表示从当前标识开始的每一个可达标识,f 总为真但 g 总为假,或对 g 为真之前的所有可达标识,f 总为真.

事实上,时序 Petri 网是在 Petri 网中引入时序逻辑[7,8]公式,而这些逻辑公式对 Petri 网的变迁引发序列施加限制.仅当变迁 t 满足 Petri 网引发条件和逻辑公式时,t 才可引发,其后继标识的定义与 Petri 网相同.

设 S 是一个集合,$S^{\infty}=S^{*}\cup S^{\omega}$,其中 S^{*}表示 S 中元素的所有有限序列集合(包含空集合 λ),S^{ω}表示 S 中元素的所有无限序列集合.对$\alpha\in S^{*}$,用$|\alpha|$表示α的长度.若$\alpha\in S^{\omega}$,用符号ω表示α的长度,且对任一正整数 $i,i<\omega.\alpha\beta$表示序列α和β的顺序连接.设 M 是 TPN 的一个标识,$L(TPN,M)$和 $L^{\omega}(TPN,M)$分别表示在 M 下的所有有限和无限引发序列集合,并且 $L^{\infty}(TPN,M)=L(TPN,M)\cup L^{\omega}(TPN,M)$.设$\alpha\in L^{\infty}(TPN,M),0\le i\le|\alpha|$,若$\beta_i$ 和γ_i 是α的两个子序列,且满足$|\beta_i|=i,\alpha=\beta_i\gamma_i$,则称$\beta_i$是$\alpha$的前缀,$\gamma_i$是$\alpha$的后缀.设 $M[\beta>M_i,f$ 是一个公式.$\langle M,\alpha\rangle\vdash f$ 意味着 M 和α使得 f 为真,其中⊢表示一个有效公式.一些 TPN 公式的定义如下:

(a) $\langle M,\alpha\rangle\vdash p$ iff $M(p)>0$;

(b) $\langle M,\alpha\rangle\vdash t_{fir}$ iff t 在 M 是可引发的;

(c) $\langle M,\alpha\rangle\vdash t$ iff $\alpha\neq\lambda$且 $t=\beta_1$,即 t 在 M 引发;

(d) $\langle M,\alpha\rangle\vdash\neg f$ iff 在 M 和α下,f不为真;

(e) $\langle M,\alpha\rangle\vdash f\cdot g$ iff $\langle M,\alpha\rangle\vdash f$且$\langle M,\alpha\rangle\vdash g$;

(f) $\langle M,\alpha\rangle\vdash f+g$ iff $\langle M,\alpha\rangle\vdash f$或$\langle M,\alpha\rangle\vdash g$;

(g) $\langle M,\alpha\rangle\vdash f\Rightarrow g$ iff $\langle M,\alpha\rangle\vdash f$意味着$\langle M,\alpha\rangle\vdash g$;

(h) $\langle M,\alpha\rangle\vdash\bigcirc f$ iff $\alpha\neq\lambda$且$\langle M_1,\gamma_1\rangle\vdash f$;

(i) $\langle M,\alpha\rangle\vdash\Box f$ iff 对每一个 $i:0\le i\le|\alpha|$,$\langle M_i,\gamma_i\rangle\vdash f$;

(j) $\langle M,\alpha\rangle\vdash\Diamond f$ iff 存在某一个 $i:0\le i\le|\alpha|$,$\langle M_i,\gamma_i\rangle\vdash f$;

(k) $\langle M,\alpha\rangle\vdash f$ until g iff 对每一个 $i:0\le i\le|\alpha|$,$\langle M_i,\gamma_i\rangle\vdash f$;或者,存在某一个 $i:0\le i\le|\alpha|$,$\langle M_i,\gamma_i\rangle\vdash g$,且对每一个 $j:0\le j<i$,$\langle M_j,\gamma_j\rangle\vdash f$.

在标识 M 下,TPN 的引发序列集 $L(TPN,M)$定义为:$L(TPN,M)=\{\alpha|\alpha\in L^{\infty}(PN,M)$ and $\langle M,\alpha\rangle|-f\}$.

