

时间约束

Petri网

可调度性

实时系统

(6)

计算机科学 2000Vol. 27No. 3

18-21

时间约束 Petri 网的可调度性分析研究

Studies about Schedulability Analysis of Timing Constraint Petri Nets

李慧芳 李人厚

TP18 TP316.2

(西安交通大学系统工程研究所 西安 710049)

Abstract The timing constraint Petri nets are a class of Petri nets which have general time constraints. At present, the studies about state reachability of TCPN's are only restricted to some simple nets. This paper gives more general analysis method of reachability, and discusses the analysis of schedulability of TCPN's with general topology structure through deeply investigating the TCPN's.

Keywords Timing constraint Petri nets, Petri nets, Schedulability analysis, Decision variables

1 引言

时间约束 Petri 网^[1] (Timing Constraint Petri Nets, TCPN's) 是具有广义时间约束的 Petri 网, 它综合了时间 Petri 网^[2,3] (Time Petri Nets) 和赋时 Petri 网^[4] (Timed Petri Nets) 的共同特点, 具有经典 Petri 网的理论基础和额外的时间约束能力。在实时系统建模中, 它可对其它与时间有关的 Petri 网所不能描述的冲突结构进行建模和分析。TCPN's 使用弱触发规则, 即使能的变迁可触发也可不触发, 完全由调度者决定。Tasi^[1] 借助于可调度分析, 讨论了 TCPN's 在实时系统规格说明验证中的应用。时间约束的引入使网的状态演化更加复杂, 从而使文[1]有关可调度分析的概念及结论产生错误。本文修正了文[1]所得的结论, 完整地给出了 TCPN's 的可达性分析方法, 以适用于更一般的 TCPN's; 通过分析网的拓扑结构, 给出了变迁可调度情况下决策变量的求取; 在状态可达时, 可求得调度者的决策范围, 从而控制网的动态行为。

2 TCPN's 及其触发规则

时间约束 Petri 网是一个 6 元组 (P, T, F, TC, D, M_0) , 其中 (P, T, F, M_0) 是基网, P 为库所集, T 为变迁集, F 是流关系, TC 是整数对 $(TC_{min}(pt), TC_{max}(pt))$ 组成的集合, 这里 pt 可以是库所, 也可以是变迁。D 是 $FIRE_{dur}(t)$, 表示变迁 t 的触发延迟时间。 M_0 为初始标记。库所时间对 $(TC_{min}(p_i), TC_{max}(p_i))$, 表示当 p_i 中的托肯到达后, 用于使其输出变迁的时间范围。如果托

肯到达时刻为 $TOKEN_{arr}(p_i)$, 则它只能在 $(TOKEN_{arr}(p_i) + TC_{min}(p_i), TOKEN_{arr}(p_i) + TC_{max}(p_i))$ 时间区间内, 使其输出变迁。变迁时间对 $(TC_{min}(t), TC_{max}(t))$, 表示当变迁 t 使能后, 可触发的时间范围。如果 t 的使能时间为 T_0 , 则 t 在 $(T_0 + TC_{min}(t), T_0 + TC_{max}(t))$ 时间范围内可触发。一个变迁可触发却不一定能成功地完成触发, 因为它需要时延 $FIRE_{dur}(t)$ 。设 p_i 为 t 的输入库所, 则变迁 t 的实际可触发时间区间由 $TOKEN_{arr}(p_i)$ 、 $TC_{min}(p_i)/TC_{max}(p_i)$ 及 $TC_{min}(t)/TC_{max}(t)$ 共同决定。当输入库所中有多个托肯时, 可按选择规则(先进先出、颜色匹配等)使其输出变迁。

根据弱触发规则, 使能变迁的实际触发由调度者决定。所有用于使能变迁 t 的托肯 $TK's$ 在 t 的触发过程中被“消耗”, 当 t 成功地完成触发时, 便向 t 的输出库所中输出相应数目的托肯。如果 t 没有成功地完成触发, 则 $TK's$ 被放回原库所。如果由 $TK's$ 使能的所有变迁都未成功地完成触发, 则 $TK's$ 在其相应的库所中变为死托肯。TCPN's 的分析方法基于绝对与相对时间模式, 特别适合于具有冲突结构(优先权、决策及结构选择)系统的建模与分析。为方便讨论, 假定: 系统的全局时钟为 $Clock$, $FIRE_{enbld}(t)$ 是变迁 t 的使能时间, $EEBT(t)/LEET(t)$ 表示 t 的最早使能开始/最晚使能结束时间, $EFTB(t)/LFET(t)$ 是 t 的最早触发开始/最晚触发结束时间, $FIRE_{begin}(t)/FIRE_{end}(t)$ 是 t 的实际触发开始/触发结束时间。 $IP(t)/OP(t)$ 是变迁 t 的输入/输出库所集合, $IT(p_i)/OT(p_i)$ 是库所 p_i 的输入/输出变迁集合。

