第四章基于属性的软件可信性度量模型

陈仪香

2024年10月22日

Outline

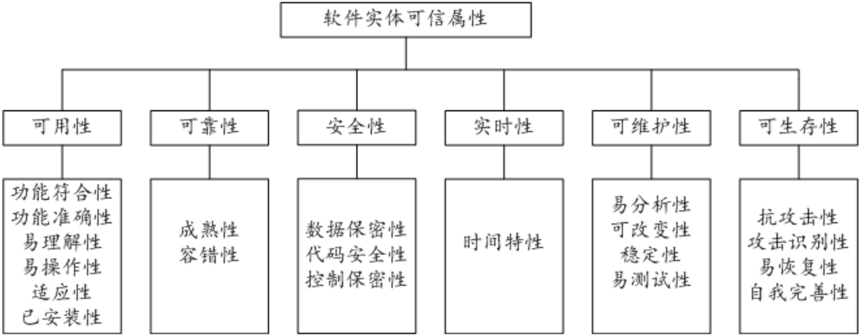
第4章基于属性的软件可信度量模型

本章介绍基于多维属性的软件可信性度量性质集和基于属性分解的软件可信性度量性质集。依据公理化方法分别建立基于属性的软件可信性度量模型、基于属性划分的软件可信性度量模型和基于属性分解的软件可信性度量模型。

分层原因

构成不同高层次属性的低层次属性集合的交集可能非空，
这样各高层次属性间可能并不是毫不相关的，
意味着属性之间可以发生替代。

软件可信属性分解模型


软件实体可信属性
可用性
可靠性
安全性
实时性
可维护性
可生存性
功能符合性
功能准确性
易理解性
易操作性
适应性
已安装性
成熟性
容错性
数据保密性
代码安全性
控制保密性
时间特性
易分析性
可改变性
稳定性
易测试性
抗攻击性
攻击识别性
易恢复性
自我完善性

Let T be a metric function w.r.t. $y_1, \cdots, y_m$ for the trustworthiness of software.

$$T = f(y_1, y_2, \cdots, y_m)$$

Metric criteria for the multi-dimensional trustworthiness of software:

(1) **Non-negativity**

$$T \geq 0$$

(2) 比例合适性：比例合适性是指各可信属性值应该有合适比例假设。

软件可信性是软件客观质量在用户心目中的主观认同，软件可信性的量化需要真实反映用户的认同度，该性质可避免出现某个（些）可信属性未获得用户认同，由于其它可信属性值偏高而经过度量模型计算后最终得到的可信度也偏高的情形。

$$(\exists c_1, c_2 \in \Re^+)\ c_1 \le \frac{y_i}{y_j} \le c_2,\ \text{其中} 1 \le i, j \le m$$

其中，$\Re^+$是非负实数集合。

(3) **Monotonicity**

It means that the metric function T is monotonically increase with respect to each y_i. That is, the increment of one attribute leads to the increase of the trustworthiness. Thus, we have

$$\partial T/\partial y_i \geq 0.$$

(4) **Acceleration**

Acceleration describes the changing rate of an attribute. Under the case of the increase of only one attribute y_i and keeping of constant for other attributes $y_j, j \neq i$, the efficiency of using the attribute y_i decreases. That means that

$$\partial^2 T/\partial^2 y_i \leq 0.$$

(5) **Sensitivity**

灵敏性描述可信属性值变化对软件可信性的影响情况，灵敏性值越高影响就越大。我们通过可信属性值变化在软件可信值变化的比重（$\frac{\partial T}{\partial y_i}$）与可信属性值在软件可信值之比重（$\frac{T}{y_i}$）的比率来定义灵敏性$\delta_i$，

$$\delta_i = \frac{\frac{\partial T}{\partial y_i}}{\frac{T}{y_i}} = \frac{\partial T}{\partial y_i}\frac{y_i}{T} \geq 0, \quad 1 \leq i \leq m$$

软件可信度关于最小属性值的灵敏性相对于其它属性要大，这是基于如下事实，最小属性值的属性改变能够对软件可信性有较大改变，因此其属性值百分比变化导致软件可信度百分比变化也应该相对灵敏。

(6) Substitutivity

替代性是指可信属性间可发生一定程度的替代，反映了在保持软件可信度不变前提下，两种可信属性值可相互替代关系。因此，相反地，改变一对属性值y_i和y_j（即一个增加，另一个减少），保持其它属性值和软件可信度不变前提下，有

$$\frac{\partial T}{\partial y_i} dy_i + \frac{\partial T}{\partial y_j} dy_j = 0$$

成立，整理可得

$$-\frac{\partial T / \partial y_j}{\partial T / \partial y_i} = \frac{dy_i}{dy_j}$$

记

$$h_{ij} = -\frac{\partial T / \partial y_j}{\partial T / \partial y_i} = \frac{dy_i}{dy_j}, \quad 1 \le i, \ j \le m, \quad i \ne j$$

h_{ij}表示在软件可信度不变情况下增加（或减少）一个单位y_j需要减少（或增加）多少个单位y_i。

(6) **Substitutivity** continued

虽然h_{ij}一定程度上可用来度量属性值间的替代难易程度，但是因为用来度量不同属性的单位可能不同，为了能够对属性间的替代难易程度进行比较，我们用无单位度量。

对于任意的$i,j(1 \leq i，j \leq m，\quad i \neq j)$ 使用符号

$$\sigma_{ij} = \frac{d(y_i/y_j)}{y_i/y_j} \div \frac{d(h_{ij})}{h_{ij}} = \frac{d(y_i/y_j)}{d(h_{ij})} \times \frac{h_{ij}}{y_i/y_j} \qquad (1)$$

来描述各属性间的替代难易程度，且δ_{ij}是有界的，即

$$(\exists c_3，\ c_4 \in \Re^+)\ \ c_3 \leq \sigma_{ij} \leq c_4$$

Remark: Substitutivity

Clearly σ_{ij} satisfies $0 \leq \sigma_{ij} \leq \infty$.
The bigger σ_{ij} is, the easier is substitution between y_i and y_j.
The attributes y_i and y_j are completely replaceable at $\sigma_{ij} = \infty$ and they are not replaceable at $\sigma_{ij} = 0$.