容易证明下述时序性质 PR1,PR2 和 PR3.PR4 在文献[3]中已证明.PR4 意味着对任意在 M 可引发的序列α,若 t 可引发,则 t 必须最终引发.通过检查交易系统时序 Petri 网模型,本文中性质 $PR4$ 成立.

PR1. $\langle M,\alpha\rangle\vdash f+\bigcirc f$ 意味着$\langle M,\alpha\rangle\vdash\Diamond f$;

PR2: $\langle M,\alpha\rangle\vdash\Box(f_1\Rightarrow\Diamond f_2)\cdot\Box(f_2\Rightarrow\Diamond f_3)$ 意味着$\langle M,\alpha\rangle\vdash\Box(f_1\Rightarrow\Diamond f_3)$;

PR3: $\langle M,\alpha\rangle\vdash\Diamond(\Diamond f)$ 意味着$\langle M,\alpha\rangle\vdash\Diamond f$;

PR4: $\langle M,\alpha\rangle\vdash\Box(t_{fir}\Rightarrow\Diamond t)$.

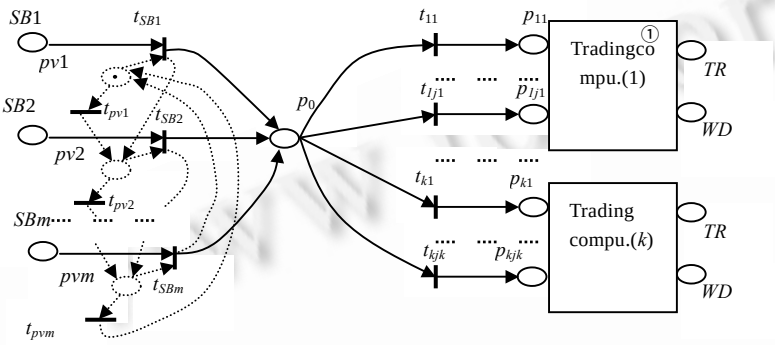
2 证券交易系统的时序 Petri 网描述

通常,股民申报的交易数据有 4 种:买、卖申报数据以及撤消买、卖申报数据.由于交易数据的分类、撮合和成交处理均在交易所进行,因此本文仅对交易所中申报数据的处理、撮合成交过程进行模拟、分析和验证.

2.1 多处理机静态交易系统

由于上市公司多达千家,交易数据的撮合成交是在同一种股票中进行的,所以交易所要对股民的申报数据作相应的分类.在某一时刻,一台交易处理机只能作一种股票的数据撮合.因此,交易所一般采用多处理机交易系统,其中一台处理机(称为前置机)采用分时间片的方式接收来自各证券商的申报数据,并按股票代码对申报数据分类.每台交易处理机(简称交易机)静态或动态地对若干种股票的申报数据进行撮合处理,前置机与交易机及交易机之间均可并行工作.下面我们来建立交易机处理系统的静态模型.

设某交易所下属 m 个证券商,有 k 台交易机和一台前置机,共处理 n 种股票的数据撮合,则交易所前置机静态处理子系统的 Petri 网模型如图 1 所示.库所 $SB1,SB2,\ldots,SBm$ 表示 m 个券商,并分别存放来自 m 个证券商的申报数据,每一个申报数据由一个标志表示.库所 $p_{11},\ldots,p_{1j1};\ldots;p_{k1},\ldots,p_{kjk}$ 表示 $n(n=j_1+\ldots+j_k)$种股票,且交易机(i)固定地处理 j_i 种股票 $p_{i1},\ldots,p_{iji}$ 的申报数据.如果库所 $pvi(1\le i\le m)$中有一个标志(称为控制标志),则表示库所 SBi 中的申报数据获得了前置机的处理优先权(privilege),只有得到优先权的数据才能被前置机处理.图中实线弧有一个可变权 $N(N$ 为正整数变量),同时表示申报数据的流向;虚线弧表示控制标志的流向且权为 1,虚圆圈表示控制库所,仅同一个变迁的输入和输出可变权弧具有相同的权 N,且 N 等于该变迁输入库所中的标志个数.变迁 t_{il} 的一次引发,从库所 p_0 中选取属于股票 p_{il} 的所有申报数据,并将它们转移到库所 p_{il} 中,$1\le l\le j_i,1\le i\le k$.为了确保前置机对各种股票数据处理的公平性,需要对图 1 中 Petri 网的动态行为作如下时序限制,对$\forall i:1\le i\le m$:



①交易机.

