ICS 35.240
A01

中 华 人 民 共 和 国 民 政 行 业 标 准

MZ/T 093—2017

中国福利彩票系统彩票随机数检验规范

Specification for welfare-lottery system lottery-random-number-test

行业标准信息服务平台

2017－10－18 发布　　2017－10－18 实施

中华人民共和国民政部　　发 布

行业标准信息服务平台

前　　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国福利彩票发行管理中心提出。

本标准由民政部社会福利和慈善事业促进司归口管理。

本标准起草单位：中国福利彩票发行管理中心。

本标准主要起草人：王素英、栗演兵、张彤、朱志新、戈维周、何天琼、张积涛、韩毅、程良辉、方捷、付小兵、李英华、杜莉婷。

行业标准信息服务平台

行业标准信息服务平台

中国福利彩票系统彩票随机数检验规范

1 范围

本标准规定了中国福利彩票系统彩票随机数字序列随机性的检验方法、检验过程和检验结果的判定。

本标准适用于中国福利彩票系统彩票随机数序列检验的测试机构和测试人员。

2 规范性引用文件

下列文件中的条款通过本规范的引用而成为本规范的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本规范，但提倡使用本规范的各方探讨使用其最新版本的可能性。凡是不注日期的引用文件，其最新版本适用于本规范。

MZ/T 079-2017 中国福利彩票系统软件测试规范

GM/T 0005-2012 随机性检测规范

3 术语和定义

3.1

彩票随机数字序列 lottery random number sequence

在中国福利彩票系统中所使用到的二进制随机数字序列，组成序列的自然数由0和1构成，连续排列。

3.2

彩票随机数字序列随机性 randomness of lottery random number sequence

彩票随机数字序列的随机性表示其具有不可预见性、均一性、可测量性。

3.3

不可预见性 unpredictability

无论彩票随机数字序列具有多少位,已经产生的数字是什么,下一个产生的数字应是不可预测的。同时，利用已经生成的数字也无法推算出种子。

3.4

均一性 uniformity

在彩票随机数字序列的任何一位上，出现0或1的概率是相等的，都是1/2。

3.5

可测量性 scalability

在彩票随机数字序列上通过的检验应该在序列的子序列中得到同样的验证。

行业标准信息服务平台

3.6

块 block

彩票随机数字序列中从某一位起，连续的一段二进制数。

3.7

游程 runs

具有同样值的连续的位的序列，在游程前面的位和后面的位则是不同的值或者没有内容。

3.8

模板 template

遵循一定规则建立的具有一定长度的二进制数序列。

3.9

线性反馈移位寄存器 linear feedback shift register，LFSR

是一组固定长度的数字序列，其中每一位的数字是通过该数字的左一位或右一位数字进行右移或者左移产生，第一位或最后一位的数字则循环进入到最后一位或第一位。

3.10

显著性水平 significance level

随机性检验中错误地判断某一个随机序列为非随机序列的概率。

4 彩票随机数字序列随机性检验方法集

4.1 概述

彩票随机数字序列随机性检验方法包括比例检验、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、二进制矩阵检验、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、二元推导检验和自相关检验共十五个检验方法。

4.2 比例检验

检验彩票随机数字序列中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。

检验方法是将被测随机数字序列的0和1分别转换成-1和1后，计算结果并和显著性水平进行比较。

4.3 块中比例检验

检验彩票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。

检验方法是将被测随机数字序列分成多个非重叠子序列，统计每个子序列中1所占的比例，计算结果并和显著性水平进行比较。

4.4 游程总数检验

检验彩票随机数字序列中游程的总数是否服从随机性要求。

检验方法是统计被测随机数字序列游程的总数量，统计数字序列中1出现的次数比例，计算结果并和显著性水平进行比较。

4.5 游程分布检验

检验彩票随机数字序列中每个游程出现的次数。检验的目的是确定在被测随机数字序列中不同长度的游程的总数符合随机序列的期望值的程度。

检验方法是统计被测随机数字序列中每一个游程的长度，记录游程的数目，计算结果并和显著性水平进行比较。

4.6 块内最长游程检验

检验彩票随机数字序列中在M位区域块中“1”的最长游程。检验的目的是确定在被测随机数字序列中“1”的最长游程的长度和一个随机序列中期望的“1”的最长游程的长度期望值符合的程度。

检验方法是将被测随机数字序列分成多个子序列，统计每一个子序列中最大的“1”游程的长度，计算结果并和显著性水平进行比较。

4.7 二进制矩阵检验

检验彩票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。

检验方法是将被测随机数字序列分成子序列，将每一个子序列组成一个矩阵，统计每一个矩阵的秩，计算结果并和显著性水平进行比较。

4.8 离散傅里叶变换检验

检验彩票随机数字序列的离散傅里叶变换的峰值大小。检验的目的是确定在被测随机数字序列中周期性的特征（即相邻的重复样式），和预期的随机数序列的特征相符合的程度。

检验方法是将被测随机数字序列的0和1分别转换成-1和1，对得到的新序列进行傅里叶变换，计算结果并和显著性水平进行比较。

4.9 扑克检验

检验彩票随机数字序列中预先指定的目标模板出现的次数。检验的目的是确定在被测随机数字序列中能够多次出现指定的非周期模板的情况与期望的随机数序列的特征值符合的程度。检验中应在数字序列中搜索指定的m位模板，如果这种模板没有找到，将往下移动一位开始继续搜索；如果找到了这种模板，将从被发现模板之后的位上开始继续搜索。

