report4

在这个项目中，我根据RFC6962的标准构建了一个10w个叶子的merkle tree，包括了任意数量的叶子传入、叶子节点与非叶子节点连接上不同的数来加以区分等。并给出了存在性证明和非存在性证明。具体结果如下所示：（如果下图没有显示出来的话，可以到当前目录pics文件夹查看）

首先，因为非存在性要求我们的节点以一定的数量排序，因此我们用0-99999作为我们每个叶子的初始值，按顺序建树并进行hash，最后结果如下图所示: 可以看到，对于10w叶子的一棵树，一共有18层，每一层的结构（从左到右叶子依次排列）如下所示：

```
C:\Users\86180>set PYTHONIOENCODING=utf8 & C:\Users\86180\AppData\Local\Programs\Python\Python39\python.exe -u "c:\Users\86180\Desktop\网络空
第 0 层的叶子数为： 68928
第 1 层的叶子数为： 65536
第 2 层的叶子数为： 32768
第 3 层的叶子数为： 16384
第 4 层的叶子数为： 8192
第 5 层的叶子数为： 4096
第 6 层的叶子数为： 2048
第 7 层的叶子数为： 1024
第 8 层的叶子数为： 512
第 9 层的叶子数为： 256
第 10 层的叶子数为： 128
第 11 层的叶子数为： 64
第 12 层的叶子数为： 32
第 13 层的叶子数为： 16
第 14 层的叶子数为： 8
第 15 层的叶子数为： 4
第 16 层的叶子数为： 2
第 17 层的叶子数为： 1
root hash为： ['182b2257ebfcd1455c928359ce38c79f2b289b5a4c79f6f343dacaeb5e4363ef']
```

关于存在性证明，要做的就是每次找它的兄弟节点，然后在前面连接上01进行hash，最后验证根节点的hash值是否相同，可以看到，对于随机选择的一个数，正常运行：

```
下面演示存在性证明：
待验证的根hash值为： 182b2257ebfcd1455c928359ce38c79f2b289b5a4c79f6f343dacaeb5e4363ef
准备验证的元素的hash值为： c3f8370fb3c6549f76cb7572bcc3e04537f0e32636012d15ad84ac8ebe10813a
第 1 步，需要的元素（层数，位置）为： (1, 37859) 计算结果为： b4822ecb00d3f338df3818fe4da952f8c6b4917b76279aefed82f0cd8b762b51
第 2 步，需要的元素（层数，位置）为： (2, 18928) 计算结果为： 461c89e6f380ef6a7ce37096cd4eaa2fb53d7df75ddad4727dc3b0058d9a2102
第 3 步，需要的元素（层数，位置）为： (3, 9465) 计算结果为： ed28667013d26307451a74ee7fec0cc5279dd8e28f2d7edf01b500964df619d1
第 4 步，需要的元素（层数，位置）为： (4, 4733) 计算结果为： 0240907ac98e531b310976b6bd4123e94d005d56ce532c752a21ca6641eabdf1
第 5 步，需要的元素（层数，位置）为： (5, 2367) 计算结果为： 86f357933a3c47460eff06f359a2bfd0f747acbaeaaf28053d5d1a39e66e9036
第 6 步，需要的元素（层数，位置）为： (6, 1182) 计算结果为： 7753273b1e9369f10555bbc4fa064d33cb771e1bb4ff83b231195ae6ab1f5abe
第 7 步，需要的元素（层数，位置）为： (7, 590) 计算结果为： 86a7f455a8b165e02f4f5f439c40ccf573241e1516da8f8a0301e21a4bca3e89
第 8 步，需要的元素（层数，位置）为： (8, 294) 计算结果为： ef32bd9915e6d6086816b4ef34bbe9d1b3ed19be056a2c3716cbcf14404b0b1b
第 9 步，需要的元素（层数，位置）为： (9, 146) 计算结果为： 06d9b1bbed7ae11c665873c10c54b1037dda776d6e8397465e08e85913495e3a
第 10 步，需要的元素（层数，位置）为： (10, 72) 计算结果为： d5504551296fc91cc1a779ec8a6fb800de3f546c051b9bbbdac0126bf8215778
第 11 步，需要的元素（层数，位置）为： (11, 37) 计算结果为： 4712e8a05d0153cdd6df2b9f63258d935f5f115073013483bceeed3b679dbdac
第 12 步，需要的元素（层数，位置）为： (12, 19) 计算结果为： 4ea6562a5baf8b6075f2bbaa881f9bf173e69e7547b3692f6ff79fd41c227d03
第 13 步，需要的元素（层数，位置）为： (13, 8) 计算结果为： f5bbe757afb810b09761dc9f9e80c4f598536b73d0ae466d13b2912e3376271e
第 14 步，需要的元素（层数，位置）为： (14, 5) 计算结果为： 773bff55fdf31cd9dbd289ffeab4b7be26ffe130ad57cd372c488928e2546eb2
第 15 步，需要的元素（层数，位置）为： (15, 3) 计算结果为： a9c1a1f0ad0e1bae51b2fe550839bbb6c6a1f4819985424930e139e69255c1ad
第 16 步，需要的元素（层数，位置）为： (16, 0) 计算结果为： 182b2257ebfcd1455c928359ce38c79f2b289b5a4c79f6f343dacaeb5e4363ef
元素 72322 的存在性证明验证成功！
```

