

## 数字 2：一种统计算法的 Verilog 实现

### 1.1 一种统计算法的 Verilog 实现

【试题说明】：一种统计算法的实现。实现常规简单在线测试和复杂在线测试。该测试是一种统计检测算法，

基本简单在线测试原理如下：

(1) 将串行输入的单比特数据，每个128比特数据分为32组，每组4个比特；

(2) 由于4个比特共有16种取值情况，因此对于Test 有  $K=16$ ，自由度

$\nu = K - 1 = 15$ ，对于16字节的样本量，独立同分布下各种情况的理论频数为

$E_i = 2$ 。对于自由度为  $\nu = 15$ ，显著性水平  $\alpha = 3.4 \cdot 10^{-7}$  的  $\chi^2$  分布查表可

知  $\chi^2_{\nu;\alpha} = 65$

计算统计量：

$$\lambda^2 = \sum_{i=1}^k \frac{(O_i - E_i)^2}{E_i},$$

其中  $O_i$  为32个分组内16种取值出现的次数。

若计算结果大于阈值65，则统计测试不通过，引发一个随机警报；否则统计测试通过。

上面描述的统计测试可用来进行简单在线测试，另外在统计测试的基础上，可以进行复杂在线测试，复杂在线测试原理如下：

一个测试套件最多由  $N=8$  个基本测试组成（此处为8个统计测试）。记  $C_1, C_2, \dots$  为表示基本测试测试值的随机变量（ $C_j$  为上述单次的计算统计量  $\lambda^2$ ，其中  $j=1 \sim 8$ ），单次测试套件有三个评估准则：（具体阈值数值在题目设计要求参考数据部分体现）

(i) 如果任意连续三次  $C_{j-2}, C_{j-1}, C_j > \text{thre\_pre1}$ ，则生成一个预备随机警报；

(ii) 如果任意一次  $C_j \notin [\text{thre\_pre2}, \text{thre\_pre3}]$ ，则生成一个预备随机警报；

(iii) 如果任意一次  $C_j > \text{thre\_entropy}$ ，则生成一个随机警报。

如果在一个测试套件过程中没有发生预备随机警报或随机警报，则开始下一个新的测试套件。

当3个连续的基本测试因为预备随机警报（评估准则i或ii）或者一个随机警报（评估准则iii）而结束时，生成一个总随机警报。总随机警报信号是电平信号。

如果存在  $C_j > \text{thre\_pre1}$ ， $C_j \notin [\text{thre\_pre2}, \text{thre\_pre3}]$  与  $C_j > \text{thre\_entropy}$ ，这三个单次基本测试发生任意一个，则丢弃该组的128bit数据（实现时可以将dout\_vld数据有效信号置为无效）。

din:1024'h55aa000055aa000055aa000055aa000055aa000055aa0000  
55aa000055aa000055aa000055aa000055aa000055aa000055aa0000  
55aa000055aa000055aa000055aa000055aa000055aa000055aa0000  
55aa000055aa000055aa000055aa000055aa000055aa000055aa0000  
55aa000055aa000055aa000055aa000055aa000055aa000055aa0000  
a0000 (32 组 32'h55aa0000):

类别	分值权重	评分标准
----	------	------

设计 (80)	20	设计文档清晰，能准确描述设计方案，准确指导代码编写。
	40	设计符合题目要求。代码实现和文档描述一致。 代码功能正确， <b>golden</b> 数据计算正确。否则仿真、综合阶段无法得分。 对代码中影响综合面积的前三个点进行识别、分析说明原因。对代码中影响综合工作频率的前三条关键路径进行识别、分析说明原因。不能有不可综合代码。
	20	代码结构合理，思路清晰，可读性好。打拍数越少越好。 代码面积越小越好，无冗余代码，代码无编译告警。
功能仿真 (20)	10	验证报告文档清晰，满足题目要求。提供编译无告警截图，对测试点描述准确，有测试点完备性说明。
	10	功能仿真结果正确、时序正确。 告警能正确拉高。 需要使用上述三组 <b>golden</b> 数据进行测试。有三条数据波形截图（其中包括 <b>golden</b> 数据仿真波形及数据）。