Decoding Secret Sequences and Mixing Up Quantifiers

Béla Bajnok and Peter Francis

Gettysburg College

American writer, teacher, and comedian, Sam Levenson, gives us the following warning:

> Somewhere on this globe, every ten seconds, there is a woman giving birth to a child. She must be found and stopped.

The joke comes from the fact that the statements "for any given time, there is a place, at which there is a woman giving birth" and "there is a place, for which there is a woman, that is always giving birth" are not equivalent. The first is believable while the second, if true, would be ridiculously disastrous.

As this example shows, there is a discrepancy between the sometimes deceiving and confusing use of quantifiers (words or phrases used to describe the quantity of objects that have a certain property) in the English language and the rigidly fundamental role that quantification plays in mathematical writing. So the question is: how do we translate? Moreover, how do we teach new Mathematical thinkers the importance of the delicate care that quantifiers need? The answer is a game of course!

$\forall$ people, $\exists$ an understanding and $\nexists$ a want for review, skip the next section. If you're confused by that last sentence, that's OK, just keep on reading!

The Notation of Quantifiers

When discussing quantifiers at length, it is useful to have a simple notation to save time and brain power, so before we get to our game, let's review some standard logical symbols.

We will write $P(x)$ to denote a statement whose truth depends on x in a set A. For example, if $P(x)$ denotes the predicate

$$x < 57 \text{ or } x \text{ is odd},$$

for a positive integer x, then $P(4)$, $P(57)$, and $P(101)$ are all true, while $P(100)$ and $P(134)$ are false.

Here are the shorthand symbols we most often use:

- $\forall$ is the universal quantifier and can be pronounced "for all".
- $\exists$ is the existential quantifier and can be pronounced "there exists".
- $\nexists$ is the non-existential quantifier and can be pronounced "there does not exist".

The sentence

$$\forall x \in A, P(x)$$

means that *for all x in the set A, $P(x)$ is true*. The sentence

$$\exists x \in A, P(x)$$

means that *there is some (at least one) x in the set A for which $P(x)$ is true*. The sentence

$$\nexists x \in A, P(x)$$

means that there is no x in the set A for which $P(x)$ is true. Equivalently, we can write

$$\forall x \in A, \neg P(x),$$

meaning that *for all $x \in A$, $P(x)$ is false*.

The order of nested quantifiers can change the meaning of the statement drastically. Returning to Sam Levenson's joke, we are now comfortable distinguishing between the statements

$$\forall \text{ time}, \exists \text{ place}, \exists \text{ woman giving birth}$$

and

$$\exists \text{ place}, \exists \text{ woman}, \forall \text{ time giving birth}.$$

The Game

Here is the game. Imagine I have a secret sequence of four positive integers that you would like to know. You are allowed to ask questions also in the form of sequences of positive integers, to which my response will be the sum of the coordinate-wise product of the two sequences, denoted by $(\ \cdot\ )$. For example, if the secret sequence is $\mathbf{s} = (1, 2, 3, 4)$, the response to the question $\mathbf{q} = (2, 3, 10, 8)$ is

$$\mathbf{q} \cdot \mathbf{s} = 2(3) + 3(2) + 10(3) + 8(4) = 74.$$

The goal of the game is to discover my sequence in as few questions as possible. Let's play!

I have a sequence (s_1, s_2, s_3, s_4) in mind. You first ask the question

$$(1, 1, 1, 1),$$

to which my response is

$$s_1 + s_2 + s_3 + s_4 = 42.$$

Now you know that every term in the sequence is less than 42, so has at most two digits. You cleverly ask the question

$$(10^6, 10^4, 10^2, 1),$$

and I respond with

$$10^6 \cdot s_1 + 10^4 \cdot s_2 + 10^2 \cdot s_3 + 1 \cdot s_4 = 20031405.$$

Looking at the digits of my response, you can deduce that my secret sequence was $(20, 3, 14, 5)$.

It is not hard to see that this two-question method will always work! Any sequence can be discovered by asking the questions $(1, 1, 1, 1)$ and $(10^{3d}, 10^{2d}, 10^d, 1)$, where d is the number of digits in the response to the first question.

Well I suppose that it is not that exciting of a game after all. However, you might be wondering if there is a more efficient method, a winning strategy with only one question.

Clearly, if the first question $(1, 1, 1, 1)$ were to have a response of 4, then we know that the secret sequence was also $(1, 1, 1, 1)$, so we know that winning the game with one question is possible. However, to go any further, we will need to get a little more technical about what we mean by 'winning the game.'

