

国家市场监督管理总局

发 布

202X-XX-XX实施

202X-XX-XX发布

**随机数生成器可信度测评方法**

中华人民共和国国家计量技术规范

**JJF** XXXX—202X

The Test Method for Confidence of Random Number Generators

（征求意见稿)

随机数生成器可信度测评方法

The Test Method for Confidence of Random Number Generators

JJF XXXX-202X

归 口 单 位：全国数字计量技术委员会

主要起草单位：

参加起草单位：

本规范委托全国数字计量技术委员会负责解释

本规范主要起草人：

参加起草人：

目 录

[1 范围 1](#_Toc148294932)

[2 引用文件 1](#_Toc148294933)

[3 名词术语 1](#_Toc148294934)

[4 概述 2](#_Toc148294943)

[5 计量要求 2](#_Toc148294944)

[5.1 样本空间的要求 2](#_Toc148294945)

[5.2 生成机制的要求 3](#_Toc148294946)

[5.3 样本的要求 3](#_Toc148294947)

[6 测试方法集 4](#_Toc148294948)

[6.1 概述 4](#_Toc148294949)

[6.2 专家确认 4](#_Toc148294950)

[6.3 仪器测量 4](#_Toc148294951)

[6.4 样本检验【1】 4](#_Toc148294952)

[7 测评条件 4](#_Toc148294953)

[8 测评 4](#_Toc148294954)

[8.1 样本空间要求的测评 4](#_Toc148294955)

[8.2 生成机制要求的测评 5](#_Toc148294956)

[8.3 样本要求的测评 5](#_Toc148294957)

[9 随机数生成器可信度分级、测评结果与表述 6](#_Toc148294958)

[附录A 8](#_Toc148294959)

[附录B 9](#_Toc148294960)

[附录C 11](#_Toc148294961)

[附录D 14](#_Toc148294962)

引  言

JJF 1071-2010《国家计量校准规范编写规则》、JJF 1001-2011《通用计量术语及定义》共同构成支撑规范制定工作的基础性系列规范。

本规范主要参考JJF 1182-2021《计量器具软件测评指南》、JJF 1365-2012《数字指示秤软件可信度测评方法》、NIST SP 800-22 Rev.1a A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications的技术要求编制而成。

本规范是首次发布。

随机数生成器可信度测评方法

* 1. 范围

本规范规定了涉及权益公平的随机数生成器可信度的测评方法。

本规范适用于涉及权益公平的随机数生成器可信度的测评工作，相关领域亦可以参考使用。

* 1. 引用文件

本规范引用了下列文件：

JJF 1001-2011 通用计量术语及定义

JJF 1182-2021 计量器具软件测评指南

JJF 1365-2012 数字指示秤软件可信度测评方法

GB/T 3358.1-2009 统计学词汇及符号 第1部分:一般统计术语与用于概率的术语

凡是注日期的引用文件，仅注日期的版本适用于本规范；凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本规范。

* 1. 名词术语
		1. 随机现象 random

在一定条件下，出现的可能结果不止一个，事前无法确切知道哪一个结果一定会出现，但大量重复试验中其结果又具有统计规律的现象称为随机现象。

* + 1. 随机试验 random experiment

为了研究随机现象的[统计规律性](https://baike.baidu.com/item/%E7%BB%9F%E8%AE%A1%E8%A7%84%E5%BE%8B%E6%80%A7/8700663?fromModule=lemma_inlink" \t "_blank)，需要对随机现象进行重复观察的试验。

* + 1. 随机数 random number

表征随机试验结果的数字。

* + 1. 随机数生成器 true random number

能够根据条件生成随机数的装置或软件。

注：

1 条件包括但不限于：样本空间、样本点、样本数量和一定的条件概率。

2 装置包括但不限于：存在随机现象的物理装置，例如白噪声装置或者量子随机数装置等；

* + 1. 样本空间 sample space

Ω。在随机试验中所有可能结果的集合。

注：

1 结果可以由一个实际的实验或一个完全假设的实验得到，这些结果可以明确列出，例如可由正整数（1,2,3,…）组成的可列集，也可能是整个实数轴。

2 样本空间是概率空间的第一要素。

[GB/T 3358.1-2009 用于概率的术语 2.1，有修改]

* + 1. 样本点 sample point

随机试验中试验的每个结果称作样本点。

* + 1. 样本 sample

由一个或者多个抽样单元组成的总体的子集。

注：

1 根据所研究总体的情况，样本中的每个单元可是真实或抽象的个体，也可是具体的数值。

2 在 GB/T 3358.2关于样本的定义中，包括一个抽样框的示例。抽样框在从有限总体中抽取随机样本时是必须的。

[GB/T 3358.1-2009 一般统计术语 1.3]

* + 1. 随机数生成器可信度 confidence of random number generator

 随机数生成器生成的随机数的统计规律与其应有的非预期性、均匀性和可测性的一致程度。

* + 1. 非预期性 unpredictability

在给定条件的样本空间中，根据已知历史样本，随机数生成器不具有被相对准确预测后序随机数字的特性。

* + 1. 均匀性 uniformity

在给定条件的样本空间中，样本点的概率是相等的。

* + 1. 可测性 scalability

在随机数生成器生成的任一随机数样本中，其统计规律应具有可被验证的特性。

* + 1. 样本数字特征 sample number feature

描述样本的某些特征的数字，包括但不限于均值、方差、概率分布等。

* + 1. 数字样本空间 digital sample space

由计算机模拟实现的随机试验中所有可能结果的集合。

* + 1. 实体样本空间 entity sample space

非数字样本空间的样本空间统称。

* 1. 概述

如图1所示，随机数生成器一般由至少一个实体或数字形成的样本空间，至少一种按统计规律的随机数生成机制，以及必要时的样本显示媒介构成。随机数生成机制可以采用物理或软件方式实现。