李慧芳 博士生, 研究方向为离散事件动态系统, 化工批处理过程调度。李人厚 教授, 博导, 研究方向为智能控制理论与方法、智能制造系统调度, 多媒体与 CSCW 理论及应用。

3 TCPN's 的可达性分析

定义 1 在某一标记 M 下,使能的变迁 t 可触发,如果 $LFET(t) - EFBT(t) \geq 0$;使能的变迁 t 可成功地完成触发,如果 $LFET(t) - EFBT(t) \geq FIRE_{Dur}(t)$ 。

定义 2 在某一标记 M 下,变迁 t 可成功地完成触发时,变迁 t 是可调度的。

当考虑 $TOKEN_{arr}(p_i)$ 时,如果变迁 t 可成功地完成触发,则称变迁 t 是强可调度的;不考虑 $TOKEN_{arr}(p_i)$ 时,变迁 t 可调度称为弱可调度。

3.1 EFBT(t)/LFET(t) 的计算

设 $p_i \in IP(t)$, 则 t 的 $EEBT(t)/LEET(t)$ 受其所有输入库所中托肯的使能时间约束,即有:

$$EEBT(t) = \max[TOKEN_{arr}(p_i) + TC_{min}(p_i)] \quad (1)$$

$$LEET(t) = \min[TOKEN_{arr}(p_i) + TC_{max}(p_i)] \quad (2)$$

定理 1 设 $p_i \in IP(t)$, 则变迁 t 可成功完成触发的必要条件为:

$$LEET(t) - EEBT(t) \geq FIRE_{Dur}(t) \quad \text{以及}$$

$$TC_{max}(t) - TC_{min}(t) \geq FIRE_{Dur}(t)$$

证明:由于 $(EEBT(t), LEET(t))$ 给出了变迁 t 被所有输入库所共同使能的时间区间,且在 t 触发后,使能 t 的托肯被保持,因此托肯的保持时间应足以使 t 持续地完成触发,即 $LEET(t) - EEBT(t) \geq FIRE_{Dur}(t)$ 。另一方面,如果变迁 t 可成功地完成触发,有: $FIRE_{begin}(t) \geq TC_{min}(t) + FIRE_{enabled}(t)$, $FIRE_{end}(t) \leq TC_{max}(t) + FIRE_{enabled}(t)$, 可是 $FIRE_{end}(t) - FIRE_{begin}(t) = FIRE_{Dur}(t)$, 所以 $TC_{max}(t) - TC_{min}(t) \geq FIRE_{Dur}(t)$ 。

定理 2 设 $p_i \in IP(t)$, 在某一使能标记 M_i 下,如果变迁 t 强可调度,那么 $EFBT(t)/LFET(t)$ 可由 (3)、(4) 式给出,且 $LFET(t) - EFBT(t) \geq FIRE_{Dur}(t)$ 。

$$EFBT(t) = EEBT(t) + TC_{min}(t) \quad (3)$$

$$LFET(t) = LEET(t) \quad (4)$$

证明:如果变迁 t 可触发,当且仅当它被每一输入库所使能,并且在使能后,经过 $TC_{min}(t)$ 个时间单位便可触发,所以 t 的最早开始触发时间 $EFBT(t) = EEBT(t) + TC_{min}(t)$ 。

一旦变迁 t 的任一个输入库所停止使能,它将立即停止触发,所以 $LFET(t) \leq LEET(t)$ 。另外 t 可成功地完成触发还应满足自身的时间约束,即 $LFET(t) \leq FIRE_{enabled}(t) + TC_{max}(t)$ 。由于 t 的使能时间约束: $EEBT(t) \leq FIRE_{enabled}(t) \leq LEET(t)$, 通过选择不同的使能时刻来调度 t , 可能导致 $FIRE_{end}(t) > LEET(t)$ 或 $FIRE_{end}(t) \leq LEET(t)$ 两种情况。在前者中, t 必然不能成功地完成触发,而后者中,在 t 结束触发后,其输