关于非存在性证明，要做的就是找到和它最近的两个元素，验证他们的存在性和是否相邻，如果这两个条件都满足，那么就验证了非存在性。可以看到，对于输入的元素10.5，我们分别验证了10 和 11 的存在性，并判断这两个元素是相邻的叶子节点，因此10.5不存在于这棵树中，非存在性验证成功。

元素 42322 的存在性证明验证成功！

下面演示非存在性证明：
待验证的根hash值为： 182b2257ebfcd1455c928359ce38c79f2b289b5a4c79f6f343dacaeb5e4363ef
准备验证的元素的hash值为： a8d0b6f0939cfd883251f62b265f971ef8a5ab97eee32b91460f08b965601d93
第 1 步，需要的元素（层数，位置）为： (0, 10) 计算结果为： 0bcb543eb527335b21ce9ca05a9701d1c87e111e8bbb9f68646b641cff94cdfe
第 2 步，需要的元素（层数，位置）为： (1, 4) 计算结果为： 2c7173361ba3d79d439a93793dc88af0ed8dd72d218ab5fc030112d6271c6e97
第 3 步，需要的元素（层数，位置）为： (2, 3) 计算结果为： a31b6799fe0ee572937d8dc2420f3210b961703f4c12965042962be1513e75c4
第 4 步，需要的元素（层数，位置）为： (3, 0) 计算结果为： 2895122adc956f65b362fe86ff21618078d70efffce6b0b10e476708bed8dd84
第 5 步，需要的元素（层数，位置）为： (4, 1) 计算结果为： 3d581580e2f52bb0a17ec1cc0c0c9e7e6bcd9c3b8ce1c67028366cd9f889d80a
第 6 步，需要的元素（层数，位置）为： (5, 1) 计算结果为： bb82c5817c2506942f35eada8d811ac784c82a5aeeac17f335941e5347cf5493
第 7 步，需要的元素（层数，位置）为： (6, 1) 计算结果为： dc32816618124ba4b933d409c798482fb803bc33422e13ff190acbf0545cafc0
第 8 步，需要的元素（层数，位置）为： (7, 1) 计算结果为： 5fb2a7b30c1ab2a02c3598635d6bb46971d084eb7728f46a885c1e0424feb1f4
第 9 步，需要的元素（层数，位置）为： (8, 1) 计算结果为： d143b80e334c884418f2962e40e8a97eb6f24fc112bea12ff227d2dd5d870570
第 10 步，需要的元素（层数，位置）为： (9, 1) 计算结果为： cb09bf7d5da436ac01b63a444dbe00228acafd62c8248226b1abb23de4c90408
第 11 步，需要的元素（层数，位置）为： (10, 1) 计算结果为： aba276627573402dee3c21c73163ce5f0d060cc3d3c5b4c55da0e35b04c0d2fa
第 12 步，需要的元素（层数，位置）为： (11, 1) 计算结果为： a95234a6ffcb5c95a0718443388f36a43c51318b569e3d10d01a0c7675498b3a
第 13 步，需要的元素（层数，位置）为： (12, 1) 计算结果为： 4607633ccc0121a0dd76cb1427d6431fe7b6867e16858f69a1d527bccf91e78e
第 14 步，需要的元素（层数，位置）为： (13, 1) 计算结果为： b4f6473b3fd3e49b67286875e09e13d5e7c3b543aec95167f5728759141e73c5
第 15 步，需要的元素（层数，位置）为： (14, 1) 计算结果为： ec938b247bf86d2929958de96a31f00b2992a489422db463157816b31897e0cb
第 16 步，需要的元素（层数，位置）为： (15, 1) 计算结果为： f19a72e237fbd78fbe02e6d798685b549b067e7f33f23523a9a878de4a2f96ae
第 17 步，需要的元素（层数，位置）为： (16, 1) 计算结果为： 182b2257ebfcd1455c928359ce38c79f2b289b5a4c79f6f343dacaeb5e4363ef