(7) 可期望性：
期望性是指如果所有可信属性均达到用户预期，则软件可信性也要满足用户预期，并且可信值不超过最大可信属性值。

$$(y_0 \le \min\{y_1, \cdots, y_m\}) \text{ 推出 } (y_0 \le T \le \max\{y_1, \cdots, y_m\})$$

其中，y_0 是用户关于所有可信属性的最低预期。

依据软件可信性度量模型应该具有的7条性质，建立基于属性的软件可信性度量模型。

最简单度量模型–不分关键属性和非关键属性

度量模型1：

$$T_0 = y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m}$$

其中要求$1 \leq y_i \leq 10$ $(i = 1, \ldots m)$，α_i是可信属性y_i的权重，满足性质

(1) $0 < \alpha_i < 1$

(2) $\sum_{i=1}^{m} \alpha_i = 1$。

注: 不使用$T = \alpha_1 * y_1 + \alpha_2 * y_2 + \cdots + \alpha_n * y_n$。为何？

模型1性质

$$T_0 = y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m} (1 \leq y_i \leq 10)$$

Claim

(1) 非负性成立：$1 \leq T_0 \leq 10$。

模型1性质

$$T_0 = y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m} (1 \leq y_i \leq 10)$$

Claim

*(2)*比例合适性成立：$\frac{1}{10} \leq \frac{y_i}{y_j} \leq 10$。

模型1性质

$$T_0 = y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m} (1 \leq y_i \leq 10)$$

Claim

(3) 单调性成立：$\frac{\partial T_0}{\partial y_i} \geq 0$。

$$\begin{aligned} \frac{\partial T_0}{\partial y_i} &= y_1^{\alpha_1} \cdots y_{i-1}^{\alpha_{i-1}} y_{i+1}^{\alpha_{i+1}} \cdots y_m^{\alpha_m} \frac{\partial y_i^{\alpha_i}}{\partial y_i} \\ &= (\alpha_i y_i^{\alpha_i - 1}) y_1^{\alpha_1} \cdots y_{i-1}^{\alpha_{i-1}} y_{i+1}^{\alpha_{i+1}} \cdots y_m^{\alpha_m} \\ &\geq 0。\end{aligned}$$

由于$0 < \alpha_i < 1$。

模型1性质

$$T_0 = y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m} (1 \leq y_i \leq 10)$$

$$\frac{\partial T_0}{\partial y_i} = (\alpha_i y_i^{\alpha_i - 1}) y_1^{\alpha_1} \cdots y_{i-1}^{\alpha_{i-1}} y_{i+1}^{\alpha_{i+1}} \cdots y_m^{\alpha_m}$$

Claim

(4) 凝聚性成立：$\frac{\partial^2 T_0}{\partial y_i^2} \leq 0$。

$$\frac{\partial^2 T_0}{\partial y_i^2} = \alpha_i(\alpha_i - 1) y_i^{\alpha_i - 2} y_1^{\alpha_1} \cdots y_{i-1}^{\alpha_{i-1}} y_{i+1}^{\alpha_{i+1}} \cdots y_m^{\alpha_m} \leq 0$$

由于$0 < \alpha_i < 1$。

模型1性质

$$T_0 = y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m} (1 \leq y_i \leq 10)$$

$$\frac{\partial T_0}{\partial y_i} = (\alpha_i y_i^{\alpha_i - 1}) y_1^{\alpha_1} \cdots y_{i-1}^{\alpha_{i-1}} y_{i+1}^{\alpha_{i+1}} \cdots y_m^{\alpha_m}$$

Claim

(5) 灵敏性成立：$\delta_i = \frac{\frac{\partial T_0}{\partial y_i}}{\frac{T_0}{y_i}} = \frac{\partial T_0}{\partial y_i} \cdot \frac{y_i}{T_0} \geq 0$。

$$\begin{aligned} \delta_i &= (\alpha_i y_i^{\alpha_i - 1}) \cdot (y_1^{\alpha_1} \cdots y_{i-1}^{\alpha_{i-1}} y_{i+1}^{\alpha_{i+1}} \cdots y_m^{\alpha_m}) \cdot (\frac{y_i}{y_1^{\alpha_1} y_2^{\alpha_2} \ldots y_m^{\alpha_m}}) \\ &= (\alpha_i y_i^{\alpha_i - 1}) \cdot y_i^{1 - \alpha_i} \\ &= \alpha_i \\ &\geq 0 \end{aligned}$$

由于$0 < \alpha_i < 1$。

模型1性质

$$T_0 = y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m} (1 \leq y_i \leq 10)$$

$$\frac{\partial T_0}{\partial y_i} = (\alpha_i y_i^{\alpha_i - 1}) y_1^{\alpha_1} \cdots y_{i-1}^{\alpha_{i-1}} y_{i+1}^{\alpha_{i+1}} \cdots y_m^{\alpha_m}$$

Claim

(6) 代替性成立：$\sigma_{ij} = 1$。

$$\begin{aligned} h_{ij} &= -\frac{\frac{\partial T_0}{\partial y_j}}{\frac{\partial T_0}{\partial y_i}} \\ &= -\frac{(\alpha_j y_j^{\alpha_j - 1}) y_i^{\alpha_i}}{(\alpha_i y_i^{\alpha_i - 1}) y_j^{\alpha_j}} \\ &= -\frac{\alpha_j}{\alpha_i} \cdot \frac{y_i}{y_j} \\ &= -\frac{\alpha_j}{\alpha_i} \cdot t \ (t = \frac{y_i}{y_j}) \end{aligned}$$

模型1性质

$$h_{ij} = -\frac{\alpha_j}{\alpha_i} \cdot t \; (t = \frac{y_i}{y_j})$$

Claim

(6) 代替性成立：$\sigma_{ij} = 1$。

$$\begin{aligned}
\sigma_{ij} &= \frac{d(y_i/y_j)}{d(h_{ij})} \times \frac{h_{ij}}{y_i/y_j} \\
&= \frac{dt}{d(h_{ij})} \times \frac{h_{ij}}{t} \\
&= \frac{1}{\frac{d(h_{ij})}{dt}} \times \frac{h_{ij}}{t} \\
&= \frac{1}{\frac{d(-\frac{\alpha_j}{\alpha_i}t)}{dt}} \times \frac{-\frac{\alpha_j}{\alpha_i}t}{t} \\
&= \frac{1}{-\frac{\alpha_j}{\alpha_i}} \times (-\frac{\alpha_j}{\alpha_i}) \\
&= 1
\end{aligned}$$