入库所仍继续使能。变迁 t 的实际触发由调度者决定,为了给调度者留有足够的决策范围,应使 $LFET(t) = LEET(t)$ 。由定义 1 可知,变迁 t 强可调度时,必须满足 $LFET(t) - EFBT(t) \geq FIRE_{Dur}(t)$ 。

3.2 TCPN's 的可达性分析

在 TCPN's 中,如果标记 M_n 从 M_0 可达,则至少存在一个触发序列 $\sigma = (M_0 t_1 M_1 t_2 M_2 \dots t_i M_i \dots t_n M_n)$ 或 $\sigma = (t_1 t_2 \dots t_i \dots t_n)$, 可将 M_0 转换为 M_n , 记为 $M_2[\sigma > M_n]$ 。由于时间约束的增加,当且仅当 σ 中的所有变迁 t_i 至 t_n 相对于 M_0 强可调度, M_n 才是可达的。由定理 1、2 可得可调度性的几个结论:

(1) 如果变迁 t 的真正使能时间区间非空,则 t 可触发。

如图 1 所示,设 $TOKEN_{arr}(p_1) = 2, TOKEN_{arr}(p_2) = 0$, 考察变迁 t 的可触发性。按文[1]的结论有: $EFBT(t) = \max(2 + 0, 0 + 3) + TC_{min}(t) = 4$; $LFET(t) = \min(2 + \min(2, 3), 0 + \min(5, 3)) = 3$, $LFET(t) - EFBT(t) = -1 < 0$, 所以 t 不可触发。实际上,由式 (1)、(2) 知: $EEBT(t) = \max(2 + 0, 0 + 3) = 3$, $LEET(t) = \min(2 + 2, 0 + 5) = 4$, 所以变迁 t 的真正使能时间区间为 $(3, 4)$, t 有可能触发。而且由式 (3)、(4) 知: $EFBT(t) = EEBT(t) + 1 = 4$, $LFET(t) = LEET(t) = 4$, $LFET(t) - EFBT(t) \geq 0$, t 可触发。当然 t 能否成功地完成触发,还取决于 $FIRE_{Dur}(t)$ 。本例中变迁 t 可触发,却不能成功地完成触发。

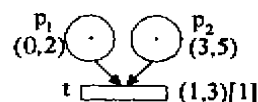


图 1

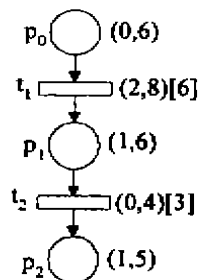


图 2

(2) 变迁 t_n 可触发的必要条件是 t_n 的上游变迁 t_{n-1} 强可调度。

如图 2 所示,设 $TOKEN_{arr}(p_0) = T_0$, 分析从初始标记 $M_0 = (p_0)$ 至 $M_3 = (p_1)$ 的可达性。按文[1]的结论知: 变迁 t_2 强可调度。但是其上游变迁 t_1 不可调度, 因

为 t_1 开始触发后的实际使能时间小于 $FIRE_{Dur}(t_1)$, 即 $LEET(t_1) - EFBT(t_1) = T_0 + 6 - (T_0 + 2) = 4 < FIRE_{Dur}(t_1) = 6$. 由公式(1)~(4)知, $LFET(t_1) - EFBT(t_1) = 4 < FIRE_{Dur}(t_1) = 6$, t_1 不可调度, 必然 t_2 不可调度. 由此可见, 利用文[1]的结论, 当 t_n 强可调度时, 并不能保证 t_n 的上游变迁 $t_i (i=1, \dots, n-1)$ 都强可调度. 事实上, 文[1]在计算 $EFBT(t_i)/LFET(t_i)$ 时, 没有考虑 t_i 的上游变迁 $t_k (k=1, 2, \dots, i-1)$ 是否能成功地完成触发. 定理1给出了 t_i 可成功地完成触发的必要条件, 即使必要条件满足, 也可能由于 $TC_{max}(t_i)$ 的约束导致 t_i 在实际开始触发后的持续使能时间小于 $FIRE_{Dur}(t_i)$, 从而 t_i 不能成功地完成触发. 作者认为, 要分析 M_n 的可达性, 必须从 M_0 出发, 利用公式(1)~(4)依次考察其上游变迁 $t_1 t_2 \dots t_n$ 的可调度性.

