ACCESS CONTROL LISTS

Nick is developing a new web server. The feature he is working on now is support for access control lists. Access control list allows to restrict access to some resources on the web site based on the IP address of the requesting party.

Each IP address is a 4-byte number that is written byte-by-byte in a decimal dot-separated notation "byte0.byte1.byte2.byte3" (quotes are added for clarity). Each byte is written as a decimal number from 0 to 255 (inclusive) without extra leading zeroes. IP addresses are organized into IP networks.

IP network is described by two 4-byte numbers — network address and network mask. Both network address and network mask are written in the same notation as IP addresses.

In order to understand the meaning of network address and network mask you have to consider their binary representation. Binary representation of IP address, network address, and network mask consists of 32 bits: 8 bits for byte0 (most significant to least significant), followed by 8 bits for byte1, followed by 8 bits for byte2, and followed by 8 bits for byte3.

IP network contains a range of 2^n IP addresses where $0 \le n \le 32$. Network mask always has $32 - n$ first bits set to one, and n last bits set to zero in its binary representation. Network address has arbitrary $32 - n$ first bits, and n last bits set to zero in its binary representation. IP network contains all IP addresses whose $32 - n$ first bits are equal to $32 - n$ first bits of network address with arbitrary n last bits.

For example, IP network with network address 194.85.160.176 and network mask 255.255.255.248 contains 8 IP addresses from 194.85.160.176 to 194.85.160.183 (inclusive).

IP networks are usually denoted as "byte0.byte1.byte2.byte3/*s*" where "byte0.byte1.byte2.byte3" is the network address and *s* is the number of bits set to one in the network mask. For example, the IP network from the previous paragraph is denoted as 194.85.160.176/29.

Access control list contains an ordered list of rules. Each rule has one of the following forms:

- "deny from " — denies access to the resource to any IP from the specified IP network.
- "deny from " — denies access to the resource to the specified IP address.
- "allow from " — allows access to the resource to any IP from the specified IP network.
- "allow from " — allows access to the resource to the specified IP address.

When some party requests some resource its IP address is first checked against its access control list. The rules are scanned in order they are listed, and the first matching rule is applied. If none of the rules matches the IP address of the party, access is granted.

Given access control list and the list of requesting IP addresses, find out for each request whether it will be granted access to the resource.

Input

The first line of the input file contains $n (0 \le n \le 100000)$ — the number of rules in the access control list. The following *n* lines contain rules, one per line. IP network is always specified as "byte0.byte1.byte2.byte3/*s*".

The next line contains $m (1 \le m \le 100000)$ — the number of IP addresses to check. The following *m* lines contain IP addresses to check, one per line.

Output

For each request output 'A' if it will be granted access to the resource, or 'D' if it will not be granted access. Output all answers in one line, do not separate output by spaces.

Examples

№	stdin	stdout
1	4 allow from 10.0.0.1 deny from 10.0.0.0/8 allow from 192.168.0.0/16 deny from 192.168.0.1 5 10.0.0.1 10.0.0.2 194.85.160.133 192.168.0.1 192.168.0.2	ADAAA