

# Distinguishable Distributions

Input file: *standard input*  
Output file: *standard output*  
Time limit: 1 second  
Memory limit: 1024 mebibytes

*This is an interactive problem.*

Lazy Sam and diligent Sarah have been tasked with coming up with two interesting distributions over the set of strings of length  $n$  over the alphabet  $\{\mathbf{H}, \mathbf{T}\}$ . Lazy Sam will simply flip a coin  $n$  times (with each side showing up with a probability of  $\frac{1}{2}$ ; all coin flips are independent) and write down “H” for each head and “T” for each tail. You want to help diligent Sarah teach lazy Sam a lesson. You are given an integer  $t$ . Help Sarah come up with a distribution that is  $t$ -close to the uniform distribution, while interactively proving that you can distinguish between the distributions of lazy Sam and diligent Sarah with oracle access of length  $t$ .

Formally, for some integer  $n$ , consider the set  $S = \{\mathbf{H}, \mathbf{T}\}^n$  of size  $2^n$ , consisting of all possible strings of length  $n$  over the alphabet of two characters: “H” and “T”. A *distribution* over the set  $S$  is defined as an array of non-negative real numbers  $\{a_s\}_{s \in S}$  of length  $2^n$  indexed by the elements of  $S$ , such that their sum equals 1. One of the simplest distributions is the *uniform* distribution, where all  $a_s$  are equal to  $2^{-n}$ .

For a pair of numbers  $\varepsilon \in [0; +\infty)$  and  $k \in \{0, 1, \dots, n\}$ , we say that  $\{a_s\}_{s \in S}$  is an  $(\varepsilon, k)$ -independent distribution if, for any choice of  $k$  indices  $1 \leq i_1 < i_2 < \dots < i_k \leq n$  and any subset  $T \subseteq \{\mathbf{H}, \mathbf{T}\}^k$  of strings of length  $k$  over the alphabet  $\{\mathbf{H}, \mathbf{T}\}$ , the following holds: the sum of  $a_s$  over the  $2^{n-k}|T|$  strings  $s$  whose subsequence  $s[i_1]s[i_2] \dots s[i_k]$  belongs to  $T$  differs from  $\frac{|T|}{2^k}$  by no more than  $\varepsilon$ . In probabilistic terms, this can be expressed as:

$$\forall 1 \leq i_1 < i_2 < \dots < i_k \leq n \quad \forall T \subseteq \{\mathbf{H}, \mathbf{T}\}^k \quad \left| \frac{|T|}{2^k} - \varepsilon \leq \mathbb{P}_{s \leftarrow \{a_s\}_{s \in S}} \{s[i_1]s[i_2] \dots s[i_k] \in T\} \leq \frac{|T|}{2^k} + \varepsilon \right.$$

Intuitively, this means that to distinguish the distribution from uniform, you will either need to distinguish probabilities whose difference does not exceed  $\varepsilon$ , or look at more than  $k$  bits of the strings produced by the distribution.

The distribution  $\{a_s\}_{s \in S}$  is called  $t$ -close to the uniform distribution if it is  $(2^{-t}t, t)$ -independent.

In the definition of  $(\varepsilon, k)$ -independence, it was implied that you must first choose  $k$  indices and only then study the probability distribution over those  $k$  indices. In the oracle access model of length  $k$ , everything is different. A random string of length  $n$  is generated, and then  $k$  rounds of the following format are conducted: you call an integer  $i \in \{1, 2, \dots, n\}$ , and in response, you will be told  $s[i]$ . You can decide which index to call next, taking into account all previously asked questions and their answers.

To prove that you can distinguish the distributions of lazy Sam and diligent Sarah, you will need to, having oracle access of length  $t$  to  $m$  strings of length  $n$  sampled from their distributions (each independently and uniformly generated from either lazy Sam’s or diligent Sarah’s distribution), conclude for each of them from whose distribution it was taken, and correctly guess at least  $0.75m - 2\sqrt{m}$  times.

## Interaction Protocol

The first line contains an integer  $t$ , denoting the required closeness to a uniform distribution and the length of oracle access ( $1 \leq t \leq 5$ ).

In response, print a line with a single integer  $n$ , denoting the length of the strings for which you are ready to provide the distribution and an interactive proof of distinguishability ( $t \leq n \leq 20$ ).

In the next line, print a line with  $2^n$  integers  $b_s$ , defining your distribution ( $0 \leq b_s < 2^{64}$ ;  $\sum_{s \in S} b_s > 0$ ). Based on this data, the jury will choose the distribution  $\{a_s\}_{s \in S}$  according to the rule  $a_s = b_s / \sum_{s \in S} b_s$ . The values of  $b_s$  must be listed in lexicographical order of the strings  $s$ : for example, for  $n = 3$ , the numbers should be printed in the following order:  $b_{\mathbf{HHH}}, b_{\mathbf{HHT}}, b_{\mathbf{HTH}}, b_{\mathbf{HTT}}, b_{\mathbf{THH}}, b_{\mathbf{THT}}, b_{\mathbf{TTH}}, b_{\mathbf{TTT}}$ .

Next, read an integer  $m$ , denoting the number of interactive checks ( $1 \leq m \leq 10^4$ ). Following this, the  $m$  checks will be presented, which need to be completed one after another.

At the beginning of each check, the jury will first choose the distribution  $\{a_s\}_{s \in S}$  either from lazy Sam or diligent Sarah with a probability of  $\frac{1}{2}$ . After that, the jury samples a random string  $s \sim \{a_s\}_{s \in S}$ : any string  $s$  can be obtained with probability  $a_s$ . The jury then gives you the opportunity to ask no more than  $t$  questions about the characters of the string  $s$ . To ask a question, print a line with an integer  $q \in \{1, 2, \dots, n\}$ , denoting the index of the character of interest. After that, read the character “H” or “T” which is the answer to the query. After asking from zero to  $t$  questions, print a line with the name “Sam” if you believe that  $s$  was taken from lazy Sam’s distribution, or “Sarah” if you believe that  $s$  was taken from diligent Sarah’s distribution. After this, immediately move on to the next check until you have completed all  $m$ .

Strings can be printed in any case.

After each printed line, do not forget to flush the output buffer.

## Example

| <i>standard input</i> | <i>standard output</i> |
|-----------------------|------------------------|
| 2                     | 3<br>7 4 8 9 7 6 7 1   |
| 3                     | 1                      |
| T                     | 2                      |
| T                     | SAM                    |
| T                     | 1                      |
| T                     | 2                      |
| T                     | Sarah                  |
| T                     | 3                      |
| T                     | sARaH                  |