(3) 弱可触发并不是强可触发的必要条件.

由文[1]知, 强可调度 $\rightarrow$ 强可触发 $\rightarrow$ 弱可触发. 设 $p_i \in IP(t)$, 如果不考虑 $TOKEN_{arr}(p_i)$, 则 p_i 中的托肯使能变迁 t 的时间区间为 $(TC_{min}(p_i), TC_{max}(p_i))$, 仅当变迁 t 被其所有输入库所中的托肯同时使能时, t 才可能触发. 如果考虑 $TOKEN_{arr}(p_i)$, 则 p_i 中的托肯使能 t 的时间区间为 $(TOKEN_{arr}(p_i) + TC_{min}(p_i), TOKEN_{arr}(p_i) + TC_{max}(p_i))$. 不同的输入库所可能具有不同 $TOKEN_{arr}(p_i)$, 因此它们使能输出变迁 t 的时间区间不同, 仅当 $LEET(t) \geq EFBT(t)$ 时, 变迁 t 才被真正使能. 在图1中, 不考虑 $TOKEN_{arr}(p_j) (j=1, 2)$ (即 $TOKEN_{arr}(p_i) = 0$) 时, 由式(1)~(4)有: $LFET(t) - EFBT(t) = 2 - (3 + 1) = -2 < 1$, 即 t 不是弱可触发; 设 $TOKEN_{arr}(p_1) = 2, TOKEN_{arr}(p_2) = 0$, 由前面(1)的分析可知, 变迁 t 强可触发, 如果 $FIRE_{Dur}(t) = 0$, 则 t 强可调度. 可见, 强可调度必然强可触发, 而强可触发未必弱可触发.

4 TCPN' s 变迁可调度的决策范围

从前面的讨论可知, $p_i \in IP(t)$ 中使能 t 的每一个托肯的状态是与系统时间动态相关的, 如用 ID 表示托肯标识, 当其使能的变迁 t 触发后, $ID=1$, 当 t 触发失败后, 所有被释放的托肯状态中, $ID=0$. 每一托肯的状态可表示如下:

$TOKEN \langle TOKEN_{arr}(p_i), TOKEN_{enabled_{dur}}(p_i), TOKEN_{enabled_{end}}(p_i), ID \rangle$

当一个托肯到达库所 p_i 时, 有

$TOKEN_{enabled_{dur}}(p_i) = TOKEN_{arr}(p_i) + TC_{min}(p_i) \quad (5)$

$TOKEN_{enabled_{end}}(p_i) = TOKEN_{arr}(p_i) + TC_{max}(p_i) \quad (6)$

在某一标记 M 下, 变迁 t 的使能时间约束由其所有输入库所中托肯的使能时间给出:

• 20 •

$FIRE_{enabled}(t) \in (MAX(TOKEN_{enabled_{dur}}(p_i)),$

$MIN(TOKEN_{enabled_{end}}(p_i))) \quad (7)$

此时 t 的 $EFBT(t)/LFET(t)$ 可表示如下:

$EFBT(t) = MAX[TOKEN_{enabled_{dur}}(p_i)] + TC_{min}(t) \quad (8)$

$LFET(t) = MIN[TOKEN_{enabled_{end}}(p_i)] \quad (9)$

弱触发规则意味着使能变迁的实际触发取决于调度者. 在实时系统规范验证中, 我们关心的是: 使能的变迁 t 可成功地完成触发时, 调度者的决策范围.

