Secrets and Quantifiers

PETER E. FRANCIS AND BÉLA BAJNOK

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?

Some Notations

We will write $P(x)$ to denote a *predicate*, a statement whose truth depends on x in a set A. For example, if $P(x)$ denotes the predicate "$x < 57$ or x 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 both false.

The symbol $\forall$ represents the universal quantifier (pronounced "for all"). Thus, the sentence

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

means "for all x in the set A, $P(x)$ is true." The symbol $\exists$ is the existential quantifier (pronounced "there exists"). The sentence

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

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

The order and type of nested quantifiers can change the meaning of the statement drastically. Sam Levenson's joke plays off the differences between the following two statements:

$$\begin{cases} \forall \text{ time}, \exists \text{ place}, \exists \text{ woman giving birth, and} \\ \exists \text{ place}, \exists \text{ woman}, \forall \text{ time giving birth.} \end{cases}$$

A Secret Game

Imagine Suzy has a secret sequence of four positive integers that Quentin would like to know. He asks questions in the form of sequences of positive integers, to which Suzy's response will be the scalar product (the sum of the coordinate-wise product) of the two sequences: if Suzy's secret sequence is $\mathbf{s} = (s_1, s_2, s_3, s_4)$, the response to the question $\mathbf{q} = (q_1, q_2, q_3, q_4)$ is

$$\mathbf{q} \cdot \mathbf{s} = q_1 s_1 + q_2 s_2 + q_3 s_3 + q_4 s_4.$$

Quentin has an idea of how to "brute force" the secret sequence: Suzy has a sequence (s_1, s_2, s_3, s_4) in mind and Quentin asks the four questions $(2,1,1,1)$, $(1,2,1,1)$, $(1,1,2,1)$, and $(1,1,1,2)$. Suzy responds with w, x, y, and z, respectively. These answers determine four equations, a linear system on the variables s_1, s_2, s_3, and s_4:

$$\begin{cases} w = 2s_1 + s_2 + s_3 + s_4 \\ x = s_1 + 2s_2 + s_3 + s_4 \\ y = s_1 + s_2 + 2s_3 + s_4 \\ z = s_1 + s_2 + s_3 + 2s_4 \end{cases}$$

Maybe Quentin has studied some Linear Algebra or maybe he was lucky, because it turns out that these four questions are *linearly independent* and so will always determine a system of four equations with a unique solution:

$$\begin{cases} s_1 = \frac{4w-x-y-z}{5} \\ s_2 = \frac{4x-w-y-z}{5} \\ s_3 = \frac{4y-w-x-z}{5} \\ s_4 = \frac{4z-w-x-y}{5} \end{cases}$$

This relies on the fact that any sequence of four *real* numbers can be written as a linear combination of Quentin's four questions.

It is exciting (at least for Quentin) that with four questions, he can always discover the secret. However, you might be wondering: can Quentin do better? Are fewer questions sufficient? This possibility takes a bit more to unpack.

We can think of some secrets where single questions decode them. For example, if Quentin asks the question $(1,5,10,20)$ and Suzy answers 36, the secret must be $(1,1,1,1)$: there is only one way to use \$1, \$5, \$10, and \$20 bills to pay \$36 so that each currency is used at least once. The situation is the same if Suzy answers 37, 38, 39, or 40; however, if Suzy answers 41, her secret could be $(6,1,1,1)$ or $(1,2,1,1)$.

So, we see that we may have a 'happy accident' in asking our question. To go further, we will need to be more technical with what we mean by 'decoding the secret with one question.'

Decoding Sequences

Let $D(\mathbf{q}, \mathbf{s})$ denote the predicate "the question $\mathbf{q}$ decodes the secret $\mathbf{s}$". In order to decode the secret with one question, you must ensure that no other secret sequence returns the same response for the question. That is, $D(\mathbf{q}, \mathbf{s})$ is true exactly when there is no sequence $\mathbf{t}$ different from $\mathbf{s}$ for which

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

Equivalently in quantifier notation,

$$\underbrace{\forall \mathbf{t},}_{\text{for all } \mathbf{t}} \quad \underbrace{\mathbf{t} \neq \mathbf{s},}_{\text{different from } \mathbf{s}} \quad \mathbf{q} \cdot \mathbf{t} \neq \mathbf{q} \cdot \mathbf{s}.$$

But is a single question *always* enough? The answer depends largely on the interpretation of this question. There are two ways to make our question precise:

1. Is "$\exists \mathbf{q}, \forall \mathbf{s}, D(\mathbf{q}, \mathbf{s})$" true?
2. Is "$\forall \mathbf{s}, \exists \mathbf{q}, D(\mathbf{q}, \mathbf{s})$" true?

