第二章
软件可靠性分析

陈仪香

华东师范大学软件学院可信智能团队TrIG

2024年9月18日

TrIG 华东师范大学软件学院可信智能团队
Trustworthy Intelligence Group

本章参考书

2.《软件可靠性工程》，主编：陆民 燕，国防工业出版社，2011.4年

第二章 软件可靠性分析

2.1 软件可靠性

2.2 软件可靠性分析

2.3 软件可靠性评估

TrIG
华东师范大学软件学院可信智能团队
Trustworthy Intelligence Group

2.3 软件可靠性评估

国家标准GB11457中， 软件可靠性评估（Software Reliability Assessment）或软件可靠性评价（Software Reliability Evaluation）是指“确定现有系统或系统部件可靠性所达到的水平的过程”。国际标准IEEE Std 1633中， 软件可靠性评估被定义为“统计学技术在系统测试和运行期间收集的可观察失效数据上的应用，用于评价软件的可靠性”。

不难看出， 二者的定义均认为，软件可靠性评估是在获得了软件失效数据之后对软件可靠性水平的定量估计和评价。

2.3 软件可靠性评估

软件失效数据可以在下述两种情况下获得：

一是在测试阶段后期，通过软件可靠性测试（即按照软件的实际使用方式测试软件的一种方法），收集测试过程中的失效数据，对软件的可靠性水平进行估计，并能够对未来可能达到的可靠性水平进行预计；

二是在软件投入使用后，通过收集实际使用过程中软件的失效数据，对软件可靠性进行评估，并对未来软件可能达到的可靠性水平进行预计。

2.3 软件可靠性评估

软件可靠性评估结果，不仅可以给出实际的可靠性水平，也可以为下一代软件或同类型软件的可靠性定量要求的确定提供参考。

软件可靠性评估是软件可靠性工程中重要活动内容之一，具有及其重要的作用。

2.3 软件可靠性评估

软件可靠性评估，不能不得不提及软件可靠性评估模型，它是软件可靠性定量评估技术的基础。

软件失效具有随机性。软件在是t时刻发生的失效数是N(t)， 显然N(t)是一个随机数，且随时间t的变化而不同， 即{N(t), t>0}是一个随机过程。

问： 这个随机过程应该服从什么分布？

2.3 软件可靠性评估

问： 这个随机过程应该服从什么分布?

参照国际标准IEEE Std.1633，可将软件可靠性评估模型分为3中通用类别:

① 指数分布的非齐次泊松(Poisson)过程模型(Non-homogeneous Poisson process，NHPP)、

② 非指数分布的NHPP模型，

③ 贝叶斯（Bayesian）模型。

2.3 软件可靠性评估

呈指数分布的NHPP模型

呈指数分布的NHHP模型使用随机过程和失效率函数方法。

失效率函数Z(t)是运行时间t的函数。

具有代表性的模型是Jelinski-Moranda模型， 1972年开发的可靠性模型，是最早建立的软件可靠性模型之一，曾用于麦克唐奈道拉斯海军工程中。现在大多数软件可靠性模型要么可认为是其变形或扩展，要么与其密切相关。该模型是软件可靠性研究领域分第一个里程碑。

