随机性检验

- 序列生成
  - 随机序列：在 $[0, 2^{64}-1)$ 中利用`mt19937_64`选取大量随机数，将数字对应的 64 位整数作为输入进行哈希，将输出保存至二进制文件中；
  - 高密序列：在 $[0, 2^{64}-1)$ 中构造二进制表示中1多（多于40位）的数字，将数字对应的 64 位整数作为输入进行哈希，将输出保存至二进制文件中；
  - 低密序列：在 $[0, 2^{64}-1)$ 中构造二进制表示中1少（少于20位）的数字，将数字对应的 64 位整数作为输入进行哈希，将输出保存至二进制文件中；
- 使用 NIST `Statistical Test Suite` 基于多种度量，对随机、高密、低密序列进行随机性测试。并根据要求参数选择 $n = 1024$ 和 $n = 131072$

随机序列

- $n = 1024$ 时，测试100组，结果如下：

编号	测试类型	通过率	p 值均匀性	非默认参数
01	Frequency	99/100	0.419021	-
02	Block Frequency	100/100	0.946308	$M = 20$
03	Cumulative Sums	2/2	通过	-
04	Runs	100/100	0.474986	-
05	Longest Run of Ones	100/100	0.574903	-
06	Approximate Entropy	100/100	0.455937	$m = \lfloor \log_2 n \rfloor - 6 = 4$
07	Serial	2/2	通过	$m = \lfloor \log_2 n \rfloor - 3 = 7$

注：其他的测试均因为n太小不满足文档中的要求，得不到有意义的结论。

- $n = 131072$ 时，测试50组，结果如下：

编号	测试类型	通过率	p 值均匀性	非默认参数
01	Frequency	49/50	0.779188	-
02	Block Frequency	50/50	0.213309	$M = 1350$
03	Cumulative Sums	2/2	通过	-
04	Runs	50/50	0.699313	-
05	Longest Run of Ones	49/50	0.657933	-
06	Approximate Entropy	49/50	0.350485	$m = \lfloor \log_2 n \rfloor - 7 = 10$
07	Serial	2/2	通过	$m = \lfloor \log_2 n \rfloor - 3 = 14$
08	FFT	50/50	0.350485	-
09	Nonperiodic Template Matchings	148/148	通过	$m = 9$
10	Overlapping Template Matchings	48/50	0.739918	$m = 9$
11	Linear Complexity	49/50	0.213309	-
12	Rank	50/50	0.455937	-
13	Random Excursions	8/8	通过	-
14	Random Excursions Variant	18/18	通过	-

注：其他的测试均因为n太小不满足文档中的要求，得不到有意义的结论。

高密序列

- $n = 1024$ 时，测试100组，结果如下：

编号	测试类型	通过率	p 值均匀性	非默认参数
01	Frequency	99/100	0.816537	-
02	Block Frequency	99/100	0.719747	$M = 20$
03	Cumulative Sums	2/2	通过	-
04	Runs	99/100	0.897763	-
05	Longest Run of Ones	98/100	0.191687	-
06	Approximate Entropy	100/100	0.595549	$m = \lfloor \log_2 n \rfloor - 6 = 4$
07	Serial	2/2	通过	$m = \lfloor \log_2 n \rfloor - 3 = 7$

注：其他的测试均因为n太小不满足文档中的要求，得不到有意义的结论。

- $n = 131072$ 时，测试50组，结果如下：

编号	测试类型	通过率	p 值均匀性	非默认参数
01	Frequency	46/50	0.000818	-
02	Block Frequency	49/50	0.096578	$M = 1350$
03	Cumulative Sums	0/2	未通过	-
04	Runs	43/50	0.000000 *	-
05	Longest Run of Ones	28/50	0.000000 *	-
06	Approximate Entropy	0/50	0.000000 *	$m = \lfloor \log_2 n \rfloor - 7 = 10$
07	Serial	0/2	未通过	$m = \lfloor \log_2 n \rfloor - 3 = 14$
08	FFT	50/50	0.739918	-
09	Nonperiodic Template Matchings	127/148	未通过	$m = 9$
10	Overlapping Template Matchings	49/50	0.262249	$m = 9$
11	Linear Complexity	49/50	0.494392	-
12	Random Excursions	8/8	通过	-
13	Random Excursions Variant	18/18	通过	-
14	Rank	45/50	0.000000 *	-

注：其他的测试均因为n太小不满足文档中的要求，得不到有意义的结论。

低密序列

- $n = 1024$ 时，测试100组，结果如下：

编号	测试类型	通过率	p 值均匀性	非默认参数
01	Frequency	100/100	0.080519	-
02	Block Frequency	100/100	0.334538	$M = 20$
03	Cumulative Sums	2/2	通过	-
04	Runs	99/100	0.419021	-
05	Longest Run of Ones	99/100	0.616305	-
06	Approximate Entropy	100/100	0.202268	$m = \lfloor \log_2 n \rfloor - 6 = 4$
07	Serial	2/2	通过	$m = \lfloor \log_2 n \rfloor - 3 = 7$

注：其他的测试均因为n太小不满足文档中的要求，得不到有意义的结论。

- $n = 131072$ 时，测试50组，结果如下：

编号	测试类型	通过率	p 值均匀性	非默认参数
01	Frequency	41/50	0.000000 *	-
02	Block Frequency	50/50	0.699313	$M = 1350$
03	Cumulative Sums	0/2	未通过	-
04	Runs	47/50	0.023545	-
05	Longest Run of Ones	49/50	0.574903	-
06	Approximate Entropy	0/50	0.000000 *	$m = \lfloor \log_2 n \rfloor - 7 = 10$
07	Serial	0/2	未通过	$m = \lfloor \log_2 n \rfloor - 3 = 14$
08	FFT	50/50	0.137282	-
09	Nonperiodic Template Matchings	130/148	未通过	$m = 9$
10	Overlapping Template Matchings	48/50	0.171867	$m = 9$
11	Linear Complexity	50/50	0.008879	-
12	Rank	34/50	0.000000 *	-

注：其他的测试均因为n太小不满足文档中的要求，得不到有意义的结论。

测试结果总结：

我们可以发现，在随机数据的测试下，随机性测试保持良好；

但是在高密和低密数据的测试下，随机性测试表现较差。