Fig.1 A subnet model of the prepositional computer static processing system

图 1 前置机静态处理子系统的 Petri 网模型

(T1): $\Box((t_{pvi})_{fir}\Rightarrow\neg SBi)$ (T2): $\Box((t_{SBi})_{fir}\Rightarrow\neg P_0)$

(T1)表明,如果券商 SBi 发送来的申报数据拥有处理优先权,前置机必须处理 SBi 数据,不允许引发变迁 t_{pvi} 将优先权传递给 $SB(i+1)$.(T2)保证一旦某券商的申报数据被处理,必须把它们传送到相应交易机后,才能处理另一券商数据.

图 2 模拟了交易机(i)$(1\le i\le k)$的申报数据撮合过程.仅标记"N"的弧具有可变权 N,其他弧的权为 1.根据交易规则,交易机在对某一种股票的申报数据撮合匹配时,总是选取买申报数据中拥有最高买价、最早到达时间的一个数据 B 和卖申报数据中拥有最低卖价、最早到达时间的一个数据 S,然后对它们进行撮合.若 B 的价格小于 S 的价格,则不能成交,但它们仍在交易机中等待再次撮合.反之,交易机对它们进行成交处理.当两股民的买卖股数不相等时,成交后的剩余部分也需保存在交易机中等待交易.p_{i-4} 和 p_{i-8} 分别存储等待交易的买、卖申报数据,p_{i-2} 和 p_{i-11} 分别存储撤消买、卖数据.当交易机(i)完成股票 p_{il} 的所有撮合处理后,p_{i-4} 和 p_{i-8} 中剩余的未成交数据将分别转存到 p_{il-2} 和 p_{il-3} 中,然后再进行另一种股票数据的撮合处理.同理,交易机(i)再次处理股票 p_{il} 的数据时,应首先将 p_{il-2} 和 p_{il-3} 中的数据分别转移到 p_{i-4} 和 p_{i-8} 中.当交易机接收到的数据中含有撤消买或卖申报数据时,应首先处理撤消数据,然后再进行撮合成交处理.因此,图 2 中 Petri 网的动态行为需要下列时序公式的约束,$\forall i,l,1\le l\le j_i,1\le i\le k$:

(T3): $\Box((t_{il-6})_{fir}\Rightarrow\neg p_{il})$

(T4): $\Box((t_{il-8})_{fir}\Rightarrow\neg p_{il-2}\cdot\neg p_{il-3})$

(T5): $\Box((t_{il-7})_{fir}\Rightarrow\neg p_{i-4}\cdot\neg p_{i-8})$

(T6): $\Box((t_{i-7})_{fir}\Rightarrow\neg p_{i-1}\cdot\neg p_{i-24}\cdot\neg p_{i-25})$

(T7): $\Box((t_{i-19})_{fir}\Rightarrow\neg p_{i-1}\cdot\neg p_{i-24}\cdot\neg p_{i-25}\cdot(\neg p_{i-4}+\neg p_{i-8}))$

(T8): $\Box((t_{i-24})_{fir}\Rightarrow\neg p_{i-7})$

(T3)的解释类似于(T1),由前面的分析可得到(T4)和(T5).(T6)意味着如果 p_{i-1} 中有撤消申报数据,则在撮合成交前,它们必须首先被撤除.若 p_{i-19} 中有标志,则表示交易机中的所有买卖申报数据都不符合成交条件.若 t_{i-19} 可引发,则意味着已不存在撤消申报数据,且剩余的买或卖数据至少有一方不存在,由此得到(T7).t_{i-20} 的一次引发,将 p_{i-5} 和 p_{i-9} 中两个数据的价格进行比较,若前者小于后者,则它们不符合成交条件,通过引发 t_{i-21},t_{i-4} 和 t_{i-14} 将它们分别送回 p_{i-4} 和 p_{i-8}.否则通过引发 t_{i-22},t_{i-8},t_{i-13} 和 t_{i-9},将成交结果和剩余部分(如果有剩余的话)传送到 p_{i-7}.若 t_{i-24} 可引发,则它引发后,将可能引起再一次撮合交易,而再次交易前需将剩余部分传回 p_{i-4} 或 p_{i-8},交易结果传送到 *TR*,故得到(T8).*TR* 和 *WD* 是券商处理系统中的库所.

