The Logic of Large Enough

Eerke Boiten and Dan Grundy

Computing Laboratory, University of Kent
e.a.boiten@kent.ac.uk, daniel.c.grundy@gmail.com

Abstract. In this paper we explore the "for large enough" quantifier, also known as "all but finitely many", which plays a central role in asymptotic reasoning, as used for example in complexity theory and cryptography. We investigate calculational properties of this quantifier, and show their application in reasoning about limits of functions.

Keywords. Calculational methods; asymptotics; generalised quantifiers.

Introduction

In what follows we explore a variant of universal quantification, namely that a particular predicate holds for "large enough" natural numbers. This quantifier occurs naturally in many areas of mathematics that employ asymptotic reasoning, in particular in complexity theory and its applications. Unfortunately, it often occurs in an encoded form (requiring two quantifiers, and worse: two dummy variables), or is left implicit in the context, thereby obscuring which manipulations are permissible. Most striking perhaps, is its negated occurrence, "for infinitely many ...", which is often seen in proofs by contradiction.

In the next section we define the "new" quantifier (in terms of existential and universal quantification) and explore its calculational properties. We then show how the quantifier can be applied in the theory of limits of sequences, where, in particular, it allows us to avoid reference to sequence indices in the resulting theorems and proofs. Finally, we indicate how this work leads to a calculational theory of asymptotics, with applications to complexity theory and beyond.

Large enough quantifiers

The property that P holds for large enough values of x can be described using an existential-universal quantifier combination:

$$\langle \exists\, X :: \langle \forall\, x : x > X : P \rangle \rangle$$

Throughout this paper we assume that x and X are natural numbers. In that case, the above is sometimes known as the "almost-all" quantifier, as it requires P to hold for all but finitely many numbers. This quantifier has been studied in

logic since at least the 1970s [0,1], and belongs to the class of "generalised", or "modal quantifiers", defined by Mostowski [2] in 1957, and studied in the 1990s by Alechina, Van Lambalgen, and Van Benthem [3, 4]. However, their work concentrated on properties of the class in general, in particular expressiveness and decidability, rather than on practical calculation.

Taking the natural numbers as a timeline, a property holding for large enough numbers means it will hold continuously from a certain point onwards; in other words, eventually it will always hold. The notation used in the following definition has been designed to emphasise the modal view of this quantifier, and that it binds a particular variable:

$$\langle \diamondsuit x :: P \rangle \quad \equiv \quad \langle \exists\, X :: \langle \forall\, x : x > X : P \rangle \rangle \tag{1}$$

where X does not occur free in P. Properties of this quantifier follow. The first collection of properties concerns situations where the quantifier can be eliminated.

First, we show that:

$$\langle \diamondsuit x :: \mathbf{true} \rangle \quad \equiv \quad \mathbf{true} \tag{2}$$

Proof:

$\langle \diamondsuit x :: \mathbf{true} \rangle$

$\equiv$ { definition of $\diamondsuit$; i.e., (1) }

$\langle \exists\, X :: \langle \forall\, x : x > X : \mathbf{true} \rangle \rangle$

$\equiv$ { property of $\forall$ }

$\langle \exists\, X :: \mathbf{true} \rangle$

$\equiv$ { the range of quantification (natural numbers) is non-empty }

true

Similarly, we have:

$$\langle \diamondsuit x :: \mathbf{false} \rangle \quad \equiv \quad \mathbf{false} \tag{3}$$

Proof:

$\langle \diamondsuit x :: \mathbf{false} \rangle$

$\equiv$ { definition of $\diamondsuit$ }

$\langle \exists\, X :: \langle \forall\, x : x > X : \mathbf{false} \rangle \rangle$

$\equiv$ { the range of $\forall$ quantification is non-empty:
there is no largest natural number }

$\langle \exists\, X :: \mathbf{false} \rangle$

$\equiv$ { property of $\exists$ }

false

We can generalise (2) and (3) as follows: if x does not occur free in P we have

$$\langle \diamondsuit x :: P \rangle \;\equiv\; P \tag{4}$$

The proof uses the two properties of natural numbers used for proofs of (2) and (3) :

$\langle \diamondsuit x :: P \rangle$

$\equiv$ { definition of $\diamondsuit$ }

$\langle \exists\, X :: \langle \forall\, x : x > X : P \rangle \rangle$

$\equiv$ { eliminate redundant quantifiers; non-empty ranges }

P

Provided x does not occur free in a real-valued expression E we have:

$$\langle \diamondsuit x :: x > E \rangle \;\equiv\; \mathbf{true} \tag{5}$$

Proof:

$\langle \diamondsuit x :: x > E \rangle$

$\equiv$ { definition of $\diamondsuit$ }

$\langle \exists\, X :: \langle \forall\, x : x > X : x > E \rangle \rangle$

$\Leftarrow$ { one-point rule, $\lceil E \rceil$ is the least integer $\geq E$ }

$\langle \forall\, x : x > \lceil E \rceil : x > E \rangle$

$\equiv$ { predicate calculus }

true

Next, we investigate properties of the quantifier in combination with standard operators and quantifiers. The following useful monotonicity property follows immediately from monotonicity of the standard quantifiers (with respect to the $\Rightarrow$ ordering):

$$\langle \forall\, x :: P \Rightarrow Q \rangle \quad \Rightarrow \quad (\langle \diamondsuit x :: P \rangle \;\Rightarrow\; \langle \diamondsuit x :: Q \rangle) \tag{6}$$

We can use (6) to prove various weakening and strengthening rules; for example:

$$\langle \diamondsuit x :: P \rangle \quad \Rightarrow \quad \langle \diamondsuit x :: P \;\vee\; Q \rangle \tag{7}$$

Similarly, we have:

$$\langle \diamondsuit x :: P \;\wedge\; Q \rangle \quad \Rightarrow \quad \langle \diamondsuit x :: P \rangle \tag{8}$$

Clearly other variations are possible.

We can use (7) to prove the following "almost" distributivity property:

$$\langle \diamondsuit x :: P \rangle \;\vee\; \langle \diamondsuit x :: Q \rangle \quad \Rightarrow \quad \langle \diamondsuit x :: P \;\vee\; Q \rangle \tag{9}$$

Proof:

$$
\begin{array}{ll}
 & \langle \Diamond x :: P \rangle \ \vee \ \langle \Diamond x :: Q \rangle \\
\Rightarrow & \quad \{ \ (7) \ , \ \text{twice} \ \} \\
 & \langle \Diamond x :: P \ \vee \ Q \rangle \ \vee \ \langle \Diamond x :: P \ \vee \ Q \rangle \\
\equiv & \quad \{ \ \text{idempotence of} \ \vee \ \} \\
 & \langle \Diamond x :: P \ \vee \ Q \rangle
\end{array}
$$

The opposite direction does not hold: replace P with $even.x$ and Q with $odd.x$, for example.

Intuitively we have

$$\langle \forall \, x :: P \rangle \quad \Rightarrow \quad \langle \Diamond x :: P \rangle \qquad , \tag{10}$$

but we can prove it without unfolding $\Diamond$ by virtue of (6) :

$$
\begin{array}{ll}
 & \langle \forall \, x :: P \rangle \\
\equiv & \quad \{ \ \text{left identify of} \ \Rightarrow , \ \text{heading for an appeal to} \ (6) \ \} \\
 & \langle \forall \, x :: \mathbf{true} \ \Rightarrow \ P \rangle \\
\Rightarrow & \quad \{ \ (6) \ \text{ with } \ P, Q := \ \mathbf{true}, P \ \} \\
 & \langle \Diamond x :: \mathbf{true} \rangle \ \Rightarrow \ \langle \Diamond x :: P \rangle \\
\equiv & \quad \{ \ (2) \ \} \\
 & \mathbf{true} \ \Rightarrow \ \langle \Diamond x :: P \rangle \\
\equiv & \quad \{ \ \text{left identity of} \ \Rightarrow \ \} \\
 & \langle \Diamond x :: P \rangle
\end{array}
$$

Next, we have the useful property that conjunction distributes over $\Diamond$:

$$\langle \Diamond x :: P \rangle \ \wedge \ \langle \Diamond x :: Q \rangle \quad \equiv \quad \langle \Diamond x :: P \ \wedge \ Q \rangle \tag{11}$$

The following proof is by mutual implication; first we prove that

$$\langle \Diamond x :: P \rangle \ \wedge \ \langle \Diamond x :: Q \rangle \quad \Rightarrow \quad \langle \Diamond x :: P \ \wedge \ Q \rangle \qquad .$$

If we assume the antecedent, then there exist witnesses X_0 and X_1 such that:

$$
\begin{array}{ll}
 & \langle \forall \, x : x > X_0 : P \rangle \ \wedge \ \langle \forall \, x : x > X_1 : Q \rangle \\
\Rightarrow & \quad \{ \ \text{arithmetic} \ \} \\
 & \langle \forall \, x : x > X_0 \uparrow X_1 :: P \rangle \ \wedge \ \langle \forall \, x : x > X_0 \uparrow X_1 : Q \rangle \\
\equiv & \quad \{ \ \text{distributivity} \ \}
\end{array}
$$

$$
\begin{array}{ll}
 & \langle \forall\, x : x > X_0 \uparrow X_1 :: P \ \wedge \ Q \rangle \\
\Rightarrow & \quad \{ \ \exists \ \text{introduction, with} \ \ X := X_0 \uparrow X_1 \ \} \\
 & \langle \exists\, X :: \langle \forall\, x : x > X : P \ \wedge \ Q \rangle \rangle \\
\equiv & \quad \{ \ \text{definition of} \ \ \langle\!\langle \Box \rangle\!\rangle \ \} \\
 & \langle \langle\!\langle \Box \rangle\!\rangle\, x :: P \ \wedge \ Q \rangle
\end{array}
$$

The opposite direction, viz

$$
\langle \langle\!\langle \Box \rangle\!\rangle\, x :: P \rangle \ \wedge \ \langle \langle\!\langle \Box \rangle\!\rangle\, x :: Q \rangle \quad \Leftarrow \quad \langle \langle\!\langle \Box \rangle\!\rangle\, x :: P \ \wedge \ Q \rangle \qquad ,
$$

is easily proved by appealing to the idempotence of conjunction, and then weakening via (8) .