模型1性质

$$T_0 = y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m} (1 \leq y_i \leq 10)$$

Claim

(7) 可期望性成立：$(y_0 \leq \min\{y_1, \cdots, y_m\}$ 推出$(y_0 \leq T_0 \leq y_M)$，其中y_0是用户所有可信属性的最低期望值,$y_M = \max\{y_1, \cdots, y_m\}$。

若$y_0 \leq \min\{y_1, \cdots, y_m\}$则$y_0 \leq y_i$ $(1 \leq i \leq m)$, 则

$$y_0 = y_0^{\alpha_1 + \cdots + \alpha_m} \leq y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m} = T_0$$

$$T_0 = y_1^{\alpha_1} \cdots y_m^{\alpha_m} \leq y_M^{\alpha_1} \cdots y_M^{\alpha_m} = y_M^{\alpha_1 + \cdots + \alpha_m} = y_M$$

Claim

度量模型$T = y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m} (1 \le y_i \le 10)$满足所有的度量性质。

Claim

例子：使用模型1计算软件可信性的度量值。

设软件S有三个属性：可靠性(R)、安全性(S)、功能性(F)，其对应的权重分别为$\alpha_R = 0.5, \alpha_S = 0.25, \alpha_F = 0.25$，计算若三个属性取值分别为$R = 6.8, S = 7.6, F = 8.9$则软件$S$的可信性值是多少？

$T_S = 6.8^{0.5} \times 7.6^{0.25} \times 8.9^{0.25} = 2.61 \times 1.66 \times 1.73 = 7.50$。

计算若三个属性取值分别为$R = 8.8, S = 9.6, F = 9.9$则软件$S$的可信性值是多少？

$T_S = 8.8^{0.5} \times 9.6^{0.25} \times 9.9^{0.25} = 3.10 \times 1.76 \times 1.77 = 9.66$。

作业一：使用模型1计算软件可信性的度量值

设软件S有五个属性，譬如功能性（Functionality）、安全性（Safety）、可靠性(Reliability)、生存性(Survivability)、可维护性（Maintainability），分别使用字母F, SF, R, SV, M表示。

α_F 0.25	α_{SF} 0.15	α_R 0.20	α_{SV} 0.23	α_M 0.17	
F	SF	R	SV	M	T
6.8	8.2	7.8	6.8	7.9	
8.8	8.9	9.2	9.0	9.3	
5.6	5.9	6.0	9.0	5.3	
4.6	7.8	3.8	5.1	4.5	

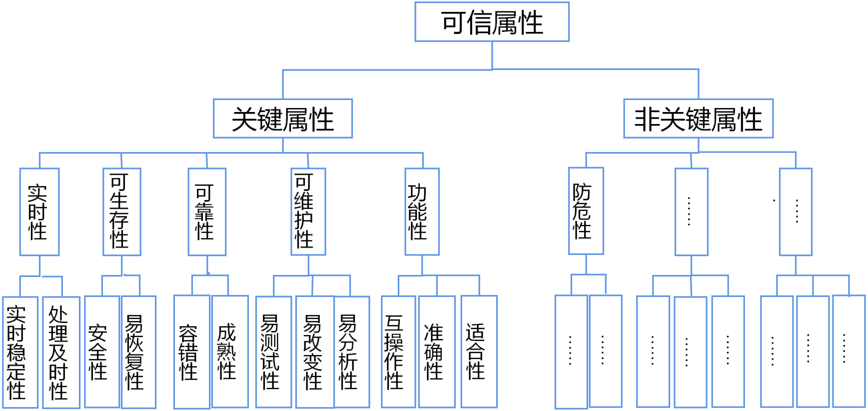
软件可信属性分解模型-关键属性与非关键属性

(1) We classify the attributes which influence the trustworthiness of software into two classes: critical and non-critical attributes.

(2) Critical attributes are the attributes that a trustworthy software must have, such as reliability, correctness, availability, controllability, security, etc.

(3) Because different softwares provide different purposes, some softwares may have other attributes except the critical attributes, such as maintainability, portability etc.. We call these attributes as non-critical.

软件可信属性分解模型-关键属性与非关键属性



To distinguish the importance between critical and non-critical attributes, we use α and β to denote the proportion of critical and non-critical attributes, respectively.

We require that $\alpha + \beta = 1$ and that α always is greater than β, i.e. $\alpha > 0.5 > \beta$;

All critical attributes are proportioned into $\alpha_1, \cdots, \alpha_m$ which satisfy $\sum_{i=1}^{m} \alpha_i = 1$.

Similarly, we proportion all non-critical attributes into $\beta_{m+1}, \cdots, \beta_{m+s}$ with $\sum_{i=m+1}^{m+s} \beta_i = 1$.

Software Trustworthy Metric Formulae

$$T = F(y_1, \cdots, y_m, y_{m+1}, \cdots, y_{m+s})$$

What is F?

Model 1

$$T_1 = \frac{10}{11}(\frac{y_{\min}}{10})^{\varepsilon} y_1^{\alpha\alpha_1} y_2^{\alpha\alpha_2} \cdots y_m^{\alpha\alpha_m} + \frac{10}{11} y_{m+1}^{\beta\beta_{m+1}} y_{m+2}^{\beta\beta_{m+2}} \cdots y_{m+s}^{\beta\beta_{m+s}}$$

(1) $0 \leq \varepsilon \leq 1 - \alpha_{\min}$ is used to control the influence of the minimal critical attribute on the trustworthiness of software, the bigger ϵ, the greater is the influence.