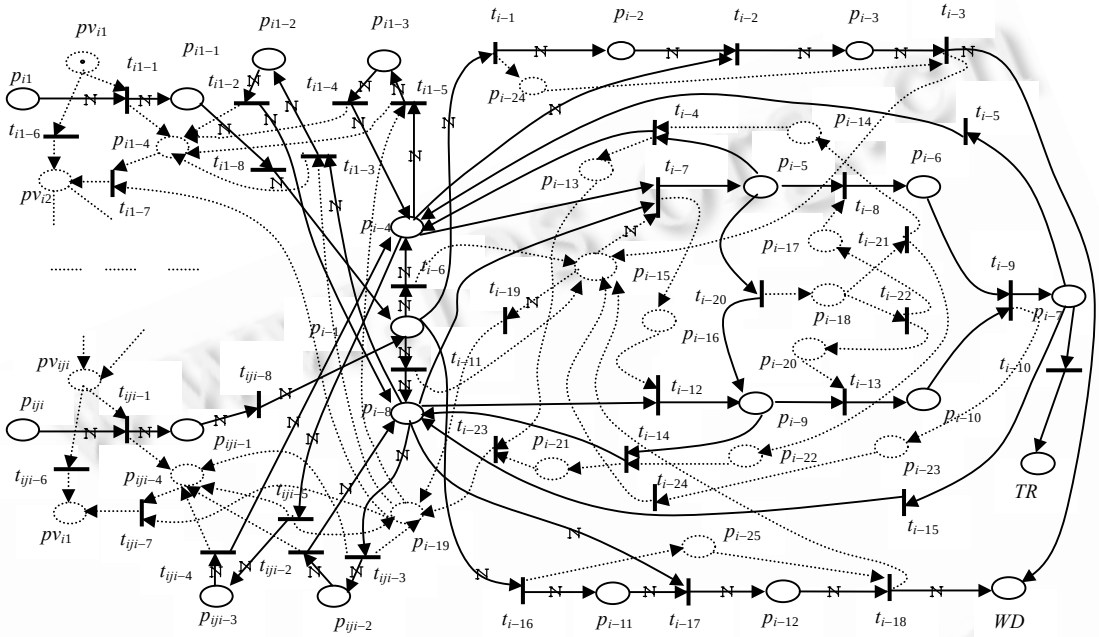


Fig.2 A subnet model of a trading processor (*i*) static processing system

图 2 交易机(*i*)静态数据撮合子系统 Petri 网模型

因此,静态证券交易系统的时序 Petri 网表示为 *TPNS*=(*NS*,*FS*),这里,*NS* 是由图 1 和图 2 中两个子网模型构成的 Petri 网.*FS* 是由(T1)~(T8)组成的时序公式组,是对 Petri 网 *NS* 动态行为的限制.

2.2 多处理机动态交易系统

在动态证券交易系统中,每个交易机处理股票的种类不再固定,而是面向所有股票.前置机动态处理子系统的 Petri 网模型与图 1 类似,仅将表示交易机(*i*)的矩形框与所有 *n* 种股票库所相连即可,每台交易机都有自己对各种股票的循环控制优先权,但当某种股票的申报数据正在被一台交易机处理时,如果前置机又传送来该种股票的交易数据,则其他交易机也不能处理这些数据,交易机之间的联系采用共享变量的分布式共享存储器方式实现,交易机动态数据撮合子系统的 Petri 网模型如图 3 所示.