图1 随机数生成器原理

* 1. 计量要求
		1. 样本空间的要求
			1. 实体样本空间的要求

a）实体样本空间的样本点如果不可分割，则该样本空间中每个样本点应具有相同的物理化学性质，包括但不限于空间、时间、机械结构、形状、质量、温度、光学、电磁学特性等；其物理化学特性以及样本点与样本点结合方式应具有不影响随机数生成机制按统计规律进行工作的特性。

b）实体样本空间的样本点如果可分割，则该样本空间中每个样本点应具有相同的物理化学性质，包括但不限于空间、时间、机械结构、形状、质量、温度、光学、电磁学特性等；其物理化学特性以及样本点与样本点在空间上的接触和力学上相互作用应具有不影响随机数生成机制按统计规律进行工作的特性。

c）不同的实体样本空间如果独立，则应不具有相关性；如果关联，则应明示。

* + - 1. 数字样本空间的要求

数字样本空间应明示。

* + - 1. 多个物理或数字样本空间组成的随机数样本空间的要求
1. 其中的实体样本空间应满足要求5.1.1；
2. 其中的数字样本空间应满足要求5.1.2；
3. 不同物理或数字样本空间如果独立，则应不具有相关性；
4. 不同物理或数字样本空间如果关联，则应明示。
	* 1. 生成机制的要求
			1. 统计规律的要求

统计规律应明示，且统计规律所应用的样本空间应符合5.1。

* + - 1. 生成机制的要求
1. 基于物体、物质的特性、现象、物理定律和事件等实现的随机数生成机制，其统计规律应符合5.2.1；
2. 基于软件实现的随机数生成机制，其统计规律应符合5.2.1；
3. 由物体、物质的特性、现象、物理定律、事件等与软件联合实现的随机数生成机制，其统计规律应符合5.2.1；
4. 在随机数生成器的使用期间，随机数生成机制应不受利益攸关方的影响；
5. 在随机数生成器的使用期间，与物体、物质的特性、现象、物理定律和事件等相关随机数生成机制，应不受包括但不限于空间、时间、机械结构、形状、质量、温度、光、电磁等因素的影响；
6. 在随机数生成器的使用期间，与软件相关的随机数生成机制，应不受软件算法、功能、参数、接口等因素的影响。
	* 1. 样本的要求
			1. 样本数字特征的要求

 样本数字特征应明示，且数字特征应与生成机制统计规律的要求5.2.1一致。

* + - 1. 样本媒介的要求
1. 在权益多方约定的条件下，样本媒介具有不被利益相关方获得确定样本点的保护措施，包括但不限于通过物理的、化学的和数学的方式获得样本媒介中的确定样本点；
2. 在权益多方约定的条件下，样本媒介应该具有及时准确可靠合法地显示样本及样本中所含样本点的特性；
3. 在权益兑现时，样本媒介应能唯一可靠合法地被利益攸关方确认。
	1. 测试方法集
		1. 概述

随机数生成器可信度测评方法包括专家确认、仪器测量和样本检验三大类。

* + 1. 专家确认

专家确认包括资料走读和目视确认两种。

* + 1. 仪器测量

采用具有有效检定、校准或检测证书的仪器进行测量。

* + 1. 样本检验【1】

包括比例检验、块中比例检验、游程总数检验、游程分布检验、 块内最长游程检验、样本点矩阵检验【2】、离散傅里叶变换检验、扑克检验、重叠模板匹配检验、通用统计检验、线性复杂度检验、近似熵检验、累积和检验、多元推导检验【3】和自相关检验共十五种检验法。

注：

1 参见附录D；

2 参见附录D二进制矩阵检验的数学原理；

3 参见附录D二元推导检验。

* 1. 测评条件

被测方需提供以下资料：

1. 随机数生成器说明资料，原理资料；
2. 随机数生成器；
3. 其他支撑文件，如用户手册等。
	1. 测评
		1. 样本空间要求的测评
			1. 样本空间要求的文档测评

采用走读的方式，判断文档中样本空间的描述与5.1的符合性和一致性。如果满足符合性和一致性，则样本空间要求的文档测评得1分，否则得0分。

* + - 1. 实体样本空间要求的测评

8.1.2.1对样本空间不同样本点的物理化学特性，采用仪器测量的方法，获得不同样本点的物理化学特性的量值和不确定度，判断样本点与文档中样本空间描述的符合性和一致性。如果满足符合性和一致性，则样本空间要求测评得分为1，否则得分为0。

 8.1.2.2 如果样本点不可分割，采用专家确认、仪器测量或二者结合的方法，判断样本点与样本点结合方式是否具有不影响随机数生成机制按统计规律进行工作的特性；如果样本点可分割，采用仪器测量方法，判断样本点在空间上的接触和力学上相互作用是否具有不影响随机数生成机制按统计规律进行工作的特性。如果具有，则得分为1，否则得分为0。