Remark. Properties (2) , (6) , and (11) , along with "dummy renaming", correspond to the "minimal logic" of generalised quantifiers described in [3]. **End of Remark.**

It should be clear that we can generalise (11) to an arbitrary, but finite number of conjuncts; that is, for any fixed, finite set F , we have:

$$
\langle \forall\, i : i \in F : \langle \langle\!\langle \Box \rangle\!\rangle\, x :: P_i \rangle \rangle \quad \equiv \quad \langle \langle\!\langle \Box \rangle\!\rangle\, x :: \langle \forall\, i : i \in F : P_i \rangle \rangle \tag{12}
$$

and as a consequence, for fixed, finite set F , we have:

$$
\langle \forall\, y : y \in F : \langle \langle\!\langle \Box \rangle\!\rangle\, x :: P \rangle \rangle \quad \equiv \quad \langle \langle\!\langle \Box \rangle\!\rangle\, x :: \langle \forall\, y : y \in F : P \rangle \rangle \tag{13}
$$

It is clear from the first part of the proof of (11) , that in the general case, finiteness is required to take the maximum over the X bounds of each conjunct. Since finiteness is only necessary in one direction, if we drop this requirement we retain the following, weaker form of (13) :

$$
\langle \forall\, y :: \langle \langle\!\langle \Box \rangle\!\rangle\, x :: P \rangle \rangle \quad \Leftarrow \quad \langle \langle\!\langle \Box \rangle\!\rangle\, x :: \langle \forall\, y :: P \rangle \rangle \tag{14}
$$

Proof:

$$
\begin{array}{ll}
 & \langle \langle\!\langle \Box \rangle\!\rangle\, x :: \langle \forall\, y :: P \rangle \rangle \\
\equiv & \quad \{ \ \text{definition of} \ \ \langle\!\langle \Box \rangle\!\rangle \ \} \\
 & \langle \exists\, X :: \langle \forall\, x : x > X : \langle \forall\, y :: P \rangle \rangle \rangle \\
\equiv & \quad \{ \ \text{nesting} \ \} \\
 & \langle \exists\, X :: \langle \forall\, y :: \langle \forall\, x : x > X : P \rangle \rangle \rangle \\
\Rightarrow & \quad \{ \ \exists \forall \Rightarrow \forall \exists \ \} \\
 & \langle \forall\, y :: \langle \exists\, X :: \langle \forall\, x : x > X : P \rangle \rangle \rangle \\
\equiv & \quad \{ \ \text{definition of} \ \ \langle\!\langle \Box \rangle\!\rangle \ \} \\
 & \langle \forall\, y :: \langle \langle\!\langle \Box \rangle\!\rangle\, x :: P \rangle \rangle
\end{array}
$$

As a counterexample for the reverse implication, consider $x \geq y$ for P .

There are several ways of generalising the definition of $\langle \diamond \rangle$ to vectors; we choose the following as it is insensitive to the ordering of dummy variables:

$$\langle \diamond \rangle x, y :: P\rangle \quad \equiv \quad \langle \exists\, X, Y :: \langle \forall\, x, y : x > X \ \wedge\ y > Y : P\rangle\rangle \tag{15}$$

Equivalently, we have what we refer to as the "diagonal" property:

$$\langle \diamond \rangle x, y :: P\rangle \quad \equiv \quad \langle \exists\, Z :: \langle \forall\, x, y : x > Z \ \wedge\ y > Z : P\rangle\rangle \tag{16}$$

We prove (16) by mutual implication. Assume X , Y , and Z are not free in P , then:

$$\begin{array}{ll}
& \langle \diamond \rangle x, y :: P\rangle \\
\equiv & \quad \{\ (15)\ \} \\
& \langle \exists\, X, Y :: \langle \forall\, x, y :: x > X \ \wedge\ y > Y : P\rangle\rangle \\
\Rightarrow & \quad \{\ \exists \text{ introduction, with } Z := X \uparrow Y\ \} \\
& \langle \exists\, X, Y :: \langle \exists\, Z :: \langle \forall\, x, y : x > Z \ \wedge\ y > Z : P\rangle\rangle\rangle \\
\equiv & \quad \{\ \text{eliminate redundant outer quantifiers}\ \} \\
& \langle \exists\, Z :: \langle \forall\, x, y : x > Z \ \wedge\ y > Z : P\rangle\rangle \\
\Rightarrow & \quad \{\ \exists \text{ introduction, with } X, Y := Z, Z\ \} \\
& \langle \exists\, Z :: \langle \exists\, X, Y :: \langle \forall\, x, y : x > X \ \wedge\ y > Y : P\rangle\rangle\rangle \\
\equiv & \quad \{\ \text{eliminate redundant outer quantifier}\ \} \\
& \langle \exists\, X, Y :: \langle \forall\, x, y : x > X \ \wedge\ y > Y : P\rangle\rangle \\
\equiv & \quad \{\ (15)\ \} \\
& \langle \diamond \rangle x, y :: P\rangle
\end{array}$$

We refer to the following distributivity property as "unvectoring". If x does not occur free in Q , and y does not occur free in P , then:

$$\langle \diamond \rangle x, y :: P \ \wedge\ Q\rangle \quad \equiv \quad \langle \diamond \rangle x :: P\rangle \ \wedge\ \langle \diamond \rangle y :: Q\rangle \tag{17}$$

Proof:

$$\begin{array}{ll}
& \langle \diamond \rangle x, y :: P \ \wedge\ Q\rangle \\
\equiv & \quad \{\ \wedge \text{ over } \diamond \text{ ; i.e., (11)}\ \} \\
& \langle \diamond \rangle x, y :: P\rangle \ \wedge\ \langle \diamond \rangle x, y :: Q\rangle \\
\equiv & \quad \{\ \text{eliminate redundant quantifiers}\ \} \\
& \langle \diamond \rangle x :: P\rangle \ \wedge\ \langle \diamond \rangle y :: Q\rangle
\end{array}$$

The generalised definition of $\langle\diamond\!\!\!\!\!\!\Box\rangle$ in (15) allows us to nest quantifications as follows:

$$\langle\diamond\!\!\!\!\!\!\Box\, x, y :: P\rangle \quad \Rightarrow \quad \langle\diamond\!\!\!\!\!\!\Box\, x :: \langle\diamond\!\!\!\!\!\!\Box\, y :: P\rangle\rangle \tag{18}$$

Proof:

$$\begin{array}{ll} & \langle\diamond\!\!\!\!\!\!\Box\, x, y :: P\rangle \\ \equiv & \quad \{\ (15)\ \} \\ & \langle\exists\, X, Y :: \langle\forall\, x, y : x > X \ \wedge\ y > Y : P\rangle\rangle \\ \equiv & \quad \{\ \text{nesting, twice}\ \} \\ & \langle\exists\, X :: \langle\exists\, Y :: \langle\forall\, x : x > X : \langle\forall\, y : y > Y : P\rangle\rangle\rangle\rangle \\ \Rightarrow & \quad \{\ \exists\forall \Rightarrow \forall\exists\ \} \\ & \langle\exists\, X :: \langle\forall\, x : x > X : \langle\exists\, Y : \langle\forall\, y : y > Y : P\rangle\rangle\rangle\rangle \\ \equiv & \quad \{\ (1)\ ,\ \text{twice}\ \} \\ & \langle\diamond\!\!\!\!\!\!\Box\, x :: \langle\diamond\!\!\!\!\!\!\Box\, y :: P\rangle\rangle \end{array}$$

The reverse implication does not hold as $\exists$ and $\forall$ do not generally commute; for example, consider $y > x$ for P .

Next, we investigate circumstances where we can replace x by $f.x$ inside $\langle\diamond\!\!\!\!\!\!\Box\rangle$-expressions, for an "eventually increasing" function f . Specifically, let f be a function from natural numbers to reals that satisfies the following property:

$$\langle\forall\, y :: \langle\diamond\!\!\!\!\!\!\Box\, x :: f.x > y\rangle\rangle \tag{19}$$

Informally, this states that $f.x$ will eventually remain above any bound. Most of the functions considered in computational complexity theory have this property, including, for example, positive polynomials, and their quotients where the numerator has a higher degree than the denominator (but excluding the constant 0); the identity function also satisfies it. For functions that satisfy (19) , by skolemising the existential quantification inside $\langle\diamond\!\!\!\!\!\!\Box\rangle$ we can introduce a function *bound* that satisfies the property:

$$\langle\forall\, x : x > \mathit{bound}.y : f.x > y\rangle$$

For functions that satisfy (19) , for Boolean function P we have:

$$\langle\diamond\!\!\!\!\!\!\Box\, x :: P.x\rangle \quad \Rightarrow \quad \langle\diamond\!\!\!\!\!\!\Box\, x :: P.(f.x)\rangle \tag{20}$$

If we assume the antecedent, then according to the definition of $\langle\diamond\!\!\!\!\!\!\Box\rangle$ we have $\langle\forall\, x : x > X : P.x\rangle$ for some X . Since f satisfies (19) we have:

$\langle \forall\, x : x > \mathit{bound}.X : f.x > X \rangle$

$\Rightarrow$ { $\exists$ introduction, with $Y := \mathit{bound}.X$ }

$\langle \exists\, Y :: \langle \forall\, x : x > Y : f.x > X \rangle \rangle$

$\Rightarrow$ { antecedent: $x > X \;\Rightarrow\; P.x$ }

$\langle \exists\, Y :: \langle \forall\, x : x > Y : P.(f.x) \rangle \rangle$

$\equiv$ { definition of $\langle\Diamond\rangle$ }

$\langle \langle\Diamond\rangle x :: P.(f.x) \rangle$

For functions that satisfy (19), "for large enough x" is equivalent to "for large enough $f.x$":

$$\langle \langle\Diamond\rangle x :: P \rangle \quad \equiv \quad \langle \exists\, Y :: \langle \forall\, x :: f.x > Y : P \rangle \rangle \tag{21}$$

We prove this by mutual implication. From left to right, (19) is not necessary. We observe that f has a maximal value on every prefix of $\mathbb{N}$; we denote this maximum $\nabla.X$, where

$$\nabla.X \quad = \quad \langle \uparrow x : x \leq X : f.x \rangle$$

It follows that if $f.x > \nabla.X$ then $x > X$. Now we calculate as follows:

$\langle \langle\Diamond\rangle x :: P \rangle$

$\equiv$ { definition of $\langle\Diamond\rangle$ }

$\langle \exists\, X :: \langle \forall\, x : x > X : P \rangle \rangle$

$\Rightarrow$ { range strengthening: $f.x > \nabla.X \;\Rightarrow\; x > X$ }

$\langle \exists\, X :: \langle \forall\, x : f.x > \nabla.X : P \rangle \rangle$

$\Rightarrow$ { $\exists$ introduction, with $Y := \nabla.X$; eliminate redundant quantifier }

$\langle \exists\, Y :: \langle \forall\, x : f.x > Y : P \rangle \rangle$

To prove the opposite direction we observe that as a consequence of (19), for every bound Y, the set $\langle x : f.x \leq Y : x \rangle$ is finite, and has a maximum, which we denote $\nabla.Y$; that is:

$$\nabla.Y \quad = \quad \langle \uparrow x : f.x \leq Y : x \rangle$$

If follows that if $x > \nabla.Y$ then $f.x > Y$. Now we calculate as follows:

$\langle \exists\, Y :: \langle \forall\, x : f.x > Y : P \rangle \rangle$

$\Rightarrow$ { range strengthening: $x > \nabla.Y \;\Rightarrow\; f.x > Y$ }

$\langle \exists\, Y :: \langle \forall\, x : x > \nabla.Y : P \rangle \rangle$

$\Rightarrow$ { $\exists$ introduction, with $X := \nabla.Y$; eliminate redundant quantifier }

$\langle \exists\, X :: \langle \forall\, x : x > X : P \rangle \rangle$

$\equiv$ { definition of $\langle\!\langle \Box \rangle\!\rangle$ }

$\langle \langle\!\langle \Box \rangle\!\rangle\, x :: P \rangle$

The corresponding "existential" operator, denoted by $[\![\Diamond]\!]$, is defined as the dual of $\langle\!\langle \Box \rangle\!\rangle$:

$$\langle [\![\Diamond]\!]\, x :: P \rangle \quad \equiv \quad \neg \langle \langle\!\langle \Box \rangle\!\rangle\, x :: \neg P \rangle \tag{22}$$

Consequently,

$$\langle [\![\Diamond]\!]\, x :: P \rangle \quad \equiv \quad \langle \forall\, X :: \langle \exists\, x : x > X : P \rangle \rangle \qquad , \tag{23}$$

which can be paraphrased as "(by increasing x) always P eventually holds"; equivalently: "there are infinitely many values of x for which P holds", i.e.:

$$\langle [\![\Diamond]\!]\, x :: P \rangle \quad \equiv \quad \langle x : P : x \rangle \text{ is infinite} \tag{24}$$

The above definition of $[\![\Diamond]\!]$ rather naturally implies that the set $\langle x : P : x \rangle$ is infinite; in the other direction we have:

$\langle x : P : x \rangle$ is infinite

$\Rightarrow$ { prefixes of $\mathbb{N}$ are finite }

$\langle \forall\, X :: \langle x : P : x \rangle \not\subseteq \langle x : x \leq X : x \rangle \rangle$

$\equiv$ { definition of $\not\subseteq$ }

$\langle \forall\, X :: \langle \exists\, x :: P \ \wedge\ \neg(x \leq X) \rangle \rangle$