$p_1,\ldots,p_n$ 为交易所处理的 *n* 种股票,$p_j(1\le j\le n)$中的申报数据被某台交易机处理后,剩余的买和卖申报数据分别存储在 p_{Bj} 和 p_{Sj} 中.如果库所 pr_j 中有一个标志,则表明 p_j 中的数据正在被某台交易机处理.当 p_{ij-2} 中有一个标志时,p_j 中的数据正被交易机(*i*)处理.库所 p_j,p_{Bj},p_{Sj} 和 pr_j 是 *k* 台交易机的共享库所,根据交易规则,图 3 的变迁可引发,除满足 Petri 网引发条件和(T5)~(T8)以外,还应满足时序公式:对 $1\le i\le k$,$1\le j\le n$:

(T9):$\Box((t_{ij-1})_{fir}\Rightarrow\neg pr_j)$ (T10):$\Box((t_{ij-6})_{fir}\Rightarrow\neg p_j)$ (T11):$\Box((t_{ij-8})_{fir}\Rightarrow\neg p_{Bj}\cdot\neg p_{Sj})$

基于前面的分析,容易得到(T9)~(T11)的解释.因此,动态交易系统的时序 Petri 网表示为 *TPND*=(*ND*,*FD*),这里 *ND* 是由类似于图 1 的网及图 3 构成的 Petri 网,*FD* 由公式组(T5)~(T11)组成.

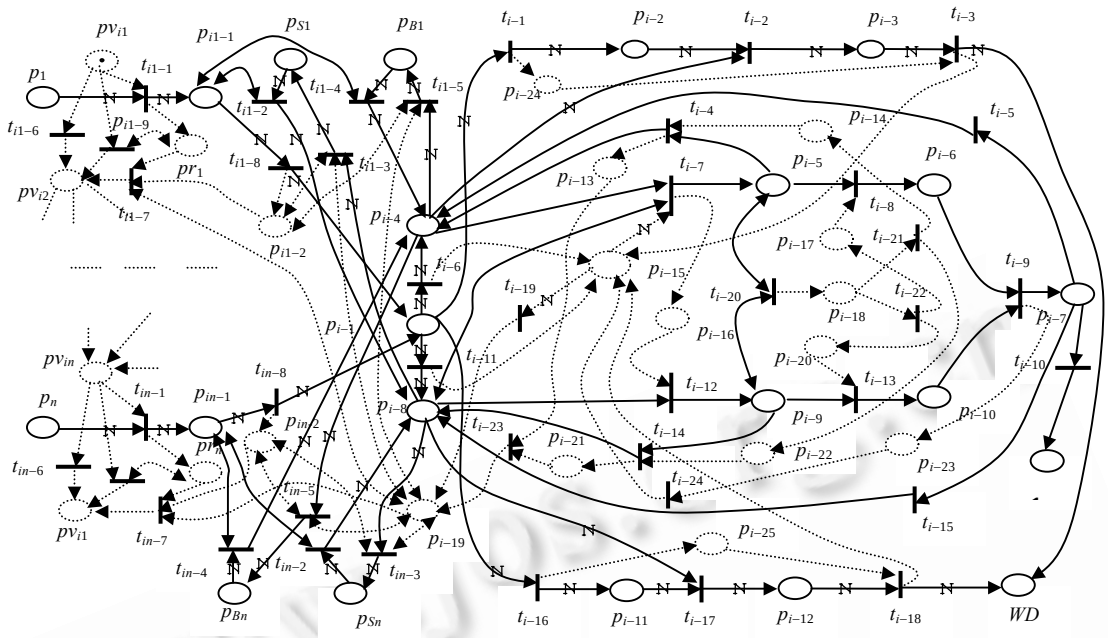


Fig.3 A subnet model of a trading processor (i) dynamic processing system

图 3 交易机(i)动态数据撮合子系统 Petri 网模型

3 证券交易系统的正确性分析与验证

在图 1 中,每个券商可并发地发送数据到前置机,前置机轮换地处理各券商的数据.因此,根据 $SBi(1\le i\le m)$中交易数据到达的随机性,假设 TPNS 的初始标识 M_0 除包含图 1 和图 2 中的控制标志以外,还包括 SBi 中的数据标志.$R(M_0)$表示 M_0 的可达标识集.本节引理的证明依据网结构容易完成,为节省篇幅,证明过程从略.