元素 11 的存在性证明验证成功！
待验证的根hash值为： 182b2257ebfcd1455c928359ce38c79f2b289b5a4c79f6f343dacaeb5e4363ef
准备验证的元素的hash值为： 0b08e3dcc50fe4e5cee9b0b3a671a8db936f8335ba9050696d41cbb9a07f22e3
第 1 步，需要的元素（层数，位置）为： (0, 11) 计算结果为： 0bcb543eb527335b21ce9ca05a9701d1c87e111e8bbb9f68646b641cff94cdfe
第 2 步，需要的元素（层数，位置）为： (1, 4) 计算结果为： 2c7173361ba3d79d439a93793dc88af0ed8dd72d218ab5fc030112d6271c6e97
第 3 步，需要的元素（层数，位置）为： (2, 3) 计算结果为： a31b6799fe0ee572937d8dc2420f3210b961703f4c12965042962be1513e75c4
第 4 步，需要的元素（层数，位置）为： (3, 0) 计算结果为： 2895122adc956f65b362fe86ff21618078d70efffce6b0b10e476708bed8dd84
第 5 步，需要的元素（层数，位置）为： (4, 1) 计算结果为： 3d581580e2f52bb0a17ec1cc0c0c9e7e6bcd9c3b8ce1c67028366cd9f889d80a
第 6 步，需要的元素（层数，位置）为： (5, 1) 计算结果为： bb82c5817c2506942f35eada8d811ac784c82a5aeeac17f335941e5347cf5493
第 7 步，需要的元素（层数，位置）为： (6, 1) 计算结果为： dc32816618124ba4b933d409c798482fb803bc33422e13ff190acbf0545cafc0
第 8 步，需要的元素（层数，位置）为： (7, 1) 计算结果为： 5fb2a7b30c1ab2a02c3598635d6bb46971d084eb7728f46a885c1e0424feb1f4
第 9 步，需要的元素（层数，位置）为： (8, 1) 计算结果为： d143b80e334c884418f2962e40e8a97eb6f24fc112bea12ff227d2dd5d870570
第 10 步，需要的元素（层数，位置）为： (9, 1) 计算结果为： cb09bf7d5da436ac01b63a444dbe00228acafd62c8248226b1abb23de4c90408
第 11 步，需要的元素（层数，位置）为： (10, 1) 计算结果为： aba276627573402dee3c21c73163ce5f0d060cc3d3c5b4c55da0e35b04c0d2fa
第 12 步，需要的元素（层数，位置）为： (11, 1) 计算结果为： a95234a6ffcb5c95a0718443388f36a43c51318b569e3d10d01a0c7675498b3a
第 13 步，需要的元素（层数，位置）为： (12, 1) 计算结果为： 4607633ccc0121a0dd76cb1427d6431fe7b6867e16858f69a1d527bccf91e78e
第 14 步，需要的元素（层数，位置）为： (13, 1) 计算结果为： b4f6473b3fd3e49b67286875e09e13d5e7c3b543aec95167f5728759141e73c5
第 15 步，需要的元素（层数，位置）为： (14, 1) 计算结果为： ec938b247bf86d2929958de96a31f00b2992a489422db463157816b31897e0cb
第 16 步，需要的元素（层数，位置）为： (15, 1) 计算结果为： f19a72e237fbd78fbe02e6d798685b549b067e7f33f23523a9a878de4a2f96ae
第 17 步，需要的元素（层数，位置）为： (16, 1) 计算结果为： 182b2257ebfcd1455c928359ce38c79f2b289b5a4c79f6f343dacaeb5e4363ef
元素 10 的存在性证明验证成功！

元素 10.5 的左右两元素均存在于树中，并且相邻
元素 10.5 的非存在性证明验证成功！