8.1.2.3 在样本空间中有多个实体样本空间的前提下，如果不同的实体样本空间独立，则采用专家确认、仪器测量或二者结合的方法判断不同实体样本空间的相关性，若不相关，则得分为1，否则得分为0；如果不同的实体样本空间不独立，则采用专家确认、仪器测量或二者结合的方法判断不同实体样本空间的关联与文档中描述的符合性和一致性，如果满足符合性和一致性，则得分为1，否则得分为0。

* + - 1. 数字样本空间要求的测评

采用走读的方式，确认是否满足5.1.2的要求。如果满足，则得分为1，否则得分为0。

* + - 1. 多个物理或数字样本空间组成的随机数样本空间要求的测评

8.1.4.1 适用时，依据8.1.2 开展测评；

8.1.4.2 适用时，依据8.1.3 开展测评；

8.1.4.3 适用时，采用专家确认、仪器测量、样本检验或三者结合的方法，判断是否满足5.1.3 中c）的要求，如果满足，则得分为1，否则得分为0；

8.1.4.4 适用时，采用专家确认、仪器测量、样本检验或三者结合的方法，判断是否满足5.1.3.中d）的要求，如果满足，则得分为1，否则得分为0。

* + - 1. 样本空间要求的测评得分

当所有适用的测评项均得1分时，样本空间要求的测评得分才为1。

* + 1. 生成机制要求的测评
			1. 生成机制要求文档的测评

采用文本走读的方式，确认是否满足5.2.1的要求。如果满足，则得分为1，否则得分为0。

* + - 1. 生成机制要求的测评

8.2.2.1 如适用，采用专家确认和仪器测量的方式，判断是否满足5.2.2 中a）的要求。如果满足，则得分为1，否则得分为0。

8.2.2.2 如适用，采用专家确认的方式，判断是否满足5.2.2 中b）的要求。如果满足，则得分为1，否则得分为0。

8.2.2.3 如适用，采用专家确认和仪器测量的方式，判断是否满足5.2.2 中c）的要求。如果满足，则得分为1，否则得分为0。

8.2.2.4 采用专家确认的方式，判断是否满足5.2.2 中d）的要求。如果满足，则得分为1，否则得分为0。

8.2.2.5 如适用，采用专家确认和仪器测量的方式，判断是否满足5.2.2中 e）的要求。如果满足，则得分为1，否则得分为0。

8.2.2.6 如适用，采用专家确认的方式，参考JJF 1365 和 JJF 1182 中的条款，判断是否满足5.2.2中 f）的要求。如果满足，则得分为1，否则得分为0。

* + - 1. 生成机制要求的测评得分

当所有适用的测评项均得1分时，生成机制要求的测评得分才为1。

* + 1. 样本要求的测评
			1. 样本要求文档的测评

采用走读的方式，确认是否满足5.3.1的要求。如果满足，则得分为1，否则得分为0。

* + - 1. 样本要求样本检验的测评

采用样本检验中包含的方法，确认是否满足5.3.1的要求。其得分按公式（1）计算

 （1）

其中：

 ——样本要求的样本检验测评得分；

 ——样本检验包含的第种方法，当检验通过时，；否则，；

 ——系数。当时，；否则，。

* + - 1. 样本媒介要求的测评

采用专家确认和仪器测量的方式，判断是否满足5.3.2的要求。如果满足或不适用，则得分为1，否则得分为0。

* + - 1. 样本要求的测评得分

 （2）

其中：

——样本要求测评得分；

——样本要求的文档测评得分；

——样本要求样本检验的测评得分；

——样本媒介要求的测评得分。

* 1. 随机数生成器可信度分级、测评结果与表述

9.1 随机数生成器可信度分级

随机数生成器可信度分级见表1。

表1 随机数生成器可信度分级表

|  |  |  |
| --- | --- | --- |
| 级别 | 含义 | 测评得分范围 |
| A | 高可信 | [90，100] |
| B | 中可信 | [72，90) |
| C | 低可信 | [60，72) |
| D | 不可信 | [0，60） |

9.2 随机数生成器可信度测评结果与表述

按公式（3）计算出随机数生成器可信度的测评总分：

(3)

式中：

——随机数生成器可信度测评总分；

——样本空间要求的测评得分；

——生成机制要求的测评得分；

——样本要求的测评得分；

按表1中可信度测评得分范围，给出相应随机数生成器的可信度级别。

测评项目的记录格式参见附录B，测评项目的报告格式参见附录C。

附录A

表A.1 随机数生成器可信度测评项目表

| **序号** | **测评项目** | **技术要求条款** | **测试方法条款** |
| --- | --- | --- | --- |
| 1 | 样本空间 | 样本空间要求的文档 | 5.1 | 8.1.1 |
| 实体样本空间 | 5.1.1 | 8.1.2 |
| 数字样本空间 | 5.1.2 | 8.1.3 |
| 多个物理或数字样本空间组成的随机数样本空间 | 5.1.3 | 8.1.4 |
| 2 | 生成机制 | 生成机制要求文档 | 5.2 | 8.2.1 |
| 统计规律 | 5.2.1 | 8.2.2 |
| 生成机制 | 5.2.2 | 8.2.3 |
| 3 | 样本 | 样本要求文档 | 5.3 | 8.3.1 |
| 样本数字特征 | 5.3.1 | 8.3.2 |
| 样本媒介 | 5.3.2 | 8.3.3 |