引理 **1**. (前置机对证券商的公平性:如果常常在无限个可达标识下 SBi 中至少有一个标志,则 t_{SBi} 必须常常无限次地引发)设 $M\in R(M_0)$,对 M 的任意一个引发序列α,$1\le i\le m$,有

$$\langle M,\alpha\rangle \vdash \Box\Diamond SBi \Rightarrow \Box\Diamond t_{SBi}.$$

引理 **2**. (交易机对各种股票数据的公平性)设 $M\in R(M_0)$,对 M 的任意引发序列α,$1\le l\le j_i$,$1\le i\le k$,有

$$\langle M,\alpha\rangle \vdash \Box\Diamond p_{il} \Rightarrow \Box\Diamond t_{il-1}.$$

引理 **3**. (安全性:任何时刻,在前置机中仅一个券商有处理优先权,在交易机(i)中仅一种股票的交易数据有撮合优先权)对 M 的任意一个引发序列α,$1\le u,l\le m$,$1\le i\le k$,且 $u\ne l$,有

$$\langle M,\alpha\rangle \vdash \Box(pvu \Rightarrow \neg pvl) \text{且} \langle M,\alpha\rangle \vdash \Box(pv_{iu} \Rightarrow \neg pv_{il}).$$

引理 **4**. (当交易机(i)开始处理某种股票的数据时,如果含有撤消申报数据,则在进行其他数据撮合之前,首先完成撤消申报数据的操作)设 $M\in R(M_0)$,对于 M 的任一引发序列α,$1\le i\le k$,有

$$\langle M,\alpha\rangle \vdash \Box((t_{i-1})_{fir}+(t_{i-16})_{fir} \Rightarrow \Box(\neg(t_{i-7})_{fi} \text{ until } (t_{i-3}+t_{i-18}))).$$

引理 4 表明,撤消申报数据比一般的买或卖数据有较高的处理优先权,这与交易规则是一致的.

引理 **5**. (若交易机(i)开始某种股票的数据撮合,则这个撮合过程重复执行,直至交易机(i)中所有待交易数据不满足交易条件为止)设 $M\in R(M_0)$,则对 M 的任一引发序列α,$1\le i\le k$,有

$$\langle M,\alpha\rangle \vdash \Box((t_{i-7})_{fir} \Rightarrow \Diamond p_{i-19}).$$

定理 **1**. (数据撮合系统的活性:如果某种股票得到交易优先权,则交易机(i)最终会将交易优先权移交给下一种股票)设 $M\in R(M_0)$,对 M 的任一引发序列α,$1\le l\le j_i$,$1\le i\le k$,有

$$\langle M,\alpha\rangle \vdash \Box(pv_{il} \Rightarrow \Diamond pv_{i(l+1)}).$$

证明:若 p_{il} 为空,则由(T3)及图 2 的网结构可知,通过引发 t_{il-6} 即可得到定理的结论.若 p_{il} 非空,则有

$$\langle M,\alpha\rangle \vdash \Box(pv_{il} \Rightarrow (t_{il-1})_{fir}), \quad (1)$$

$$\langle M,\alpha\rangle \vdash\Box(t_{il-1}\Rightarrow\bigcirc(p_{il-1}\cdot p_{il-4})). \tag{2}$$

如果交易机(i)在上次结束股票 p_{il} 的数据撮合时,尚有剩余的待交易数据,则 p_{il-2} 或 p_{il-3} 非空,由图 2 的网结构可知,通过引发 t_{il-2} 或 t_{il-4},可将其分别传送到 p_{i-8} 或 p_{i-4}.因此,假设 p_{il-2} 和 p_{il-3} 为空,由(T4)得

$$\langle M,\alpha\rangle\vdash\Box(p_{il-1}\cdot p_{il-4}\Rightarrow(t_{il-8})_{fir}), \tag{3}$$

$$\langle M,\alpha\rangle \vdash\Box(t_{il-8}\Rightarrow\bigcirc(p_{il-4}\cdot p_{i-1})), \tag{4}$$

$$\langle M,\alpha\rangle\vdash\Box(p_{il-4}\cdot p_{i-1}\Rightarrow(t_{i-1})_{fir}+(t_{i-16})_{fir}+(t_{i-6})_{fir}+(t_{i-11})_{fir}). \tag{5}$$