Decoding Sequences

Let $D(\mathbf{q}, \mathbf{s})$ denote the predicate that the question $\mathbf{q}$ decodes the secret $\mathbf{s}$. In order to decode the secret with one question, you must be sure that no other secret sequence will return the same response for your question.

That is, $D(\mathbf{q}, \mathbf{s})$ is true exactly when there is no sequence $\mathbf{t} \neq \mathbf{s}$ for which

$$\mathbf{q} \cdot \mathbf{s} = \mathbf{q} \cdot \mathbf{t}.$$

In quantifier notation,

$$D(\mathbf{s}, \mathbf{t}) \iff \nexists \mathbf{t} \neq \mathbf{s}, \mathbf{q} \cdot \mathbf{t} = \mathbf{q} \cdot \mathbf{s},$$

or equivalently,

$$D(\mathbf{s}, \mathbf{t}) \iff \forall \mathbf{t} \neq \mathbf{s}, \mathbf{q} \cdot \mathbf{t} \neq \mathbf{q} \cdot \mathbf{s}.$$

So now we can ask our question more carefully. Is there a question sequence that can decode any secret sequence: is

$$\exists \mathbf{q}, \forall \mathbf{s}, D(\mathbf{q}, \mathbf{s})$$

true?

Now you might see why this game is so interesting. We can ask quite a few similar sounding questions that are really quite different, just by changing the order and type of the quantifiers.

Mixing Up Quantifiers

Here is a list of different modifications we can make to the quantifier chain above. (5 is the same as above.)

1. "There is some question that can decode some secret."
$$\exists \mathbf{q}, \exists \mathbf{s}, D(\mathbf{q}, \mathbf{s}).$$
2. "Every question decodes every secret."
$$\forall \mathbf{q}, \forall \mathbf{s}, D(\mathbf{q}, \mathbf{s}).$$
3. "It is possible to ask any question and sometimes decode the secret."
$$\forall \mathbf{q}, \exists \mathbf{s}, D(\mathbf{q}, \mathbf{s}).$$
4. "There is some secret that can be decoded by any question."
$$\exists \mathbf{s}, \forall \mathbf{q}, D(\mathbf{q}, \mathbf{s}).$$
5. "There is some fixed question that can decode any secret."
$$\exists \mathbf{q}, \forall \mathbf{s}, D(\mathbf{q}, \mathbf{s}).$$
6. "For any secret, we can pick a question to decode it."
$$\forall \mathbf{s}, \exists \mathbf{q}, D(\mathbf{q}, \mathbf{s}).$$

Before moving on, attempt to determine the truth of each of these claims. Do not get discouraged; while some of these require simple counterexamples or short proofs, others are a bit more involved to prove. I have arranged them from (what I believe to be) simplest to prove to most challenging.

Remember that a neat artifact of this notation is that in order to negate a statement quantified with only ∃s and ∀s, we can just switch the ∀s and ∃s and negate the last predicate. For example, the negation of the sentence

$$\exists a \in A, \forall b \in B, P(a, b)$$

is the sentence

$$\forall a \in A, \exists b \in B, \neg P(a, b).$$

Each of these six statements is either proven or disproven below.

1. $\exists \mathbf{q}, \exists \mathbf{s}, D(\mathbf{q}, \mathbf{s})$ is true.

   Proof. The question $\mathbf{q} = (1,1,1,1)$ decodes the secret sequence $\mathbf{s} = (1,1,1,1)$. □

2. $\forall \mathbf{q}, \forall \mathbf{s}, D(\mathbf{q}, \mathbf{s})$ is false.

   Proof. We must show that

   $$\exists \mathbf{q}, \exists \mathbf{s}, \exists \mathbf{t} \neq \mathbf{s}, \mathbf{q} \cdot \mathbf{s} = \mathbf{q} \cdot \mathbf{t}.$$

   Take $\mathbf{q} = (1,1,1,1)$, $\mathbf{s} = (2,1,1,1)$, and $\mathbf{t} = (1,2,1,1)$. Then

   $$\mathbf{q} \cdot \mathbf{s} = 2 + 1 + 1 + 1 = \mathbf{q} \cdot \mathbf{t}.$$

   □

3. $\forall \mathbf{q}, \exists \mathbf{s}, D(\mathbf{q}, \mathbf{s})$ is true.