附录B

 随机数生成器可信度测评记录格式

 随机数生成器可信度测评的记录是基于本规范中对随机数生成器的基本要求和解释。本记录描述被测随机数生成器和本规范要求的一致性。

表B.1测评基本信息及资料审查格式

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 申请编号 |  |  随机数生成器名称 |  | 版本号 |  |
| 申请单位名称 |  | 申请单位地址 |  |
| 联系人 |  | 电话 |  | 传真 |  |
| 依据的技术文件（代号和名称） |  |
| 测评的目的和方法 |  |
| 参考环境条件及地点 |  |
| 温度 |  | 地点 |  |
| 相对湿度 |  | 静压 |  |
| 开发环境 |  | 操作系统 |  |
| 测评结论 |  |
| 测评 |  | 审核 |  | 日期 |  |
| 提交资料清单 |
| 依据 | 资料名称 | 是否提交 | 备注 |
| 7 | 随机性说明资料，原理资料  |  |  |
| 7 | 随机数生成器 |  |  |
| 7 | 其他支撑文件，如用户手册等 |  |  |

表B.2样本空间测评记录格式

|  |  |
| --- | --- |
| 测评工具 |  |
| 依据 | 测评项目 | 测评方法 | 测评得分 | 备注 |
| 5.1 | 样本空间要求的文档 | 8.1.1 |  |  |
| 5.1.1 | 实体样本空间 | 8.1.2 |  |  |
| 5.1.2 | 数字样本空间 | 8.1.3 |  |  |
| 5.1.3 | 多个物理或数字样本空间组成的随机数样本空间 | 8.1.4 |  |  |
| 样本空间测评总分 |  |  |

表B.3生成机制测评记录格式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 依据 | 测评项目 | 测评方法 | 测评得分 | 备注 |
| 5.2 | 生成机制要求文档 | 8.2.1 |  |  |
| 5.2.1 | 统计规律 | 8.2.2 |  |  |
| 5.2.2 | 生成机制 | 8.2.3 |  |  |
| 生成机制测评总分 |  |  |

表B.4样本测评记录格式

|  |  |
| --- | --- |
| 测评工具 |  |
| 依据 | 测评项目 | 测评方法 | 测评得分 | 备注 |
| 5.3 | 样本要求文档 | 8.3.1 |  |  |
| 5.3.1 | 样本数字特征 | 8.3.2 |  |  |
| 5.3.2 | 样本媒介 | 8.3.3 |  |  |
| 样本测评总分 |  |

附录C

随机数生成器可信度测评报告格式

报告编号：

|  |  |
| --- | --- |
| 随机数生成器名称及版本号： |  |
| 申请单位名称： |  |
| 申请单位地址： |  |

测评单位：（盖章）

测评：审核：批准：

日期：日期：日期：

第页共页

报告编号：

|  |
| --- |
| 参照的技术文件（代号和名称）： |
| 测评的目的和方法： |
| 参考环境条件及地点 |
| 温度 |  | 地点 |  |
| 相对湿度 |  | 静压 |  |
| 软件开发环境 |  | 操作系统 |  |
| 处理器 |  | 其它 |  |
| 测评要求 |
| 编号 | 测评项目 | 对应要求 | 测评方法 |
| 1 | 样本空间 | 5.1 | 8.1 |
| 2 | 生成机制 | 5.2 | 8.2 |
| 3 | 样本 | 5.3 | 8.3 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 所用测评工具 |
| 名称 | 版本 |
|  |  |
|  |  |
|  |  |
|  |  |

注：本报告的测试结果仅对所测试的样品/样机/对象有效。

第页共页

报告编号：

1 测评结论

|  |
| --- |
| 随机数生成器可信度为xx%，满足（不满足）JJFXXX-XXXX的要求。 |

2测评结果

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 依据 | 测评项目 | 测评方法 | 测评得分 | 备注 |
| 5.1 | 样本空间要求的文档 | 8.1.1 |  |  |
| 实体样本空间 | 8.1.2 |  |  |
| 数字样本空间 | 8.1.3 |  |  |
| 多个物理或数字样本空间组成的随机数样本空间 | 8.1.4 |  |  |
| 5.2 | 生成机制要求文档 | 8.2.1 |  |  |
| 统计规律 | 8.2.2 |  |  |
| 生成机制 | 8.2.3 |  |  |
| 5.3 | 样本要求文档 | 8.3.1 |  |  |
| 样本数字特征 | 8.3.2 |  |  |
| 样本媒介 | 8.3.3 |  |  |