2.3 软件可靠性评估

Jelinski-Moranda模型

（1） 假设与数据要求：

模型的基本假设如下：

① 程序中的固有错误数N_0是一个未知的常数；

② 程序中的各个错误是相互独立的，每个错误导致系统发生失效的可能性大致相同，各次失效间隔也是相互独立的；

③ 测试过程中检测到的错误都被排除，每次排错只排除一个错误，排错时间可以忽略不计，在排错过程中不引入新的错误；

2.3 软件可靠性评估

Jelinski-Moranda模型

（1） 假设与数据要求：

模型的基本假设如下：

④ 程序失效率在每个失效间隔时间内是常数，其数值正比于程序中残留的错误数，在第i个测试区间，其失效率函数为

$$Z(x_i)=k(N_0-i+1)$$

式中：k为比例常数， x_i为第i次失效间隔中以i-1次失效为起点的时间变量。

2.3 软件可靠性评估

Jelinski-Moranda模型

在第i个测试区间，其失效率函数为

$$Z(x_i)=k(N_0-i+1)$$

式中：k为比例常数， x_i为第i次失效间隔中以i-1次失效为起点的时间变量。

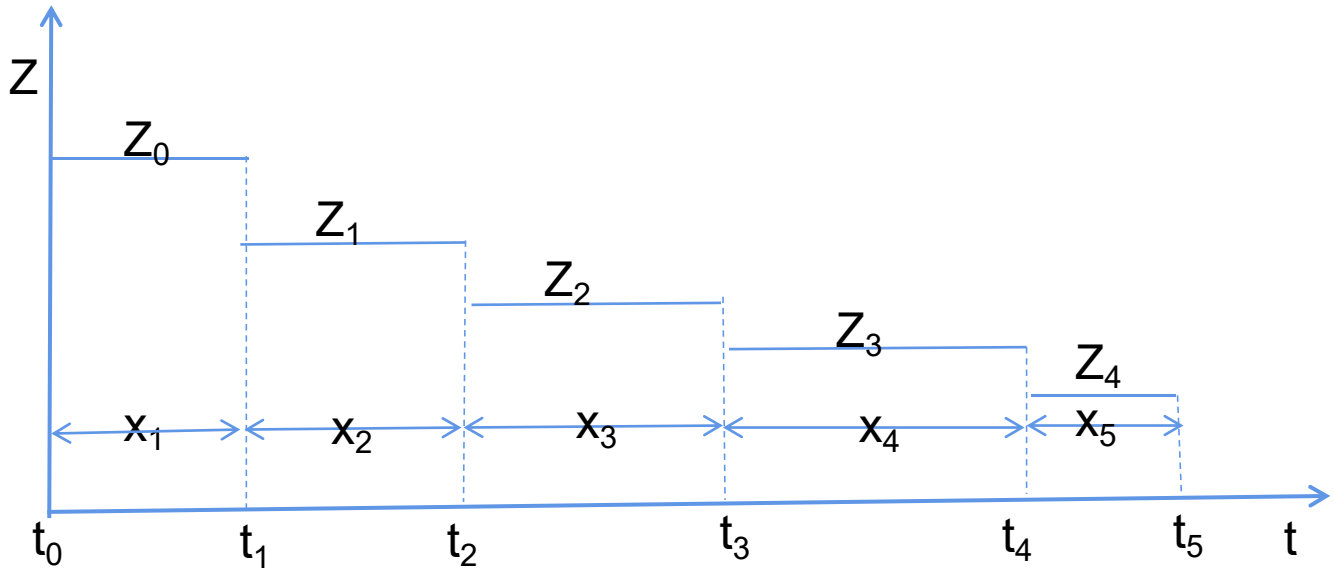

图7-1是J-M模型失效率随时间变化的曲线。图中ti是以时间0点为起点的第i次失效的累计发生时间， 即$x_i=t_i-t_{i-1}$，且i≥1， $t_0=0$。

2.3 软件可靠性评估

Jelinski-Moranda模型

（1） 假设与数据要求：

模型的基本假设如下：

⑤ 错误以相等的可能发生，且相互独立，错误检测率正比于当前程序中的错误数。

⑥ 软件的运行方式与预期的运用方式相似。

2.3 软件可靠性评估

Jelinski-Moranda模型

（2） 模型构造与参数估计：

在假设的基础上，运用可靠性工程学的基本理论，以第i-1次失效为起点的第i次失效发生的时间是一个随机变量，它服从以K（N_0-i+1）为参数的指数分布，其（失效）密度函数为

$$f(x_i)=\mathrm{k}(N_0-i+1)e^{-\mathrm{k}(N_0-i+1)x_i}$$

2.3 软件可靠性评估

Jelinski-Moranda模型

（2） 模型构造与参数估计：

它服从以k(N_0-i+1)为参数的指数分布，其（失效）密度函数为

$$f(x_i)=\mathrm{k}(N_0-i+1)e^{-\mathrm{k}(N_0-i+1)x_i}$$

其(失效)分布函数

$$F(x_i)=\int_0^{x_i} f(x_i)\mathrm{d}x_i=1-e^{-\mathrm{k}(N_0-i+1)x_i}$$

2.3 软件可靠性评估

Jelinski-Moranda模型

（2） 模型构造与参数估计：

其（失效）分布函数

$$F(x_i)=\int_0^{x_i} f(x_i)\mathrm{d}x_i = 1-e^{-\mathrm{k}(N_0-i+1)x_i}$$

其可靠性函数为

$$R(x_i)=1-F(x_i)=e^{-\mathrm{k}(N_0-i+1)x_i}$$

系数k和程序故有错误数N_0确定后，可靠性函数就确定了。

2.3 软件可靠性评估

Jelinski-Moranda模型　系数k和程序故有错误数N_0确定后，可靠性函数就确定了。

（2） 模型构造与参数估计：

假设总共发生了n个失效，则似然函数为

$$L(x_1,\cdots,x_n)=\prod_{i=1}^{n}f(x_i)=\prod_{i=1}^{n}\mathrm{k}(N_0-i+1)e^{-\mathrm{k}(N_0-i+1)x_i}$$

对上式两边取对数，得

$$\ln L(x_1,\cdots,x_n)=\sum_{i=1}^{n}\ln f(x_i)=\sum_{i=1}^{n}(\ln \mathrm{k}(N_0-i+1)-\mathrm{k}(N_0-i+1)x_i)$$

2.3 软件可靠性评估

Jelinski-Moranda模型 系数k和程序故有错误数N_0确定后，可靠性函数就确定了。

（2） 模型构造与参数估计：

假设总共发生了n个失效，则似然函数为 $L(x_1,\cdots,x_n)=\prod_{i=1}^{n} f(x_i)=\prod_{i=1}^{n} \mathrm{k}(N_0-i+1)e^{-\mathrm{k}(N_0-i+1)x_i}$