(2) $1 \leq y_i \leq 10, 1 \leq i \leq m + s$。

(3) $y_{\min} = \min\{y_i \mid i = 1, \cdots, m\}$。

Model 1

$$T_1 = \frac{10}{11}(\frac{y_{\min}}{10})^{\varepsilon} y_1^{\alpha\alpha_1} y_2^{\alpha\alpha_2} \cdots y_m^{\alpha\alpha_m} + \frac{10}{11} y_{m+1}^{\beta\beta_{m+1}} y_{m+2}^{\beta\beta_{m+2}} \cdots y_{m+s}^{\beta\beta_{m+s}}$$

Claim

断言 *1*：

$$1 \leq T_1 \leq 10。$$

因为$1 \leq y_i \leq 10$,所以将所有$y_i = 1$带入T_1可以得到$T_1 = \frac{10}{11}(\frac{1}{10^{\varepsilon}} + 1)$。又因为$10^{\varepsilon} < 10$，所以$\frac{1}{10^{\varepsilon}} > \frac{1}{10}$。这时，我们有$T_1 = \frac{10}{11}(\frac{1}{10^{\varepsilon}} + 1) \geq \frac{10}{11}(\frac{1}{10} + 1) = 1$。
将所有$y_i = 10$带入T_1可以得到$T_1 = \frac{10}{11}(10^{\alpha} + 10^{\beta})$。因为$\alpha + \beta = 1$并且$\alpha > \frac{1}{2} > \beta$，所以$10^{\alpha} + 10^{\beta} \leq 11$。故而，$T_1 = \frac{10}{11}(10^{\alpha} + 10^{\beta}) \leq 10$。

Model 1

$$T_1 = \frac{10}{11}(\frac{y_{\min}}{10})^{\varepsilon} y_1^{\alpha\alpha_1} y_2^{\alpha\alpha_2} \cdots y_m^{\alpha\alpha_m} + \frac{10}{11} y_{m+1}^{\beta\beta_{m+1}} y_{m+2}^{\beta\beta_{m+2}} \cdots y_{m+s}^{\beta\beta_{m+s}}$$

Claim

断言*2*：比例合适性：$1 \leq \frac{y_i}{y_j} \leq 10$，因为$1 \leq y_i \leq 10$。

Claim

断言3：T_1 *is a monotonically increase function.*

Denote the i with $\min_{1\le i\le m}\{y_i\}$ by $\min$, in the three models we present, we always require that $\alpha\alpha_{min}+\epsilon\le 1$, in case that the change in the minimal critical attribute induces the change in T is too big.

Since

$$\frac{\partial T_1}{\partial y_i}=\begin{cases}\frac{10\alpha\alpha_i}{11\times 10^{\varepsilon}}y_1^{\alpha\alpha_1}\cdots y_i^{\alpha\alpha_i-1}\cdots y_{min}^{\alpha\alpha_{min}+\varepsilon}\cdots y_m^{\alpha\alpha_m} & i\ne min,\ 1\le i\le m\\ \frac{10(\alpha\alpha_{min}+\varepsilon)}{11\times 10^{\varepsilon}}y_1^{\alpha\alpha_1}\cdots y_{min}^{\alpha\alpha_{min}+\varepsilon-1}\cdots y_m^{\alpha\alpha_m} & i=min\\ \frac{10}{11}\beta\beta_i y_{m+1}^{\beta\beta_{m+1}}\cdots y_i^{\beta\beta_i-1}\cdots y_{m+s}^{\beta\beta_{m+s}} & m+1\le i\le m+s\end{cases}$$

Hence

$$\frac{\partial T_1}{\partial y_i}\ge 0.$$

Acceleration of Model 1

Claim

断言4：T_1 *satisfies the acceleration criterion. That is, for* $1 \le i \le m+s$, *we can derive that* $\frac{\partial^2 T_1}{\partial^2 y_i} \le 0$.

Since

$$\frac{\partial^2 T_1}{\partial^2 y_i} = \begin{cases} \frac{10\alpha\alpha_i(\alpha\alpha_i - 1)}{11 \times 10^{\varepsilon}} y_1^{\alpha\alpha_1} \cdots y_i^{\alpha\alpha_i - 2} \cdots y_{min}^{\alpha\alpha_{min}+\varepsilon} \cdots y_m^{\alpha\alpha_m} & i \ne min, 1 \le i \le m \\ \frac{10(\alpha\alpha_{min}+\varepsilon)(\alpha\alpha_{min}+\varepsilon-1)}{11 \times 10^{\varepsilon}} y_1^{\alpha\alpha_1} \cdots y_{min}^{\alpha\alpha_{min}+\varepsilon-2} \cdots y_m^{\alpha\alpha_m} & i = min \\ \frac{10}{11}\beta\beta_i(\beta\beta_i - 1) y_{m+1}^{\beta\beta_{m+1}} \cdots y_i^{\beta\beta_i - 2} \cdots y_{m+s}^{\beta\beta_{m+s}} & m+1 \le i \le m+s \end{cases}$$

Hence

$$\frac{\partial^2 T_1}{\partial^2 y_i} \le 0.$$

Sensitivity of Model 1

Claim

断言5：T *is sensitive to all attributes.*

$$\delta_i = \frac{\partial T_1}{\partial y_i}\frac{y_i}{T_1} = \begin{cases} 10\alpha\alpha_i \dfrac{y_1^{\alpha\alpha_1}\cdots y_i^{\alpha\alpha_i}\cdots y_{min}^{\alpha\alpha_{min}+\varepsilon}\cdots y_m^{\alpha\alpha_m}}{11\times 10^{\varepsilon}T_1} & i \neq min, 1 \leq i \leq m \\ 10(\alpha\alpha_{min}+\varepsilon)\dfrac{y_1^{\alpha\alpha_1}\cdots y_{min}^{\alpha\alpha_{min}+\varepsilon}\cdots y_m^{\alpha\alpha_m}}{11\times 10^{\varepsilon}T_1} & i = min \\ 10\beta\beta_i \dfrac{y_{m+1}^{\beta\beta_{m+1}}\cdots y_i^{\beta\beta_i}\cdots y_{m+s}^{\beta\beta_{m+s}}}{11T_1} & m+1 \leq i \leq m+s \end{cases}$$

The attribute with the minimal critical attribute affects on the whole trustworthy degree more than other attributes by adding of ε.