由式(5)及公式(f)得

$$\langle M,\alpha\rangle\vdash\Box(p_{il-4}\cdot p_{i-1}\Rightarrow(t_{i-6})_{fir}+(t_{i-11})_{fir}), \tag{6}$$

或

$$\langle M,\alpha\rangle\vdash\Box(p_{il-4}\cdot p_{i-1}\Rightarrow(t_{i-1})_{fir}+(t_{i-16})_{fir}). \tag{7}$$

有 3 种情况:仅式(6)成立;仅式(7)成立;式(6)和式(7)都成立.现仅讨论式(6)有效的情况,其他可类似处理.由式(6)及式(f)得

$$\langle M,\alpha\rangle \vdash\Box(t_{i-6}+t_{i-11}\Rightarrow\bigcirc((p_{i-4}+p_{i-8})\cdot p_{i-15}\cdot p_{il-4}\cdot\neg p_{i-1})). \tag{8}$$

根据假设,p_{i-24} 和 p_{i-25} 是空的,若 p_{i-4} 和 p_{i-8} 至少一个是空的,则由引理 4、(T7)、式(1)~(6)、式(8)及 PR4 得

$$\langle M,\alpha\rangle \vdash\Box(pv_{il}\Rightarrow\Diamond(p_{i-19}\cdot p_{il-4})). \tag{9}$$

若 p_{i-4} 和 p_{i-8} 均非空,由式(8)及(T6)得

$$\langle M,\alpha\rangle\vdash\Box((p_{i-4}+p_{i-8})\cdot p_{i-15}\cdot p_{il-4}\cdot\neg p_{i-1}\Rightarrow(t_{i-7})_{fir}). \tag{10}$$

根据式(1)~(6)、式(8)、式(10)、引理 5 及 PR4 得到式(9)也是有效的,此时,若 p_{i-4} 或 p_{i-8} 非空,则 t_{il-5} 或 t_{il-3} 可引发,故不妨设 p_{i-4} 和 p_{i-8} 是空的.因此,由式(9)及(T5)得

$$\langle M,\alpha\rangle\vdash\Box(p_{i-19}\cdot p_{il-4}\Rightarrow(t_{il-7})_{fir}), \tag{11}$$

$$\langle M,\alpha\rangle \vdash\Box(t_{il-7}\Rightarrow\bigcirc pv_{i(l+1)}). \tag{12}$$

由式(9)、式(11)、式(12)、PR1 和 PR2 知,定理结论成立. □

定理 **2**. 时序 Petri 网 TPNS 是活的、有界的和公平的.

定理 **3**. 时序 Petri 网 TPNS 的动态行为与静态证券交易系统的需求规范是一致的.

对动态交易系统模型作类似的分析,可得到相似的结论.下面给出动态交易系统的一个定理.

定理 **4**. (在动态交易系统中,一种股票获得交易优先权,则在对它的数据撮合匹配完成后,一定释放优先权)设 M_0 是 TPND 的一个初始标识,$M\in R(M_0)$,则对 M 的任一引发序列 α,$1\le j\le n$,$1\le i\le k$,有

$$\langle M,\alpha\rangle \vdash\Box(p_j\cdot pv_{ij}\cdot\neg pr_j\Rightarrow\Diamond pv_{i(j+1)}).$$

4 结论及进一步研究的问题

本文给出了静态和动态证券交易系统的时序 Petri 网模型,从形式上证明了交易系统需求规范与其模型动态行为的一致性,以及所模拟交易系统的正确性、活性和安全性.事实证明,时序 Petri 网可作为并发系统形式描述和分析的重要工具,特别适合描述并发系统中某些与时间有关的重要性质.时序 Petri 网的不完美之处是不能明确地表达数据项的值及其类型.因此,交易数据的价格及所属何种股票都没有表示出来.但是,如果需要这些性质,可将 Petri 网扩充为高级 Petri 网,如谓词/变迁网[9]或有色 Petri 网[10].在动态交易系统网模型中,每台交易机处理所有股票的数据撮合,这样可能导致交易机花费过长的时间去寻找交易数据.为此,可采用静态和动态相结合的交易方式,即将 n 种股票分成 k 部分,分别固定分派到 k 台交易机上,当某台交易机空闲时,再去访问另一台交易机的申报数据,可用分布式共享内存或共享变量的方法实现交易机之间的互访.此时,本文的分析方法仍然有效.我们将进一步研究用随机 Petri 网对动态和静态证券交易系统进行性能分析和评价,发现系统存在的问题,提出改进建议和策略,使证券交易系统更加公平和有效.