第页共页

附录D

D.1比例检验

D.1.1 检验目的

检测随机数字序列中0和1出现的次数总和所占的比例。检验的目的是确定在被测随机数字序列中，每个数字出现的次数比例应接近于1/2。

D.1.2 参数定义

：序列的长度。

：由正在测试的RNG或PRNG生成的比特序列。

D.1.3 检验流程

（1）转换为：将被测随机数字数列的0和1分别转换成-1和1，

，其中。

例如，所以且

（2）计算检验统计量。

对于本节示例，

（3）计算值，

对于本节示例，值

D.1.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.1.5 结论和结果解释

对于本节示例，值=0.527089＞0.01，则被测序列是随机的。

D.1.6 数列长度建议

建议测试的每个序列至少由100个比特组成（即）。

D.2块中比例检验

D.2.1 检验目的

检验随机数字序列的每一块中0和1出现的次数所占的比例。检验的目的是确定在被测随机数字序列的子序列中，0和1出现的次数比例应接近于1/2。

D.2.2 参数定义

：每个块的长度。

：序列的长度。

：块的个数。

：由正在测试的RNG或PRNG生成的比特序列。

D.2.3 检验流程

（1）将输入序列划分为的非重叠块，丢弃掉未使用的块。

例如，，，将创建3个块（），包含011、001、101，末位的0被舍弃。

（2）确定每个块中1的比例，，其中。

对于本节示例，，，。

（3）计算统计量，。

对于本节示例，

（4）计算值，igamc是定义的的不完全函数。

对于例子，值= 。

D.2.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.2.5 结论和结果解释

对于本节示例，值=0.801252＞0.01，则被测序列是随机的。

D.2.6 数列长度建议

建议测试的每个序列至少由100个比特组成（即）。注意，。块大小应选择为和。

D.3游程检验

D.3.1 检验目的

检验的目的是确定不同长度的1和0的运行次数是否与随机序列的预期一致。

D.3.2 参数定义

：序列的长度。

：由正在测试的RNG或PRNG生成的比特序列。

：游程总数（包含0的游程也包含1的游程）。

D.3.3 检验流程

（1）计算输入序列中1的预测试比例：

例如，，

（2）确定先决条件比例测试是否通过。如果，则不需要执行此游程检验。如果测试不适用，则将P值设置为0.0000。其中。

对于本节示例，，。由于观测值在选定的范围内，所以此游程检验是可适用的。

（3）计算统计量，如果，那么，反之。

对于本节示例，因为，所以

。

（4）计算值

对于本节示例，值。

D.3.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.3.5 结论和结果解释

对于本节示例，值=0.147232＞0.01，则被测序列是随机的。

D.3.6 数列长度建议

建议测试的每个序列至少由100个比特组成（即）。

D.4块内最长游程检验

D.4.1 检验目的

检验的目的是确定测试序列中最长序列的长度是否与随机序列中预期的最长序列长度一致。

D.4.2 参数定义

：序列的长度。

：每个块的长度。

|  |  |
| --- | --- |
| 的最小长度 |  |
| 128 | 8 |
| 6272 | 128 |
| 750000 |  |

：块的个数。

D.4.3 检验流程

（1）将序列分为位块。

例如，



其中，。

（2）将每个块中1的最长运行的频率列成表，并分类，其中每个单元格包含给定长度的1的运行的次数。

对于本节示例，

|  |  |  |  |
| --- | --- | --- | --- |
| 子块 | 最大游程 | 子块 | 最大游程 |
| 11001100 | 2 | 00010101 | 1 |
| 01101100 | 2 | 01001100 | 2 |
| 11100000 | 3 | 01010001 | 1 |
| 01001101 | 2 | 01010001 | 1 |
| 00010011 | 2 | 11010110 | 2 |
| 10000000 | 1 | 11010111 | 3 |
| 11001100 | 2 | 11100110 | 3 |
| 11011000 | 2 | 10110010 | 2 |

（最大游程是1的有4个，最大游程是2的有9个，最大游程是3的有3个，最大游程是4的有0个）

（3）计算 其中由下表给出：

|  |  |
| --- | --- |
| 类别 | 概率 |
|  |  |
|  |  |
|  |  |
|  |  |

和的值由决定：

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 8 | 3 | 16 |
| 128 | 5 | 49 |
|  | 6 | 75 |

对于本节示例，



（4）计算值，igamc是不完全伽马函数。

D.4.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.4.5 结论和结果解释

对于本节示例，值=0.180609＞0.01，则被测序列是随机的。

D.4.6 数列长度建议

建议测试的每个序列至少由100个比特组成（即）。注意，。块大小应选择为和。

D.5二进制矩阵检验

D.5.1 检验目的

检验随机数字序列的子矩阵的秩。检验的目的是确定在被测随机数字序列中，原始序列的固 定长度子串的线性相关。

D.5.2 参数定义

：序列的长度。

：每个矩阵的行数。

：每个矩阵的列数。

D.5.3 检验流程

（1）将序列划分为位不相交块，存在个块。

例如，如果，，，最后两位0和1将被舍弃。这两个矩阵为和。

（2）考虑每一个矩阵的二进制秩。

对于本节示例，第一个矩阵的秩为2（），第二个矩阵的秩为3（）。

（3）令秩为的矩阵的数量（满秩）；令秩为的矩阵的数量；

剩余矩阵的数量。

对于本节示例，。

（4）计算



对于本节示例，

。

（5）计算值。

对于本节示例，值。

D.5.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.5.5 结论和结果解释

对于本节示例，值=0.741948＞0.01，则被测序列是随机的。

D.5.6 数列长度建议

的概率已经被计算并插入到测试代码中。可以选择和的其他选择，但是需要计算概率。要测试的最小位数必须使得（即至少创建38个矩阵）。对于，要测试的每个序列应该至少由38912个比特组成。