检验方法是将被测随机数字序列划分成多个非重叠子序列，统计子序列模板出现的频数，计算结果并和显著性水平进行比较。

4.10 重叠模板匹配检验

检验彩票随机数字序列中预先指定的目标模板出现的次数。检验的目的是确定在被测随机数字序列中能够多次出现指定的非周期模板的情况与期望的随机数序列的特征值符合的程度。检验中应在数字序列中搜索指定的m位模板，如果这种模板没有找到，将往下移动一位开始继续搜索；如果找到了这种模板，也将往下移动一位开始继续搜索。

检验方法是将被测随机数字序列开始的一些位数据添加到序列结尾得到新序列，统计每一种子序列模板出现的频数，计算结果并和显著性水平进行比较。

4.11 通用统计检验

检验彩票随机数字序列中匹配模板之间相距的位数(这是与压缩过的序列长度相关的一种度量)。检验的目的是确定在被测随机数字序列中能否在没有信息丢失的前提下能够压缩的程度。

检验方法是将被测随机数字序列分成初始序列和检验序列，针对初始序列创建一个表，统计表中元素的值，计算结果并和显著性水平进行比较。

4.12 线性复杂度检验

检验彩票随机数字序列中LFSR的长度。检验的目的是根据被测随机数字序列的复杂度判断其随机性，好的随机序列有较长的LFSR，较短的LFSR表示非随机性。

检验方法是将被测随机数字序列划分为多个非重叠子序列，统计每一个子序列的线性复杂度，计算结果并和显著性水平进行比较。

4.13 近似熵检验

检验彩票随机数字序列中整个序列的所有可能的重叠的m位模板的概率。检验的目的是在被测随机数字序列中，把两个连续相邻的长度为（m和m+1）的重叠数据块的概率和期望的结果进行比较，以判断和期望的随机数序列特征值符合的程度。

检验方法是将被测随机数字序列开始的部分位数据添加到序列的结尾得到新序列，统计新序列中所有的2m 个m 位子序列模式的出现频数，计算结果并和显著性水平进行比较。

4.14 累积和检验

检验彩票随机数字序列中由序列中调整过的（-1，+1）数字进行累积求和得到的最大范围内的随机游程距离。检验的目的是确定在被测随机数字序列中的一部分序列进行累积求和相对于期望的随机序列中一部分序列的累积求和的结果相符合的程度。

检验方法是将被测随机数字序列的0和1分别转换为-1和1，统计和，计算结果并和显著性水平进行比较。

4.15 二元推导检验

检验彩票随机数字序列中由二元推导生成的一个新的序列,它是通过依次将初始序列中相邻两位0或1作异或操作所得的结果。二元推导检验的目的是判定第k次二元推导序列中0和1的数量是否接近一致。

检验方法是对被测随机数字序列依次将初始序列中相邻两位0或1作异或操作得到新序列，并重复操作，将新序列中的0和1分别转换成-1和1，然后对其累加求和，计算结果并和显著性水平进行比较。

4.16 自相关检验

检验彩票随机数字序列与将其逻辑左移d 位后所得新序列的关联程度。

检验方法是对被测随机数字序列进行统计，计算结果并和显著性水平进行比较。

5 彩票随机数字序列随机性检验的过程

5.1 样本准备

检验样本为在中国福利彩票系统中所使用到的二进制随机数字序列，宜采用二进制文件采集和存储。文件名以采集日期和时间组合方式命名。

5.2 计划

检验前应制定检验计划，并对计划进行评审。计划及评审的要求应符合 MZ/T 079-2017《中国福利彩票系统软件测试规范》中有关测试计划的要求。

5.3 设计

应进行检验的设计，并对设计进行评审。设计及评审的要求应符合MZ/T 079-2017《中国福利彩票系统软件测试规范》中有关测试设计的要求。

5.4 执行

使用第4章所列出的全部方法，按照检验设计对彩票随机数字序列样本进行检验。执行检验的要求应符合MZ/T 079-2017《中国福利彩票系统软件测试规范》中有关测试执行的要求。

检验结果的计算方法应符合 GM/T 0005-2012《随机性检测规范》的要求。

5.5 总结

检验完毕后应对检验进行总结，并对总结进行评审。总结及评审的要求应符合MZ/T 079-2017《中国福利彩票系统软件测试规范》中有关测试总结的要求。

6 彩票随机数字序列随机性的判定

对于本标准第4章中的每一个随机性检验方法，若一个样本的计算结果不小于显著性水平，则表示该样本通过该方法检验。

若样本数量为s ，显著性水平为α，则通过检验的样本个数应不小于 $s(1-a-3\sqrt{\frac{a(1-a)}{s}})$ 。

显著性水平取值宜在[0.001，0.01]之间。

若通过的样本个数不小于上述值，则彩票随机数字序列通过此方法检验；否则，未通过此方法检验。

行业标准信息服务平台

参 考 文 献

[1] NIST SP800-22 rev1, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

行业标准信息服务平台