则模型参数的极大似然法估计值是以下方程组的解：

$$\begin{cases} \hat{\mathrm{k}}=\dfrac{\mathrm{n}}{\hat{N}\left(\sum_{i=1}^{n} x_i\right)-\sum_{i=1}^{n}(i-1)x_i} \\ \sum_{i=1}^{n}\dfrac{1}{\hat{N}-(i-1)}=\dfrac{n}{\hat{N}-(1/\sum_{i=1}^{n} x_i)(\sum_{i=1}^{n}(i-1)x_i)} \end{cases}$$

其中 $\hat{\mathrm{k}}$ 和 $\hat{N}$是模型参数k和N_0的点估计值。
这是一个超越方程，可用数值计算法求解方程组，可以得到模型参数k和N_0的点估计值。

2.3 软件可靠性评估

Jelinski-Moranda模型 系数k和程序固有错误数N_0确定后，可靠性函数就确定了。

（3） 可靠性预计：

运用可靠性工程学的基本理论，利用上述推导出的估计值 $\hat{k}$ 和 $\hat{N}$，可相应地求得以下可靠性参数的估计值：

① 可靠度：

$$R_{n+1}(x) = R(x \mid t_n) = e^{-(\hat{N}-n)\hat{k}x}$$

② 不可靠度：

$$F_{n+1}(x) = 1 - e^{-\hat{k}(\hat{N}-n)x}$$

2.3 软件可靠性评估

Jelinski-Moranda模型 系数k和程序固有错误数N_0确定后，可靠性函数就确定了。

（3） 可靠性预计：

运用可靠性工程学的基本理论，利用上述推导出的估计值 $\hat{k}$ 和 $\hat{N}$，可相应地求得以下可靠性参数的估计值：

③失效密度：

$$f_{n+1}(x) = -\frac{dR_{n+1}(x)}{dx} = (\hat{N}-n)\hat{k}e^{-(\hat{N}-n)\hat{k}x}$$

2.3 软件可靠性评估

Jelinski-Moranda模型

系数k和程序固有错误数N_0确定后，可靠性函数就确定了。

（3） 可靠性预计：

运用可靠性工程学的基本理论，利用上述推导出的估计值 $\hat{k}$ 和 $\hat{N}$，可相应地求得以下可靠性参数的估计值：

④ 平均失效前时间MTTF：给定第n个软件失效发生时刻t_n，由失效独立性假设知，t_n时刻之后软件失效的MTTF为：

$$T_{TF_{n+1}} = E\{X_{n+1} \mid x_1, \cdots, x_n\} = \int_0^{\infty} R_{n+1}(x)\mathrm{d}x = \frac{1}{k(N_0 - n)}$$

则 $$\hat{T}_{TF_{n+1}} = \frac{1}{\hat{k}(\hat{N} - n)}$$

由此我们可以估计出软件可靠性的参数。他们都是依赖于前n次失效时刻，依据这n次失效时间，估计出了J-M模型的参数k和N0。n值越大估计的准确性就越高。

第2.3节作业

3）假定某一软件在测试过程中，已发现了10次失效，其时间分别为

失效编号	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}
失效时间	15	13	9	10	21	23	18	22	17	16

基于J-M模型，估计第11次失效发生时，软件可靠度、不可靠度、失效密度和失效前平均时间MTTF的值。

2.2 软件可靠性分析--软件FTA

2、软件故障树分析（Software Fault Tree Analysis, 软件FTA）、

2.2 软件可靠性分析--软件FEMA与FTA综合分析

1、软件失效模式和影响分析（Software Failure Tree Modes and Effects Analysis, 软件FMEA）、

2、软件故障树分析（Software Fault Tree Analysis, 软件FTA）、

3、将二者结合的软件FEMA与FTA综合分析，以及

4、事件树分析

2.2 软件可靠性分析--软件事件树分析

1、软件失效模式和影响分析（Software Failure Tree Modes and Effects Analysis, 软件FMEA）、

2、软件故障树分析（Software Fault Tree Analysis, 软件FTA）、

3、将二者结合的软件FEMA与FTA综合分析，以及

4、事件树分析

2.2 软件可靠性分析--软件事件树分析

1、软件失效模式和影响分析（Software Failure Tree Modes and Effects Analysis, 软件FMEA）、

2、软件故障树分析（Software Fault Tree Analysis, 软件FTA）、

3、将二者结合的软件FEMA与FTA综合分析，以及

4、事件树分析

第二章作业

1）总结软件可靠性定义以及相关度量参数，字数不少于1000字

2）总结系统级软件FMEA的定义以及分析步骤，并阐述每个步骤功能。

3）

华东师范大学软件学院可信智能团队

Trustworthy Intelligence Group