D.6扑克检验

D.6.1 检验目的

检验随机数字序列中预先指定的目标模板出现的次数。检验的目的是检验产生过多给定非周期模式的生成器。

D.6.2 参数定义

：每个模板的长度，模板是目标字符串。

：被测试的字符串的长度。

：由正在测试的RNG或PRNG生成的比特序列。

：要匹配的位模板，是一个由0和1组成的字符串(长度为)。

：要测试的子串的长度。

：独立块的数量。

D.6.3 检验流程

（1）将序列划分为个长度为的独立块。

对于例子，，所以。如果，那么两个块为1010010010和1110010110。

（2）令是模板出现在块中的次数。通过在序列上创建一个位窗口，将窗口内的位与模板进行比较，来进行匹配的搜索。如果没有匹配，窗口将滑动一位。如果有匹配，窗口滑动位，例如如果当前窗口含3到5位，那么下一个窗口将包含6到8位。

对于例子，其中，

|  |  |  |
| --- | --- | --- |
| 比特位置 | 块1 | 块2 |
| 比特 |  | 比特 |  |
| 1-3 | 101 | 0 | 111 | 0 |
| 2-4 | 010 | 0 | 110 | 0 |
| 3-5 | 100 | 0 | 100 | 0 |
| 4-6 | 001 | 增加到1 | 001 | 增加到1 |
| 5-7 | 不检查 |  | 不检查 |  |
| 6-8 | 不检查 |  | 不检查 |  |
| 7-9 | 001 | 增加到2 | 011 | 1 |
| 8-10 | 010 | 2 | 110 | 1 |

所以。

（3）在假设随机的情况下，计算理论均值和方差。

，

对于本节示例，，。

（4）计算。

对于本节示例，。

（5）计算值。对于每个模板，都要计算值。

对于例子，值。

D.6.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.6.5 结论和结果解释

对于本节示例，值=0.344154＞0.01，则被测序列是随机的。

D.6.6 数列长度建议

应选择，使，以确保值有效。此外，确保。

D.7重叠模板匹配检验：

D.7.1 检验目的

检验随机数字序列中预先指定的目标模板出现的次数。与扑克检验的区别是在搜索到了指定模板后，只向后移动一位就继续搜索。

D.7.2 参数定义

：以位为单位的模板长度。

：位串的长度。

：由正在测试的RNG或PRNG生成的比特序列。

：要匹配的位模板。

：自由度的数目。

：要测试的子串的长度。

：独立块的数量。

D.7.3 检验流程

（1）将序列划分为个长度为的独立块。

例如，，其中。如果，则五个块为1011101111，0010110100，0111001011，1011111000，0101101001。

（2）计算每个块中出现的数目。通过递增数组（其中）记录在每个块中的出现次数。当子串中没有出现时递增，当出现一次时递增，出现5次及以上时递增。

对于本节示例，如果，

|  |  |  |
| --- | --- | --- |
| 序列段位置 | 序列段 | 的出现次数 |
| 1-2 | 10 | 0 |
| 2-3 | 01 | 0 |
| 3-4 | 11 | 增加到1 |
| 4-5 | 11 | 增加到2 |
| 5-6 | 10 | 2 |
| 6-7 | 01 | 2 |
| 7-8 | 11 | 增加到3 |
| 8-9 | 11 | 增加到4 |
| 9-10 | 11 | 增加到5 |

对于块1,11出现了5次，递增，所以。

在块2中，有2个；在块3中，有3个；在块4中，有4个，在块5中，有1个，所以在所有块检查完后。

（3）计算和来用于计算类对应的理论概率的值,。

对于本节示例，，。

（4）计算，其中





对于本节示例，



（5）计算值

对于本节示例，值=。

D.7.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.7.5 结论和结果解释

对于本节示例，值=0.274932＞0.01，则被测序列是随机的。

D.7.6 数列长度建议

目前，建议或。如果需要其他值，请按如下方式选择这些值：

1. ；
2. ；
3. ；
4. ；
5. 。注意，对于除5以外的值，需要重新计算值。

D.8通用统计检验：

D.8.1 检验目的

检验随机数字序列中匹配模板之间相距的位数。检验的目的是检验序列是否可以在不丢失信息的情况下被显著压缩。

D.8.2 参数定义

：每个块的长度。

：初始化序列中的块数。

：序列的长度。

：由正在测试的RNG或PRNG生成的比特序列。

D.8.3 检验流程

（1）位序列被划分为两个段：初始段由个长度的不重叠块组成，测试段由个长度的不重叠块组成。在序列末尾未形成完整长度的块的剩余位被丢弃。第一个块用于初始化测试。剩下的块是测试块。

例如，，这时。如果，那么

，初始段为01011010，测试段为011101010111。

|  |  |  |
| --- | --- | --- |
| 块 | 类型 | 块内容 |
| 1 | 初始段 | 01 |
| 2 | 01 |
| 3 | 10 |
| 4 | 10 |
| 5 | 测试段 | 01 |
| 6 | 11 |
| 7 | 01 |
| 8 | 01 |
| 9 | 01 |
| 10 | 11 |

（2）使用初始化段，为每个可能的位值创建一个表。每个位块最后出现的块号在表中被记录下来（对于从1到，，其中是第个位块内容的十进制表示。）

|  |  |
| --- | --- |
|  | 可能的值 |
| 00() | 01() | 10() | 11() |
| 初始化 | 0 | 2 | 4 | 0 |

（3）检查测试段中的每个中的块，并确定自最后一次出现相同的中的块（即）以来的块的数量；

用当前块的位置替换表中的值（例如）；

将相同位块重复出现之间的计算距离加到块中检测到的所有差异的累加和（即）.