Substitutivity of Model 1

Claim

断言6：T_1 *has the substitutivity between attributes.*

(a) Substitutivity among critical attributes:

$$\sigma_{ij} = 1 \quad 1 \le i,j \le m;$$

(b) Substitutivity among non-critical attributes:

$$\sigma_{ij} = 1 \quad m+1 \le i,j \le m+s$$

(c) Substitutivity between critical and non-critical attributes:

$$\sigma_{ij} = \begin{cases} \dfrac{\beta\beta_j a + \frac{1}{10\epsilon}\alpha\alpha_i b}{(1-\alpha\alpha_i)\beta\beta_j a + (1-\beta\beta_j)\frac{1}{10\epsilon}\alpha\alpha_i b} \ge 1, & 1 \le i \le m, i \ne min, m+1 \le j \le m+s \\ \dfrac{\beta\beta_j a + \frac{1}{10\epsilon}(\alpha\alpha_i + \epsilon)b}{(1-\alpha\alpha_i-\epsilon)\beta\beta_j a + (1-\beta\beta_j)\frac{1}{10\epsilon}(\alpha\alpha_i+\epsilon)b} \ge 1, & i = min, m+1 \le j \le m+s \end{cases}$$

where

$$\begin{cases} a = y_{m+1}^{\beta\beta_{m+1}} \cdots y_j^{\beta\beta_j} \cdots y_{m+s}^{\beta\beta_{m+s}} \\ b = y_1^{\alpha\alpha_1} \cdots y_i^{\alpha\alpha_i} \cdots y_m^{\alpha\alpha_m} \end{cases}$$

Expectation of Model 1

$$T_1 = \frac{10}{11}(\frac{y_{\min}}{10})^{\varepsilon} y_1^{\alpha\alpha_1} y_2^{\alpha\alpha_2} \cdots y_m^{\alpha\alpha_m} + \frac{10}{11} y_{m+1}^{\beta\beta_{m+1}} y_{m+2}^{\beta\beta_{m+2}} \cdots y_{m+s}^{\beta\beta_{m+s}}$$

Claim

断言7：T_1 具有可期望性??。

设$y_0 \le \min\{y_1, \cdots, y_{m+s}\}$则$y_0 \le T_1 \le \max\{y_1, \cdots, y_{m+s}\}$。
这是因为$y_0^{\alpha+\varepsilon} \le y_{\min}^{\alpha+\varepsilon}$，进而，

Model 2

$$T_2 = \frac{10}{11}(\frac{y_{\min}}{10})^{\varepsilon} y_1^{\alpha\alpha_1} y_2^{\alpha\alpha_2} \cdots y_m^{\alpha\alpha_m} + \frac{10}{11} y_{\min'}^{\beta\beta_i},$$

where $y_{\min}, \varepsilon$ and y_i are the same as those t in model 1 and $y_{\min'} = \min\{y_j \mid m+1 \leq j \leq m+s\}$。

Claim

非负性：

$$1 \leq T_2 \leq 10。$$

Claim

比例合适性：

$$\frac{1}{10} \leq \frac{y_i}{y_j} \leq 10$$

Claim

单调性：T_2 *is a monotonically increase function.*

Since

$$\frac{\partial T_2}{\partial y_i} = \begin{cases} \frac{10\alpha\alpha_i}{11 \times 10^{\varepsilon}} y_1^{\alpha\alpha_1} \cdots y_i^{\alpha\alpha_i - 1} \cdots y_{min}^{\alpha\alpha_{min}+\varepsilon} \cdots y_m^{\alpha\alpha_m} & i \neq min, 1 \leq i \leq m \\ \frac{10(\alpha\alpha_{min} + \varepsilon)}{11 \times 10^{\varepsilon}} y_1^{\alpha\alpha_1} \cdots y_{min}^{\alpha\alpha_{min}+\varepsilon-1} \cdots y_m^{\alpha\alpha_m} & i = min \\ \frac{10}{11}\beta\beta_i y_i^{\beta\beta_i - 1} & i = min' \\ 0 & m+1 \leq i \leq m+s, i \neq min' \end{cases}$$

Hence

$$\frac{\partial T_2}{\partial y_i} \geq 0$$

凝聚性：

Claim

T_2 satisfies the acceleration criterion. That is, for $1 \leq i \leq m+s$, we can derive that $\frac{\partial^2 T}{\partial^2 y_i} \leq 0$.

Since

$$\frac{\partial^2 T_2}{\partial^2 y_i} = \begin{cases} \frac{10\alpha\alpha_i(\alpha\alpha_i - 1)}{11 \times 10^{\varepsilon}} y_1^{\alpha\alpha_1} \cdots y_i^{\alpha\alpha_i - 2} \cdots y_{min}^{\alpha\alpha_{min}+\varepsilon} \cdots y_m^{\alpha\alpha_m} & i \neq min, 1 \leq i \leq m \\ \frac{10(\alpha\alpha_{min} + \varepsilon)(\alpha\alpha_{min} + \varepsilon - 1)}{11 \times 10^{\varepsilon}} y_1^{\alpha\alpha_1} \cdots y_{min}^{\alpha\alpha_{min}+\varepsilon-2} \cdots y_m^{\alpha\alpha_m} & i = min \\ \frac{10}{11}\beta\beta_i(\beta\beta_i - 1) y_i^{\beta\beta_i - 2} & i = min' \\ 0 & m+1 \leq i \leq m+s, i \neq min' \end{cases}$$

Hence

$$\frac{\partial^2 T_2}{\partial^2 y_i} \leq 0.$$

敏感性：

Claim

T_2 is sensitive to almost all attributes.

$$\delta_i = \frac{\partial T_2}{\partial y_i}\frac{y_i}{T_2} = \begin{cases} 10\alpha\alpha_i \dfrac{y_1^{\alpha\alpha_1}\cdots y_i^{\alpha\alpha_i}\cdots y_{min}^{\alpha\alpha_{min}+\varepsilon}\cdots y_m^{\alpha\alpha_m}}{11\times 10^{\varepsilon}T_2} & 1\le i\le m, i\ne min \\ 10(\alpha\alpha_{min}+\varepsilon)\dfrac{y_1^{\alpha\alpha_1}\cdots y_{min}^{\alpha\alpha_{min}+\varepsilon}\cdots y_m^{\alpha\alpha_m}}{11\times 10^{\varepsilon}T_2} & i = min \\ 10\beta\beta_i\dfrac{y_i^{\beta\beta_i}}{11T_2} & i = min' \\ 0 & m+1\le i\le m+s, i\ne min' \end{cases}$$

which means that T is sensitive to all attributes except the non-critical attributes which are not minimal.

Remark The sensitivity of T to non-critical attributes which are not minimal are zero, the reason is that in this model we just emphasis the influence of the minimal non-critical attribute on the trustworthiness of software.