定义3 在某一标记 M 下, 变迁 t 可调度时, 如果用 $D(t)$ 表示 t 的决策延时变量, $UD(t)$ 表示 t 的决策延时上界, 则调度者的可决策范围是

$0 \leq D(t) \leq UD(t) = LFET(t) - EFBT(t) - FIRE_{Dur}(t)$

这时变迁 t 的实际开始触发时间, 可由下式计算

$FIRE_{begin}(t) = D(t) + EFBT(t) \quad (10)$

当变迁 t 触发后, 所有使能 t 的托肯, 其 $ID=1$. 如果 t 成功地完成触发, 则 $\forall p_i \in OP(t)$, 其托肯的到达时间为 $TOKEN_{arr}(p_i) = FIRE_{end}(t)$. t 不能成功完成触发, 有两个原因: 一是 t 本身强可调度, 因 $D(t)$ 的选择超界而使 t 未能成功完成触发; 二是 t 不可调度, 但是当 t 触发失败时, 其停止触发时间总是 $LEFT(t)$, 一个有效的系统规范应避免第二种情况.

如果取 $D(t) > UD(t)$ 来调度 t , 则 $FIRE_{end}(t) = FIRE_{begin}(t) + FIRE_{Dur}(t) > LEFT(t)$, 这时变迁 t 不能成功地完成触发. 由 t 释放的 TK's 被放回原库所, 且可用于 t 的冲突变迁的触发, 这正是 TCPN' s 在实时系统建模中的独特优点. 在全局时钟 Clock 下, 设 t 在 τ 时刻终止触发, 则 $\tau = LFET(t)$, 所有被 t 释放的 TK's, 其 $ID=0$, 且使能时间修正为

$TOKEN_{enabled_{dur}}(p_i) = \tau + 1$, 其中 $p_i \in IP(t) \quad (11)$

5 决定变量的选取原则

对一个有效的系统规范, 在相应 TCPN' s 中, M_0 必须是从 M_0 可达的. PN' s 和 TCPN' s 在可达性上具有不同的行为. 时间约束的引入, 使一个 PN' s 模型中可达的标记 M_n , 在 TCPN' s 中未必是可达的. 在 PN' s 模型中, 如果存在一变迁序列 σ , 且 σ 中的所有变迁至少触发一次后, 可将 M_0 转换为 M_n . 则 M_n 是可达的. 然而在 TCPN' s 中增加了时间约束, 如 $TC_{max}(t_i) \geq TC_{min}(t_i)$ 及 $TC_{max}(t_i) - TC_{min}(t_i) \geq FIRE_{Dur}(t_i)$ 等, 根据 TCPN' s 建模的定义, σ 中的变迁可能不可触发或不可调度. 如 σ 中的一个变迁不可调度, 则 M_n 就是不可达的. 所以在 TCPN' s 中, 要使标记 M_n 从 M_0 可达, 必须证明 σ 中的所有变迁 t_1 至 t_n 相对于 M_0 强可调度. 由于 $p_i \in OP(t_{i-1})$ 中托肯的到达时间与 t_{i-1} 的调度决

策 $D(t_{n-1})$ 的选取有关, 因此要分析 M_i 至 M_n 的可达性, 必须依次考察 M_n 的上游变迁 $t_1 t_2 \cdots t_n$ 的可调度性。因网结构的不同, $D(t_{n-1})$ 的选取原则也不一样, 有下面几种情况 (设网中所有的变迁都满足定理1的条件):

(1) 每个变迁只有一个输入、输出库所, 每个库所只有一个输入、输出变迁

如图2所示, 设 t_1 强可调度, 且 t_1 的可调度决策上界 $UD(t_1)$, 由于 $TOKEN_{arr}(p_1)$ 取决于 $D(t_1)$ 的选取, 所以 $TOKEN_{arr}(p_1) = D(t_1) + EFBT(t_1) + FIRE_{D_{arr}}(t_1)$, 进一步可得 $EFBT(t_2) = TOKEN_{arr}(p_1) + TC_{max}(p_1) + TC_{max}(t_2)$, $LFET(t_2) = TOKEN_{arr}(p_1) + TC_{max}(p_1)$, $UD(t_2) = LFET(t_2) - EFBT(t_2) - FIRE_{D_{arr}}(t_2)$, 所以 $UD(t_2)$ 与 $D(t_1)$ 无关, 即在 t_1 可调度决策范围内, $D(t_1)$ 的选取不影响 t_2 的可调度性, 这时可按系统的协调控制要求, 依次在各自的取值范围内选取 $D(t_1)$ 、 $D(t_2) \cdots D(t_{n-1})$ 。