$\equiv$ { trading }

$\langle \forall\, X :: \langle \exists\, x : x > X : P \rangle \rangle$

$\equiv$ { (23) }

$\langle [\![\Diamond]\!]\, x :: P \rangle$

As a corollary, we have the property mentioned above, namely that $\langle\!\langle \Box \rangle\!\rangle$ denotes "all but finitely many":

$$\langle \langle\!\langle \Box \rangle\!\rangle\, x :: P \rangle \quad \equiv \quad \langle x : \neg P : x \rangle \text{ is finite} \tag{25}$$

Limits of sequences

As a simple application of the $\langle\!\langle \Box \rangle\!\rangle$ quantifier, we reason about limits of sequences, which we define as follows:

$$\lim_{x \to \infty} f.x = a \quad \equiv \quad \langle \forall\, \epsilon : \epsilon > 0 : \langle \langle\!\langle \Box \rangle\!\rangle\, x :: |f.x - a| < \epsilon \rangle \rangle \tag{26}$$

where f is a function from naturals to reals, and ϵ and a are reals.

As a first example, we show that multiplication by a positive constant commutes with taking a limit. For $c > 0$, we have:

$$
\begin{array}{ll}
& \lim_{x\to\infty} f.x \;=\; a \\
\equiv & \quad \{\ (26)\ \} \\
& \langle \forall\, \epsilon : \epsilon > 0 : \langle \diamondsuit\, x :: |f.x - a| < \epsilon \rangle \rangle \\
\equiv & \quad \{\ \text{arithmetic}\ \} \\
& \langle \forall\, \epsilon : \epsilon > 0 : \langle \diamondsuit\, x :: |c \cdot f.x \;-\; c \cdot a| < c \cdot \epsilon \rangle \rangle \\
\equiv & \quad \{\ \text{dummy translation:}\ \ \epsilon' := \ c \cdot \epsilon\ \} \\
& \langle \forall\, \epsilon' : \epsilon' > 0 : \langle \diamondsuit\, x :: |c \cdot f.x \;-\; c \cdot a| < \epsilon' \rangle \rangle \\
\equiv & \quad \{\ (26)\ \} \\
& \lim_{x\to\infty} c \cdot f.x \;=\; c \cdot a
\end{array}
$$

In the following proof that limits distribute over addition, we avoid reference to particular values of the function's arguments by appealing to the distributivity of $\diamondsuit$ over conjunction:

$$
\begin{array}{ll}
& \lim_{x\to\infty} f.x = a \;\wedge\; \lim_{x\to\infty} g.x = b \\
\equiv & \quad \{\ (26)\ ,\ \text{twice}\ \} \\
& \langle \forall\, \epsilon : \epsilon > 0 : \langle \diamondsuit\, x :: |f.x - a| < \epsilon \rangle \rangle \;\wedge\; \langle \forall\, \epsilon : \epsilon > 0 : \langle \diamondsuit\, x :: |g.x - b| < \epsilon \rangle \rangle \\
\equiv & \quad \{\ \text{distributivity}\ \} \\
& \langle \forall\, \epsilon : \epsilon > 0 : \langle \diamondsuit\, x :: |f.x - a| < \epsilon \rangle \;\wedge\; \langle \diamondsuit\, x :: |g.x - b| < \epsilon \rangle \rangle \\
\equiv & \quad \{\ \diamondsuit\ \text{over}\ \wedge\ \} \\
& \langle \forall\, \epsilon : \epsilon > 0 : \langle \diamondsuit\, x :: |f.x - a| < \epsilon \;\wedge\; |g.x - b| < \epsilon \rangle \rangle \\
\Rightarrow & \quad \{\ \text{arithmetic}\ \} \\
& \langle \forall\, \epsilon : \epsilon > 0 : \langle \diamondsuit\, x :: |(f.x + g.x) - (a + b)| \;<\; 2 \cdot \epsilon \rangle \rangle \\
\equiv & \quad \{\ \text{dummy translation:}\ \ \epsilon' := \ \epsilon/2\ \} \\
& \langle \forall\, \epsilon' : \epsilon' > 0 : \langle \diamondsuit\, x :: |f.x - a| < \epsilon' \;\wedge\; |g.x - b| < \epsilon' \rangle \rangle \\
\equiv & \quad \{\ (26)\ \} \\
& \lim_{x\to\infty} (f.x + g.x) \;=\; a + b
\end{array}
$$

Next, we prove that every converging sequence is bounded. First, we establish:

$$
\begin{array}{ll}
& \lim_{x\to\infty} f.x = a \\
\equiv & \quad \{\ (26)\ \} \\
& \langle \forall\, \epsilon : \epsilon > 0 : \langle \diamondsuit\, x :: |f.x - a| < \epsilon \rangle \rangle \\
\Rightarrow & \quad \{\ \text{instantiation, with}\ \ \epsilon := \ 1\ \}
\end{array}
$$

$\langle \Diamond\!\!\!\!\Box\, x :: |f.x - a| < 1 \rangle$

$\Rightarrow$ { arithmetic }

$\langle \Diamond\!\!\!\!\Box\, x :: f.x \ < \ a + 1 \rangle$

Now we can prove boundedness of f :