Claim

替代性：T_2 *has the substitutivity between attributes.*

(a) Substitutivity among critical attributes:

$$\sigma_{ij} = 1 \quad 1 \leq i,j \leq m;$$

(b) Substitutivity among non-critical attributes:

$$\sigma_{ij} = 1 \quad m+1 \leq i,j \leq m+s$$

(c) Substitutivity between critical and non-critical attributes:

$$\sigma_{ij} = \begin{cases} \dfrac{\beta\beta_j y_j^{\beta\beta_j} + \frac{\alpha\alpha_i}{10^{\epsilon}} b}{(1-\alpha\alpha_i)\beta\beta_j y_j^{\beta\beta_j} + (1-\beta\beta_j)\frac{\alpha\alpha_i}{10^{\epsilon}} b} \geq 1, & 1 \leq i \leq m, i \neq min, j = min' \\ \dfrac{\beta\beta_j y_j^{\beta\beta_j} + \frac{\alpha\alpha_i+\epsilon}{10^{\epsilon}} b}{(1-\alpha\alpha_i-\epsilon)\beta\beta_j y_j^{\beta\beta_j} + (1-\beta\beta_j)\frac{\alpha\alpha_i+\epsilon}{10^{\epsilon}} b} \geq 1, & i = min, j = min' \\ 0 & 1 \leq i \leq m, j \neq min' \end{cases}$$

where $b = y_{m+1}^{\beta\beta_{m+1}} \cdots y_j^{\beta\beta_j} \cdots y_{m+s}^{\beta\beta_{m+s}}$

Remark: Compared with model 1, in this model except the substitutivity between the critical attributes and the minimal non-critical attribute, all the substitutivity between critical attributes and non-critical attributes are more difficult than either the substitutivity among critical attributes or that among non-critical attributes. In the view of substitutivity, this model is better than model 1.

$$T_2 = \frac{10}{11}(\frac{y_{\min}}{10})^{\varepsilon} y_1^{\alpha\alpha_1} y_2^{\alpha\alpha_2} \cdots y_m^{\alpha\alpha_m} + \frac{10}{11} y_{\min}^{\beta\beta_i},$$

Claim

断言7：T_2 具有可期望性??。

设$y_0 \leq \min\{y_1, \cdots, y_{m+s}\}$则$y_0 \leq T_2 \leq \max\{y_1, \cdots, y_{m+s}\}$。
这是因为$y_0^{\alpha+\varepsilon} \leq y_{\min}^{\alpha+\varepsilon}$，进而，

Model 3

$$T_3 = \{\alpha[\min_{1\le i\le m}\{(\frac{y_i}{10})^{\epsilon}\}y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_m^{\alpha_m}]^{-\rho}+\beta[y_{m+1}^{\beta_{m+1}}y_{m+2}^{\beta_{m+2}}\cdots y_{m+s}^{\beta_{m+s}}]^{-\rho}\}^{-\frac{1}{\rho}}$$

其中，

1. ϵ：调控参数，用来调控最小关键属性对软件可信性的影响，满足$0\le\epsilon\le\min\{1-\alpha_{\min'}, \frac{\ln y_0-\ln y_{\min'}}{\ln y_{\min'}-\ln 10}\}$，且$\epsilon$越大，影响越大，$\alpha_{\min'}$表示最小关键属性在整个关键属性集中所占的权重；
2. y_0：由用户提供的可信属性值需达到的阈值；
3. ρ：与关键属性和非关键属性之间替代性相关的参数，满足$0<\rho$，且其值越大，则关键属性与非关键属性间替代性越难；
4. y_i：第$i(1\le i\le m+s)$个可信属性的可信值，满足$1\le y_0\le y_i\le 10$。

Model 3

为了方便起见，记满足$\min\limits_{1\le i\le m}\{y_i\}$的$i$为$min'$（关键属性），满足$\max\limits_{1\le i\le m}\{y_i\}$的$i$为$max'$（关键属性），满足$\min\limits_{m+1\le i\le m+s}\{y_i\}$的$i$为$min''$（非关键属性），满足$\max\limits_{m+1\le i\le m+s}\{y_i\}$的$i$为$max''$（非关键属性），并记

$$y_{min'} = \min_{1\le i\le m}\{y_i\}$$

$$y_{max'} = \max_{1\le i\le m}\{y_i\}$$

$$y_{min''} = \min_{m+1\le i\le m+s}\{y_i\}$$

$$y_{max''} = \max_{m+1\le i\le m+s}\{y_i\}$$

再记

$$a_1 = \min_{1\le i\le m}\{(\frac{y_i}{10})^{\epsilon}\}y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_m^{\alpha_m}$$

$$b_1 = y_{m+1}^{\beta_{m+1}}y_{m+2}^{\beta_{m+2}}\cdots y_{m+s}^{\beta_{m+s}}$$

Model 3

$$T_3 = \{\alpha[\min_{1\le i\le m}\{(\frac{y_i}{10})^{\epsilon}\}y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_m^{\alpha_m}]^{-\rho}+\beta[y_{m+1}^{\beta_{m+1}}y_{m+2}^{\beta_{m+2}}\cdots y_{m+s}^{\beta_{m+s}}]^{-\rho}\}^{-\frac{1}{\rho}}$$

Claim

非负性：

$$1 \le T_3 \le 10$$

Claim

比例合适性：

$$\frac{1}{10} \le \frac{y_i}{y_j} \le 10$$

Model 3

Claim

模型T_3关于$y_i(1 \leq i \leq m+s)$是单调递增函数。

$$\frac{\partial T_3}{\partial y_i} = \begin{cases} \alpha\alpha_i T_3^{1+\rho} a_1^{-\rho} y_i^{-1}, & i \neq min',\ 1 \leq i \leq m \\ \alpha(\alpha_i + \epsilon) T_3^{1+\rho} a_1^{-\rho} y_i^{-1}, & i = min' \\ \beta\beta_i T_3^{1+\rho} b_1^{-\rho} y_i^{-1}, & m+1 \leq i \leq m+s \end{cases}$$

$$\begin{cases} 0 \leq \alpha, \alpha_i \leq 1,\ 1 \leq i \leq m \\ 0 \leq \beta, \beta_i \leq 1,\ m+1 \leq i \leq m+s \\ 0 \leq \epsilon \leq \min\{1-\alpha_{\min'}, \dfrac{\ln y_0 - \ln y_{\min'}}{\ln y_{\min'} - \ln 10}\} \\ 1 \leq y_0 \leq y_i \leq 10,\ 1 \leq i \leq m+s \end{cases}$$