对于例子，

对于块5（第一个测试块）：块5是‘01’，对应表中的，表中‘01’对应的最后出现的块变为5，；

对于块6：块6是‘11’，对应表中的，表中‘11’对应的最后出现的块变为6，；

对于块7：块7是‘01’，对应表中的，表中‘01’对应的最后出现的块变为7，；

对于块8：块8是‘01’，对应表中的，表中‘01’对应的最后出现的块变为8，；

对于块9：块9是‘01’，对应表中的，表中‘01’对应的最后出现的块变为9，；

对于块10：块9是‘11’，对应表中的，表中‘11’对应的最后出现的块变为10，；

（4）计算检验统计量：。

对于本节示例，。

（5）计算值。其中，。

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  6 | 5.2177052 | 2.954 |
| 7 | 6.1962507 | 3.125 |
| 8 | 7.1836656 | 3.238 |
| 9 | 8.1764248 | 3.311 |
| 10 | 9.1723243 | 3.356 |
| 11 | 10.170032 | 3.384 |
| 12 | 11.168765 | 3.401 |
| 13 | 12.168070 | 3.410 |
| 14 | 13.167693 | 3.416 |
| 15 | 14.167488 | 3.419 |
| 16 | 15.167379 | 3.421 |

D.8.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.8.5 结论和结果解释

表中没有的期望值和方差，因为长度为2的块不建议进行测试。

D.8.6 数列长度建议

该测试需要一个长的比特序列（），该序列被划分为两段比特块，其中应选择为。第一段由个初始段组成，其中应选择，使。第二段由个测试段组成，其中。

D.9线性复杂度检验：

D.9.1 检验目的

检验的目的是确定序列是否足够复杂，可以被认为是随机的。

D.9.2 参数定义

：块的长度。

：序列的长度。

：由正在测试的RNG或PRNG生成的比特序列。

：自由度的数量。

D.9.3 检验流程

（1）将长度为的序列划分为个独立的长度为的块，其中。

（2）使用Berlekamp-Massey算法，确定个块中每个块的线性复杂度。是生成块中所有位的最短线性反馈移位寄存器序列的长度。在任何位序列中，当以模2相加时，这些位的一些组合产生序列中的下一位（位）。