(2) 一个变迁有多个输入库所

如图3所示, 设 t_{11} 、 t_{12} 强可调度, 且决策变量的取值上界为 $UD(t_{11})$ 、 $UD(t_{12})$, 则 $D(t_{11})$ 、 $D(t_{12})$ 的不同取值直接影响 p_{11} 、 p_{12} 中托肯的到达时间 $TOKEN_{arr}(p_k)$ ($k=1, 2$), 可是 p_{11} 、 p_{12} 中的托肯到达后, 使能 t_2 的时间区间 $(TOKEN_{arr}(p_k) + TC_{max}(p_k), TOKEN_{arr}(p_k) + TC_{max}(p_k))$, 在 $i=1, 2$ 时的交集为 t_2 的真正使能区间。因此这时 $D(t_{11})$ 、 $D(t_{12})$ 的选取原则是: 兼顾系统协调控制要求的同时, 尽量使 t_2 的真正使能时间长, 为 t_2 的调度决策留有足够的裕量。

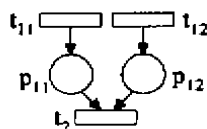


图3

(3) 一个库所有多个输入变迁

如图4所示, t_{11} 、 t_{12} 触发结束后向 p_1 中输出的托肯具有不同的到达时间, 且与 $D(t_{11})$ 、 $D(t_{12})$ 有关。设 p_1 中到达的托肯以先进先出的原则使能输出变迁, 则 $D(t_{11})$ 、 $D(t_{12})$ 的选取原则是: 满足系统的协调控制, 并

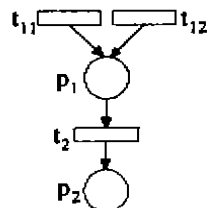


图4

应尽量使 p_1 的真正使能时间早, 以满足实时系统的快速性。

(4) 冲突结构

TCPN' s 对冲突结构的建模是在于采用弱触发模式, 为冲突变迁赋予不同的截止触发时间, 可表示它们被同一托肯使能时可触发的优先权, 截止时间早的变迁优先触发。图5中 t_{22} 比 t_{21} 优先触发。如果变迁序列 σ 中的某一变迁处于冲突结构中, 则调度问题必须考虑可触发的优先权。考察图5中 $M(p_2)$ 的可达性, 在相应的 PN' s 中, M_0 至 $M(p_2)$ 的可达路径为 $(t_1 t_{21})$, 而 TCPN' s 中, t_{21} 的触发是在 t_{22} 成功完成触发失败后, 所以实际的可达路径为 $(t_1 t_{22} t_{21})$, t_{22f} 表示 t_{22} 触发失败。在 t_{22} 触发失败后, p_1 中被释放托肯的到达时间为 $\tau = FIRE_{end}(t_{22f}) + 1$, 且 $\tau = \tau(D(t_1))$, 该托肯可继续使能变迁 t_{21} , 此时 t_{21} 的调度决策不仅要考虑其上游变迁 t_1 , 还要考虑冲突变迁 t_{22} 。

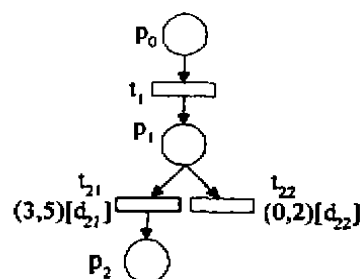


图5

结论 深入研究了 TCPN' s 的可达性, 完善了 TCPN' s 的调度分析技术, 针对网的不同拓扑结构, 给出了决策变量的选取原则; 实时系统的调度是动态决策的过程, 对含冲突结构网的可达性分析, 充分体现了 TCPN' s 对实时系统复杂性的建模能力。

参考文献

1. Tasi J J P, Yang S J. Timing Constraint Petri Nets and Their Application to Schedulability Analysis of Real-Time System Specifications. IEEE Trans. Software Engineering, 1995, 21(1): 32~49
2. Serthomeu B, Diaz M. Modelling and Verification of Time Dependent Systems Using Time Petri Nets. IEEE Trans. Software Engineering, 1991, 17(3): 259~273
3. Joel T, et al. Time Constraints Verification Methods Based on Time Petri Nets. In: Proc. of the IEEE Computer Society Workshop on Future Trends of Distributed Computing Systems, 1997. 262~267
4. Baopu L, Anthony R. TipNet: a Graphical Tool for Timed Petri Nets. International Workshop on Petri Nets and Performance Models, 1995. 212~213 Specification