则

$$\frac{\partial T_3}{\partial y_i} \geq 0, \quad 1 \leq i \leq m+s$$

即T_3 是关于$y_i(1 \leq i \leq m+s)$的单调递增函数。

Model 3

Claim

模型T_3 满足凝聚性。

对T_3关于每一个$y_i(1 \leq i \leq m+s)$求二阶导数可得

$$\frac{\partial^2 T_3}{\partial {y_i}^2} = \begin{cases} \left(\alpha\alpha_i^2(1+\rho)c_1 - \alpha\alpha_i^2\rho - \alpha\alpha_i\right) d_1, & i \neq min', \ 1 \leq i \leq m \\ \left(\alpha(\alpha_i+\epsilon)^2(1+\rho)c_1 - \alpha(\alpha_i+\epsilon)^2\rho - \alpha(\alpha_i+\epsilon)\right) d_1, & i = min' \\ \left(\beta\beta_i^2(1+\rho)e_1 - \beta\beta_i^2\rho - \beta\beta_i\right) f_1, & m+1 \leq i \leq m+s \end{cases}$$

其中

$$\begin{cases} c_1 = \dfrac{\alpha[\min_{1\leq i\leq m}\{(\frac{y_i}{10})^{\epsilon}\}y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_m^{\alpha_m}]^{-\rho}}{T_3^{-\rho}} \\ d_1 = T_3^{1+\rho}[\min\limits_{1\leq i\leq m}\{(\dfrac{y_i}{10})^{\epsilon}\}y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_m^{\alpha_m}]^{-\rho}y_i^{-2} \\ e_1 = \dfrac{\beta[y_{m+1}^{\beta_{m+1}}y_{m+2}^{\beta_{m+2}}\cdots y_{m+s}^{\beta_{m+s}}]^{-\rho}}{T_3^{-\rho}} \\ f_1 = T_3^{1+\rho}[y_{m+1}^{\beta_{m+1}}y_{m+2}^{\beta_{m+2}}\cdots y_{m+s}^{\beta_{m+s}}]^{-\rho}y_i^{-2} \end{cases}$$

Model 3

因为

$$\begin{cases} 0 \le \alpha，\ \alpha_i \le 1，\ 1 \le i \le m \\ 0 \le \beta，\ \beta_i \le 1，\ m+1 \le i \le m+s \\ 0 \le \epsilon \le \min\{1-\alpha_{\min'}，\ \dfrac{\ln y_0 - \ln y_{\min'}}{\ln y_{\min'} - \ln 10}\} \\ 1 \le y_0 \le y_i \le 10，\ \ 1 \le i \le m+s \end{cases}$$

并且

$$\begin{cases} 0 \le c_1 = \dfrac{\alpha[\min_{1\le i\le m}\{(\frac{y_i}{10})^{\epsilon}\} y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m}]^{-\rho}}{T_3^{-\rho}} \le 1 \\ 0 \le d_1 = T_3^{1+\rho}[\min\limits_{1\le i\le m}\{(\dfrac{y_i}{10})^{\epsilon}\} y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m}]^{-\rho} y_i^{-2} \\ 0 \le e_1 = \dfrac{\beta[y_{m+1}^{\beta_{m+1}} y_{m+2}^{\beta_{m+2}} \cdots y_{m+s}^{\beta_{m+s}}]^{-\rho}}{T_3^{-\rho}} \le 1 \\ 0 \le f_1 = T_3^{1+\rho}[y_{m+1}^{\beta_{m+1}} y_{m+2}^{\beta_{m+2}} \cdots y_{m+s}^{\beta_{m+s}}]^{-\rho} y_i^{-2} \end{cases}$$

和

$$\alpha\alpha_{min'} + \epsilon \leq 1$$

所以

$$\begin{cases} \left(\alpha\alpha_i^2(1+\rho)c_1 - \alpha\alpha_i^2\rho - \alpha\alpha_i\right) d_1 & \\ \leq \left(\alpha\alpha_i^2(1+\rho) - \alpha\alpha_i^2\rho - \alpha\alpha_i\right) d_1 \leq 0, & i \neq min',\ 1 \leq i \leq m \\ \left(\alpha(\alpha_i+\epsilon)^2(1+\rho)c_1 - \alpha(\alpha_i+\epsilon)^2\rho - \alpha(\alpha_i+\epsilon)\right) d_1 & \\ \leq \left(\alpha(\alpha_i+\epsilon)^2(1+\rho) - \alpha(\alpha_i+\epsilon)^2\rho - \alpha(\alpha_i+\epsilon)\right) d_1 \leq 0, & i = min' \\ \left(\beta\beta_i^2(1+\rho)e_1 - \beta\beta_i^2\rho - \beta\beta_i\right) f_1 & \\ \leq \left(\beta\beta_i^2(1+\rho) - \beta\beta_i^2\rho - \beta\beta_i\right) f_1 \leq 0, & m+1 \leq i \leq m+s \end{cases}$$

因此对于所有的$1 \leq i \leq m+s$有

$$\frac{\partial^2 T_3}{\partial^2 y_i} \leq 0$$

Model 3

Claim

模型T_3 满足灵敏性。

由计算可得

$$\delta_i = \frac{\partial T_3}{\partial y_i}\frac{y_i}{T_3} = \begin{cases} \alpha\alpha_i a_1^{-\rho} T_3^{-\rho}, & i \neq min',\ 1 \leq i \leq m \\ \alpha(\alpha_i + \epsilon) a_1^{-\rho} T_3^{-\rho}, & i = min' \\ \beta\beta_i b_1^{-\rho} T_3^{-\rho}, & m+1 \leq i \leq m+s \end{cases}$$

易证$0 \leq \delta_i, 1 \leq i \leq m+s$，且在关键属性中最小关键属性灵敏性$\delta_{min'}$最高。
其中

$$a_1 = \min_{1\leq i\leq m}\{(\frac{y_i}{10})^{\epsilon}\} y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m}$$

$$b_1 = y_{m+1}^{\beta_{m+1}} y_{m+2}^{\beta_{m+2}} \cdots y_{m+s}^{\beta_{m+s}}$$