$\langle \exists\, b :: \langle \forall\, x :: f.x < b \rangle \rangle$

$\equiv$ { range splitting on $f.x \ < \ a + 1$ }

$\langle \exists\, b :: \langle \forall\, x : f.x \ < \ a + 1 \ \vee \ f.x \ \geq \ a + 1 : f.x < b \rangle \rangle$

$\Leftarrow$ { predicate calculus }

$\langle \exists\, b :: b \ \geq \ a + 1 \ \wedge \ \langle \forall\, x : f.x \ \geq \ a + 1 : f.x < b \rangle \rangle$

$\equiv$ { above: $\langle \Diamond\!\!\!\!\Box\, x :: f.x \ < \ a + 1 \rangle$ so by (25) the maximum of the complement exists }

$\langle \exists\, b :: b \ \geq \ a + 1 \ \wedge \ b \ > \ \langle \uparrow\, x : f.x \ \geq \ a + 1 : f.x \rangle \rangle$

$\equiv$ { one point rule: $b \ = \ 1 + (a \uparrow \lceil \langle \uparrow\, x : f.x \ \geq \ a + 1 : f.x \rangle \rceil)$ }

true

Convergence of functions can also be characterised through the Cauchy criterion:

$$\langle \forall\, \epsilon : \epsilon > 0 : \langle \Diamond\!\!\!\!\Box\, x, y :: |f.x - f.y| < \epsilon \rangle \rangle \tag{27}$$

This follows from the existence of a limit, as proved below. (Note that the reverse implication relies on the function's codomain being a complete metric space.)

$\langle \forall\, \epsilon : \epsilon > 0 : \langle \Diamond\!\!\!\!\Box\, x, y :: |f.x - f.y| < \epsilon \rangle \rangle$

$\Leftarrow$ { arithmetic: $|x - c| < \epsilon \ \wedge \ |y - c| < \epsilon \quad \Rightarrow \quad |x - y| \ < \ 2 \cdot \epsilon$ }

$\langle \exists\, a :: \langle \forall\, \epsilon : \epsilon > 0 : \langle \Diamond\!\!\!\!\Box\, x, y :: |f.x - a| \ < \ \epsilon/2 \ \wedge \ |f.y - a| \ < \ \epsilon/2 \rangle \rangle \rangle$

$\equiv$ { dummy translation: $\epsilon' := \ 2 \cdot \epsilon$ }

$\langle \exists\, a :: \langle \forall\, \epsilon' : \epsilon' > 0 : \langle \Diamond\!\!\!\!\Box\, x, y :: |f.x - a| \ < \ \epsilon' \ \wedge \ |f.y - a| \ < \ \epsilon' \rangle \rangle \rangle$

$\equiv$ { unvector, i.e., (17) }

$\langle \exists\, a :: \langle \forall\, \epsilon' : \epsilon' > 0 : \langle \Diamond\!\!\!\!\Box\, x :: |f.x - a| \ < \ \epsilon' \rangle \ \wedge \ \langle \Diamond\!\!\!\!\Box\, y :: |f.y - a| \ < \ \epsilon' \rangle \rangle \rangle$

$\equiv$ { dummy renaming, with $y := \ x$; idempotence of $\wedge$ }

$\langle \exists\, a :: \langle \forall\, \epsilon' : \epsilon' > 0 : \langle \Diamond\!\!\!\!\Box\, x :: |f.x - a| \ < \ \epsilon' \rangle \rangle \rangle$

$\equiv$ { (26) }

$\langle \exists\, a :: \lim_{x \to \infty} f.x \ = \ a \rangle$

Remark. The above proofs still require extensive reasoning about the dummy variable ϵ in the definition of limits. A reviewer pointed out that one way of avoiding this may be by defining limits in terms of "limit superior" and "limit inferior", viz.

$$\begin{array}{l}\text{liminf } f \;=\; \langle \uparrow n :: \langle \downarrow m : m \geq n : f.n \rangle \rangle \\ \text{limsup } f \;=\; \langle \downarrow n :: \langle \uparrow m : m \geq n : f.n \rangle \rangle \\ \lim_{x\to\infty} f.x \;=\; a \quad \equiv \quad (\text{liminf } f = a \;\wedge\; \text{limsup } f = a)\end{array}$$

and that it may be useful to explore the connection between the $\langle\Box\rangle$ quantifier and infima and suprema over tails of sequences as used above.
End of Remark.

Towards calculational asymptotics

Our exploration of the "for large enough" quantifier was originally motivated by its application in proofs in asymptotics, which occur commonly in complexity theory and cryptography. Typically, as in the definition of limits, two quantities occur as dummies in asymptotic characterisations: the point where the function value is "close enough", and how close it is. The $\langle\Box\rangle$ quantifier eliminates the former, but not yet the latter (the ϵ in the limit definition). In this section we define relations between functions that address this issue.