We will decipher the meaning of these two questions and determine their truth. Our examination will expose that the order of the quantifiers results in two rather different outcomes.

The Master Key

The first quantifier chain "$\exists \mathbf{q}, \forall \mathbf{s}, D(\mathbf{q}, \mathbf{s})$" means "there is some fixed question that can decode any secret." We can understand this situation by thinking of questions as keys and secrets as locks; the predicate $D(\mathbf{q}, \mathbf{s})$ can be interpreted as "key $\mathbf{q}$ opens lock $\mathbf{s}$."

Continuing the metaphor, the statement above means "there is some key that can open any lock." In the context of the game, if this were true, Quentin would always win by asking the same one question; the game would be quite boring. Is this true? Let $\mathbf{q} = (q_1, q_2, q_3, q_4)$ be an arbitrary question. Define $\mathbf{s} = (1, 1, 1 + q_4, 1)$ and $\mathbf{t} = (1, 1, 1, 1 + q_3)$. Then

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

Thus, given a question, we can build at least two sequences between which the question cannot distinguish. In other words, if we thought we had a 'master key' (one that could open any lock), we would be wrong because we showed how to build at least two locks that the key cannot open.

The Unbreakable Secret

The second quantifier chain "$\forall \mathbf{s}, \exists \mathbf{q}, D(\mathbf{q}, \mathbf{s})$" can be read "for any secret, we can pick a question to decode it": there is no secret safe from being decoded in one question. At first glance, this sentence sounds quite similar to the previous, 'master key,' sentence. Here is evidence that a small change in quantifiers can make a big difference in meaning. While (1) is false, (2) happens to be true. Let's see why.

Suppose that $\mathbf{s} = (s_1, s_2, s_3, s_4)$ is an arbitrary sequence. Pick four pairwise relatively prime positive integers a_1, a_2, a_3, and a_4 (that is, four integers with no common prime factors) greater than s_1, s_2, s_3, and s_4, respectively. Then 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 $\mathbf{q} = (q_1, q_2, q_3, q_4)$. We claim $\mathbf{q}$ decodes $\mathbf{s}$. To show this, assume there is some sequence $\mathbf{t} = (t_1, t_2, t_3, t_4)$ with $\mathbf{q} \cdot \mathbf{s} = \mathbf{q} \cdot \mathbf{t}$. Then we have

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

Since a_1 divides the last three summands and 0, a_1 must also divide $q_1(s_1 - t_1)$. As a_1 is relatively prime to q_1 (by design), a_1 must divide $s_1 - t_1$. Because s_1 and t_1 are positive integers, we conclude $s_1 - t_1 < s_1$. We chose $a_1 > s_1$, so a_1 dividing $s_1 - t_1$ implies $t_1 \geq s_1$. Similarly, $t_2 \geq s_2$, $t_3 \geq s_3$, and $t_4 \geq s_4$. As the above equation shows four nonpositive integers sum to 0, we conclude that each summand must be 0, so $s_i = t_i$ for each i. Thus, $\mathbf{s} = \mathbf{t}$. There is no 'unbreakable secret'!

The Solution

These two examples classify major differences that quantification makes in the truth of a statement, as well as the change in caliber of proof needed to keep up with seemingly small variations to sentence structure.

At the very least, now if anyone tells you that they have a shirt for every day of the week, you can rightfully ask them how they manage to wash it!

As we have seen, Quentin can always find the secret with four questions, but not necessarily with one. However, it turns out that two questions are always sufficient. Can you prove it?

Peter E. Francis *is an undergraduate Mathematics student at Gettysburg College.*

Béla Bajnok *is a Professor of Mathematics at Gettysburg College and is the Director of the American Mathematics Competitions of the MAA.*