Model 3

Claim

替代性：模型T_3满足替代性，且关键属性与非关键属性间替代性既难于关键属性间替代性又难于非关键属性间替代性。

由计算可得，对于关键属性间替代性有

$$\sigma_{ij}=1,\ 1\le i,j\le m,\ i\ne j$$

类似的对于非关键属性间替代性有

$$\sigma_{ij}=1,\ m+1\le i,j\le m+s,\ i\ne j$$

接下来考虑关键属性和非关键属性间替代性。因为

$$h_{ij}=\begin{cases}\dfrac{-\alpha\alpha_j a_1^{-\rho}y_j^{-1}}{\beta\beta_i b_1^{-\rho}y_i^{-1}}, & j\ne min',\ 1\le j\le m,\ m+1\le i\le m+s\\[2ex] \dfrac{-(\alpha\alpha_j+\epsilon)a_1^{-\rho}y_j^{-1}}{\beta\beta_i b_1^{-\rho}y_i^{-1}}, & j=min',\ m+1\le i\le m+s\end{cases}$$

Model 3

Claim

替代性：模型T_3满足替代性，且关键属性与非关键属性间替代性既难于关键属性间替代性又难于非关键属性间替代性。

$$\sigma_{ij} = \begin{cases} \dfrac{1 + \frac{y_i}{y_j}\frac{\partial T/\partial y_i}{\partial T/\partial y_j}}{(1+\rho\beta_i) + (1+\rho\alpha_j)\frac{y_i}{y_j}\frac{\partial T/\partial y_i}{\partial T/\partial y_j}}, & j \neq min',\ 1 \leq j \leq m,\ m+1 \leq i \leq m+s \\ \dfrac{1 + \frac{y_i}{y_j}\frac{\partial T/\partial y_i}{\partial T/\partial y_j}}{(1+\rho\beta_i) + (1+\rho\epsilon+\rho\alpha_j)\frac{y_i}{y_j}\frac{\partial T/\partial y_i}{\partial T/\partial y_j}}, & j = min',\ m+1 \leq i \leq m+s \end{cases}$$

由此可得：且关键属性与非关键属性间的替代性σ_{ij}在$\frac{1}{1+\rho}$与1之间。由于$\rho > 0$，则关键属性与非关键属性间的替代性既难于关键属性间替代性又难于非关键属性间替代性，而且参数ρ越大其替代性越难。

Claim

模型T_3 满足可期望性，即

$$y_0 \leq T_3 \leq \max\{y_1, \cdots, y_{m+s}\}$$

$$T_3 = \{\alpha[\min_{1\leq i\leq m}\{(\frac{y_i}{10})^{\epsilon}\}y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_m^{\alpha_m}]^{-\rho}+\beta[y_{m+1}^{\beta_{m+1}}y_{m+2}^{\beta_{m+2}}\cdots y_{m+s}^{\beta_{m+s}}]^{-\rho}\}^{-\frac{1}{\rho}}$$

该模型满足非负性、比例合适性、单调性、凝聚性、灵敏性、替代性和可期望性7条性质。并且，在模型T_3中关键属性与非关键属性间替代性要难于关键属性间替代性以及非关键属性间替代性。

T_3模型好于T_1和T_2模型。

关于模型T_3的模拟

设有4个软件系统，分别编号为1,2,3,4。它们都有7个属性，其中4个为关键属性，编号为y_1, y_2, y_3, y_4, 其权重分别为$\alpha_1 = 0.2, \alpha_2 = 0.3, \alpha_3 = 0.35, \alpha_4 = 0.15$。3个为非关键属性，编号为$y_5, y_6, y_7$，其权重分别为$\beta_1 = 0.25, \beta_2 = 0.35, \beta_3 = 0.40$。关键属性权重$\alpha = 0.75$, 非关键属性$\beta = 0.25$。

Table: 关于模型T_3的模拟

编号	y_1	y_2	y_3	y_4	y_5	y_6	y_7	ϵ	ρ	T_3
1	8	7	8	6	9	8	8	0.1	0.10	7.285
	8	7	8	6	9	8	8	0.05	0.15	7.426
2	8	8	8	6	9	8	8	0.1	0.10	7.508
	8	8	8	6	9	8	8	0.05	0.15	7.653
3	8	7	8	7	9	8	8	0.1	0.10	7.500
	8	7	8	7	9	8	8	0.05	0.15	7.600
4	9	7	8	6	9	8	8	0.1	0.10	7.415
	8	7	8	7	9	8	8	0.05	0.15	7.600

$$T_3 = \{\alpha[\min_{1\le i\le m}\{(\frac{y_i}{10})^{\epsilon}\}y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_m^{\alpha_m}]^{-\rho}+\beta[y_{m+1}^{\beta_{m+1}}y_{m+2}^{\beta_{m+2}}\cdots y_{m+s}^{\beta_{m+s}}]^{-\rho}\}^{-\frac{1}{\rho}}$$

作业二

设有4个软件系统，分别编号为1,2,3,4。它们都有7个属性，其中4个为关键属性，编号为y_1, y_2, y_3, y_4, 其权重分别为$\alpha_1 = 0.3, \alpha_2 = 0.2, \alpha_3 = 0.35, \alpha_4 = 0.15$。3个为非关键属性，编号为$y_5, y_6, y_7$，其权重分别为$\beta_1 = 0.35, \beta_2 = 0.40, \beta_3 = 0.25$。关键属性权重$\alpha = 0.70$, 非关键属性$\beta = 0.30$。依据下表的个属性取值使用模型$T_3$计算各软件的可信性度值。

编号	y_1	y_2	y_3	y_4	y_5	y_6	y_7	ϵ	ρ	T_3
1	8.3	7.1	8.1	6.9	9.1	8.5	8.6	0.1	0.10	
	7.8	8.7	8.0	6.2	8.9	8	8.8	0.05	0.15	
2	5.8	8.1	6.8	5.6	7.9	6.8	8.1	0.1	0.10	
	6.8	7.8	8.1	6.9	8.9	7.8	8.8	0.05	0.15	
3	3.8	3.7	4.8	4.7	3.9	5.8	6.8	0.1	0.10	
	8.4	7.2	8.1	7.7	7.9	.88	.68	0.05	0.15	
4	9.0	8.7	8.9	8.6	9.1	8.8	8.9	0.1	0.10	
	8.0	7.8	6.8	8.7	7.9	8.1	8.3	0.05	0.15	