例如，如果，并且要测试的块是1101011110001，则，并且通过将4比特子序列内的第1比特和第2比特相加来产生该序列，以产生下一比特（第5比特）。

（3）在随机性假设下，计算理论平均值：



对于本节示例，。

（4）对于每个子序列，计算的值，其中



对于本节示例，。

（5）将值记录在中，如下所示：

如果，将增加1；，将增加1；，将增加1；，将增加1；，将增加1；，将增加1；，将增加1。

（6）计算，其中，，，，，，。

（7）计算值。

D.9.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.9.5 数列长度建议

选择。的值必须在和的范围内，结果才能有效。

D.10连续检验：

D.10.1 检验目的

检验的重点是整个序列中所有可能重叠的位模式的频率。检验的目的是确定出现个位重叠模式的次数是否与预期的随机序列大致相同。当时，连续检验等同于比例检验。

D.10.2 参数定义

：每个块的长度。

：序列的长度。

D.10.3 检验流程

（1）形成一个增广序列：当有余数时，将序列的前位附加到序列的末尾，从而扩展序列。

例如，给定，如果，那么。如果，那么。如果，那么等于原序列。

（2）确定所有可能重叠的位块、所有可能重叠的位块和所有可能重叠的位块的频率。令代表位模式的频率；令代表位模式的频率；令代表的位模式的频率。

对于本节示例，当时，。所有3位块的频率是

；

位块的频率为；

位块的频率为。

（3）计算





对于本节示例，





（4）计算，。

对于本节示例，，



（5）计算和。

对于本节示例，，

D.10.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.10.5 结论和结果解释

对于本节示例，，，则被测序列是随机的。

D.10.6 数列长度建议

选择和，使得。

D.11近似熵检验：

D.11.1 检验目的

检验随机数字序列中整个序列的所有可能的重叠的位模板的概率。检验的目的是比较两个连续或相邻长度（和）的重叠块的频率与随机序列的预期结果。

D.11.2 参数定义

：每个块的长度。

：序列的长度。

D.11.3 检验流程

（1）通过从序列开始的位添加到序列的末尾来创建个重叠的位序列。

例如，如果，那么。将序列的前两位添加到末尾变成。

（2）对个重叠块进行频率计数。设可能的位值的计数用表示，其中为位序列的值。

对于本节示例，重叠的位块（其中 =3）变成。计算结果为的可能的位序列：



（3）对于每个，计算。

对于本节示例，

。

（4）计算，其中，。

对于本节示例，。

（5）重复1-4步，将替换为。

Step1：将前位添加到末尾，序列变为。

Step2：重叠块为。

计算的值为：

，其余为0。

Step3：，其余为0。

Step4：。

（6）计算检验统计量：，其中。

对于本节示例，，



（7）计算值。

对于本节示例，值。

D.11.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.11.5 结论和结果解释

对于本节示例，值，则被测序列是随机的。

D.11.6 数列长度建议

选择和，使得。

D.12累计和检验：

D.12.1 检验目的

检验随机数字序列中由序列中调整过的数字进行累积求和得到的最大范围内的随机游程距离。

D.12.2 参数定义

：用于通过输入序列（）向前或通过序列（）向后应用测试的开关。

：序列的长度。

D.12.3 检验流程

（1）生成标准化序列：将0和1根据转化为-1和1。

例如，对于，那么。

（2）计算较大子序列的部分和，每个子序列从（）或（）开始。



（3）计算检验统计量，其中是部分和的绝对值中最大的一个。

对于本节示例，。

（4）计算

对于本节示例，。

D.12.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.12.5 结论和结果解释

对于本节示例，，则被测序列是随机的。

D.12.6 数列长度建议

建议测试的每个序列至少由100个比特组成（即）。

D.13自由游程检验：

D.13.1 检验目的

检验的目的是确定一个周期内对特定状态的访问次数是否偏离了随机序列的预期。

D.13.2 参数定义

：序列的长度。

*：*由正在测试的RNG或PRNG生成的比特序列。

D.13.3 检验流程

（1）生成标准化序列：将0和1根据转化为-1和1。

例如，如果，那么，。

（2）计算从开始的连续较大子序列的部分和，形成集合：

对于本节示例，。

（3）在前后加0，形成一个新的序列。

对于本节示例，

（4）令，其中0是出现在起始0之后的值。同时也是中的周期数，其中的周期数称为包含着从0开始，到下一个0结束的的子序列。

对于本节示例，如果，那么（这是中的第3、5、12位置的0）。同时它也有3个周期，。

（5）对于每个周期，对于每个非0且值在中的，计算每个周期中每个的频率。

对于本节示例，

|  |  |
| --- | --- |
|  | 周期 |
| 周期1 | 周期2 | 周期3 |
| -4 | 0 | 0 | 0 |
| -3 | 0 | 0 | 0 |
| -2 | 0 | 0 | 0 |
| -1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 3 |
| 2 | 0 | 0 | 3 |
| 3 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 |

（6）对于的八种状态，计算状态在所有周期中恰好出现次的周期的总数，对于，所有≥5的频率都存储在中，。

对于本节示例：

（在周期2,3中出现了0次）

（在周期1中出现了1次）

（在所有周期中出现2-5次的次数都为0）；

（在周期1中出现了0次）

（在周期2中出现了1次）

（在周期3中出现了3次）

（在所有周期中出现2、4、5次的次数都为0）

|  |  |
| --- | --- |
|  | 周期数 |
| 0 | 1 | 2 | 3 | 4 | 5 |
| -4 | 3 | 0 | 0 | 0 | 0 | 0 |
| -3 | 3 | 0 | 0 | 0 | 0 | 0 |
| -2 | 3 | 0 | 0 | 0 | 0 | 0 |
| -1 | 2 | 1 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| 2 | 2 | 0 | 0 | 1 | 0 | 0 |
| 3 | 3 | 0 | 0 | 0 | 0 | 0 |
| 4 | 3 | 0 | 0 | 0 | 0 | 0 |

（7）对于的八种状态，计算检验统计量，将生成8个检验统计量。







|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  | 0.5000 | 0.2500 | 0.1250 | 0.0625 | 0.0312 | 0.0312 |
|  | 0.7500 | 0.0625 | 0.0469 | 0.0352 | 0.0264 | 0.0791 |
|  | 0.8333 | 0.0278 | 0.0231 | 0.0193 | 0.0161 | 0.0804 |
|  | 0.8750 | 0.0156 | 0.0137 | 0.0120 | 0.0105 | 0.0733 |
|  | 0.9000 | 0.0100 | 0.0090 | 0.0081 | 0.0073 | 0.0656 |
|  | 0.9167 | 0.0069 | 0.0064 | 0.0058 | 0.0053 | 0.0588 |
|  | 0.9286 | 0.0051 | 0.0047 | 0.0044 | 0.0041 | 0.0531 |

（8）对于每个状态，计算，将产生8个值。

对于本节示例，当，。

D.13.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.13.5 结论和结果解释

对于本节示例，，则被测序列是随机的。

D.13.6 数列长度建议

建议测试的每个序列至少由1000000个比特组成（即）。

D.14 随机偏移变化检验

D.14.1 检验目的

检验的重点是在累计和随机游走中访问特定状态的总次数。

D.14.2 参数定义

：序列的长度。

*：*由正在测试的RNG或PRNG生成的比特序列。

D.14.3 检验流程

（1）形成标准化序列X，将0和1转换成-1和1，通过，其中

。

例如，如果，那么，。

（2）计算较大子序列的部分和，每个都起始于。形成集合。



对于本节示例，集合。

（3）在集合前后加0，形成一个新的序列，即。

对于本节示例，，得到的随机游走如下所示：



（4）对于的18个非零状态的每一个，计算状态在所有个周期中出现的总次数。

对于本节示例，，其它的。

（5）对于每个，计算值，18个值被计算出来。

对于本节示例，当时，值。

D.14.4 决策规则

如果计算的值，则得出该序列为非随机序列的结论。否则，得出序列是随机的结论。

D.14.5 结论和结果解释

对于本节示例，，则被测序列是随机的。

D.14.6 数列长度建议

建议测试的每个序列至少由1000000个比特组成（即）。