   Proof. Given any question $\mathbf{q} = (q_1, q_2, q_3, q_4)$, let $\mathbf{s} = (1,1,1,1)$, and suppose indirectly that there is some $\mathbf{t} = (t_1, t_2, t_3, t_4) \neq \mathbf{s}$ for which

   $$\begin{aligned} q_1 + q_2 + q_3 + q_4 &= \mathbf{q} \cdot \mathbf{s} \\ &= \mathbf{q} \cdot \mathbf{t} \\ &= q_1 t_1 + q_2 t_2 + q_3 t_3 + q_4 t_4. \end{aligned}$$

   If any $t_i > 1$, then $\mathbf{q} \cdot \mathbf{t} > \mathbf{q} \cdot \mathbf{s}$, so

   $$t_1 = t_2 = t_3 = t_4 = 1,$$

   contradicting that $\mathbf{s} \neq \mathbf{t}$. □

4. $\exists \mathbf{s}, \forall \mathbf{q}, D(\mathbf{q}, \mathbf{s})$ is true.

   Proof. Let $\mathbf{s} = (1,1,1,1)$, and similarly to (3), for all $\mathbf{q} = (q_1, q_2, q_3, q_4)$, there is no $\mathbf{t} \neq \mathbf{s}$ for which

   $$\begin{aligned} q_1 + q_2 + q_3 + q_4 &= \mathbf{q} \cdot \mathbf{s} \\ &= \mathbf{q} \cdot \mathbf{t} \\ &= q_1 t_1 + q_2 t_2 + q_3 t_3 + q_4 t_4. \end{aligned}$$

   □

5. $\exists \mathbf{q}, \forall \mathbf{s}, D(\mathbf{q}, \mathbf{s})$ is false.

   Proof. We must show that

   $$\forall \mathbf{q}, \exists \mathbf{s}, \exists \mathbf{t} \neq \mathbf{s}, \mathbf{q} \cdot \mathbf{s} = \mathbf{q} \cdot \mathbf{t}.$$

   Well, given any $\mathbf{q} = (q_1, q_2, q_3, q_4)$, let

   $$\mathbf{s} = (1 + q_2, 1, 1, 1)$$

   and

   $$\mathbf{t} = (1, 1 + q_1, 1, 1).$$

   Then

   $$\begin{aligned} \mathbf{q} \cdot \mathbf{s} &= q_1(1 + q_2) + q_2 + q_3 + q_4 \\ &= q_1 + q_2(1 + q_1) + q_3 + q_4 \\ &= \mathbf{q} \cdot \mathbf{t}. \end{aligned}$$

   □

6. $\forall \mathbf{s}, \exists \mathbf{q}, D(\mathbf{q}, \mathbf{s})$ is true.

   Proof. Let $\mathbf{s} = (s_1, s_2, s_3, s_4)$. Pick pairwise relatively prime positive integers a_1, a_2, a_3, and a_4, each greater than $\max\{s_1, s_2, s_3, s_4\}$. Let

   $$\begin{aligned} q_1 &= a_2 a_3 a_4, \\ q_2 &= a_1 a_3 a_4, \\ q_3 &= a_1 a_2 a_4, \\ q_4 &= a_1 a_2 a_3, \end{aligned}$$

   and $\mathbf{q} = (q_1, q_2, q_3, q_4)$. Then assume indirectly that there is some $\mathbf{t} = (t_1, t_2, t_3, t_4) \neq \mathbf{s}$ for which

   $$\mathbf{q} \cdot \mathbf{s} = \mathbf{q} \cdot \mathbf{t},$$

   or equivalently,

   $$0 = q_1(s_1 - t_1) + q_2(s_2 - t_2) + q_3(s_3 - t_3) + q_4(s_4 - t_4).$$

   Since a_1 divides the last three terms and 0, a_1 must also divide $q_1(s_1 - t_1)$; a_1 does not divide q_1, so a_1 divides $s_1 - t_1$. Because s_1 and t_1 are positive integers,

   $$s_1 - t_1 < s_1.$$

   Since $a_1 > s_1$ in order to have that $a_1 | s_1 - t_1$, it must be that $t_1 \geq s_1$. Similarly, $t_2 \geq s_2$, $t_3 \geq s_3$, and $t_4 \geq s_4$. Then since $\mathbf{s} \neq \mathbf{t}$ we know that one of these inequalities is strict. Thus,

   $$q_1(s_1 - t_1) + q_2(s_2 - t_2) + q_3(s_3 - t_3) + q_4(s_4 - t_4) < 0,$$

   a contradiction. □

Conclusion

Perhaps you are surprised with the results in the previous section (6 was most surprising to me), but hopefully you can see the large differences that quantification make in the truth of a statement, as well as the change in caliber of proof needed to keep up with the variation. Clearly, this is a difficult topic to teach budding mathematicians.

Now, are we sure we aren't missing any combinations of quantifier chains in our lineup?