References:

[1] Suzuki, I. Formal analysis of the alternating bit protocol by temporal Petri nets. IEEE Transactions on Software Engineering, 1990, 16(11):1273~1281.

[2] Zurawski, R. Verifying correctness of interfaces of design models of manufacturing systems using functional abstractions. IEEE Transactions on Industrial Electronics, 1997,44(3):307~320.

[3] Suzuki, I., Lu, H. Temporal Petri nets and their application to modeling and analysis of a handshake daisy chain arbiter. IEEE Transactions on Computers, 1989,38(5):696~704.

[4] Murata, M. Petri nets: properties, analysis and applications. Proceedings of the IEEE, 1989,77(4):541~580.

[5] Coolhan, E., Jr Roussopoulos, N. Timing requirements for time-driven systems using augmented Petri nets. IEEE Transactions on Software Engineering, 1983,SE-9(6):603~616.

[6] Berthomieu, B., Diaz, M. Modeling and verification of time dependent systems using time Petri nets. IEEE Transactions on Software Engineering, 1991,17(3):259~273.

[7] Manna, Z., Pnueli, A. The temporal logic of reactive and concurrent systems. In: Specification. New York: Springer-Verlag, 1992.

[8] Stirling, C. Model and temporal logics. In: Abramsky, S., Gabby, D.M., Maibaum, T.S.E., eds. Handbook of Logic in Computer Science. Oxford: Oxford University Press, 1992. 477~563.

[9] Murata, T., Zhang, D. A predicate-transition net model for parallel interpretation of logic programs. IEEE Transactions on Software Engineering, 1988,14(4):481~497.

[10] Jensen, K. Colored Petri nets. Vol 1, New York: Springer-Verlag, 1992.

Description and Verification of an Online Stock Trading System by Using Temporal Petri Nets*

DU Yu-yue[1,2,3], JIANG Chang-jun[1]

[1](*Department of Computer Science and Engineering, Tongji University, Shanghai* 200092, *China*);

[2](*Department of Computer Science, Liaocheng Teachers University, Liaocheng* 252059, *China*);

[3](*Key Laboratory of Computer Science, Institute of Software, The Chinese Academy of Sciences, Beijing* 100080, *China*)

E-mail: yydu001@163.com; cjjiang@online.sh.cn

http://www.tongji.edu.cn

Abstract: The modeling, formal description and correctness verification of online static and dynamic stock trading systems, based on Shanghai Stock Exchange, are shown by using temporal Petri nets in order to make online stock trading systems more effective and rational. In the temporal Petri net models of the given static and dynamic systems, two types of tokens, namely data tokens representing trading data and control tokens used for keeping trading rules, are introduced. And the temporal constraint formulae are clearly and compactly represented by means of functional requirements of stock trading systems. The consistency between the functional requirements specifications of the online static and dynamic stock trading systems and the dynamic behavior of the temporal Petri net models is formally proved by means of the temporal logic operators to express temporal assertions. Also, certain primary properties of the temporal Petri net models are described and analyzed, such as liveness, fairness and safeness properties. It is further confirmed that temporal Petri nets are a promising describing and analyzing tool of discrete-event dynamic concurrent systems, and can describe explicitly certain time-related fundamental properties of concurrent systems, such as eventuality and fairness. Finally, the further study subjects are found.

Key words: model checking; stock trading system; temporal logic; Petri net; formal description; correctness verification; electronic commerce

* Received July 10, 2001; accepted November 26, 2001

Supported by the National Natural Science Foundation of China under Grant No.69973029, 69933020; the National Grand Fundamental Research 973 Program of China under Grant No.G1998030604; the Foundation of the Key Laboratory of Computer Science, Institute of Software, The Chinese Academy of Sciences under Grand No.SYSKF0205