In the rest of this section we overload constants to denote constant functions, where, in particular, variable x denotes the identity function, and we lift operators on numbers pointwise to operators on functions. Thus, $x+1$ in a position where a function is required denotes $\langle \lambda\, x :: x \rangle + \langle \lambda\, y :: 1 \rangle \;=\; \langle \lambda\, x :: x + 1 \rangle$ as expected.

Two types of asymptotic comparisons between functions exist: comparing asymptotic behaviour (based on absolute differences), and comparing asymptotic growth (based on relative differences). In the former, we define a number of operators between functions as follows:

$$f \leftrightarrow g \quad \equiv \quad \langle \forall\, \epsilon : \epsilon > 0 : \langle \langle\Box\rangle x :: |f.x - g.x| < \epsilon \rangle \rangle \tag{28}$$

$$f \lhd g \quad \equiv \quad \langle \forall\, \epsilon : \epsilon > 0 : \langle \langle\Box\rangle x :: 0 \;\leq\; g.x - f.x \;<\; \epsilon \rangle \rangle \tag{29}$$

$$f \rhd g \quad \equiv \quad g \lhd f \tag{30}$$

Oberserve that the above remove the dummy ϵ, with the first generalising the constant in the definition of a limit to a function.

The relation $\leftrightarrow$ is reflexive, symmetric and transitive; the proof of transitivity has the same shape as that for the addition of limits in the previous section. Indeed, we have that

$$\lim_{x\to\infty} f.x = a \quad \equiv \quad f \leftrightarrow a \tag{31}$$

Using this notation we can encode a number of "asymptotic" relations from the well-known textbook "Concrete Mathematics" [6]. The strict ordering of functions by asymptotic growth is captured by the following definition:

$$f \prec g \quad \equiv \quad f/g \leftrightarrow 0 \tag{32}$$

It is easy to prove from this that $\prec$ is transitive and irreflexive. We also write $g \succ f$ for $f \prec g$.

Useful relations in the world of asymptotic growth can be defined as follows:

$$f \ll g \quad \equiv \quad \langle \exists\, C :: \langle \diamondsuit x :: |f.x| \leq C \cdot |g.x| \rangle \rangle \tag{33}$$

$$f \asymp g \quad \equiv \quad f \ll g \ \wedge \ g \ll f \tag{34}$$

$$f \sim g \quad \equiv \quad f/g \leftrightarrow 1 \tag{35}$$

It is easy to prove that the first is a preorder and that the other two are equivalence relations. Our definition of $\asymp$ differs from the one in [6] in that the latter uses a single quantification over C for both instances of $\ll$. However, the two definitions are equivalent, as the inner predicate in the definition of $\ll$ is upward closed in C , so in both cases we can choose the maximum of the two instances of C .

Some further properties of these relations are stated below:

$$f \leftrightarrow g \ \wedge \ \neg(f \leftrightarrow 0) \quad \Rightarrow \quad f \sim g \tag{36}$$

$$\sim \quad \subseteq \quad \asymp \tag{37}$$

$$\asymp \quad \subseteq \quad \ll \tag{38}$$

$$\asymp \fatsemi \prec \quad \subseteq \quad \prec \tag{39}$$

$$\prec \fatsemi \asymp \quad \subseteq \quad \prec \tag{40}$$

where $\fatsemi$ denotes forward function composition. The reverse of (36) does not hold, e.g. $x \sim x+1$ but not $x \leftrightarrow x+1$.

As an example, in [7], for the full verification of a proof in [5], a proof obligation was to show that, for a polynomial a of degree at least 2,

$$\langle \diamondsuit x :: (1 - \tfrac{x}{a.x})^{a.x} < 2^{-x} \rangle$$

Starting from a standard result, we derive for constant C :

$$\begin{array}{ll} & (1 + \frac{C}{x})^x \leftrightarrow e^C \\ \Rightarrow & \quad \{ \text{ (21) , } f.x := a.x/x \text{ satisfies (19) } \} \\ & (1 + \frac{C}{a.x/x})^{a.x/x} \leftrightarrow e^C \\ \Rightarrow & \quad \{ \text{ (36) } \} \\ & (1 + \frac{C}{a.x/x})^{a.x/x} \sim e^C \end{array}$$

Also, we need a result based on continuity, which we state without further proof: if f is a curried two-argument function such that $f.x$ is continuous for large enough x, then

$$g \leftrightarrow h \quad \Rightarrow \quad f.x.(g.x) \leftrightarrow f.x.(h.x) \tag{41}$$

Then we calculate:

$$\begin{array}{ll} & (1 - \frac{x}{a.x})^{-a.x} \\ = & \quad \{ \text{ fractions } \} \\ & (1 + \frac{(-1)}{a.x/x})^{-a.x} \\ = & \quad \{ \text{ exponents } \} \\ & ((1 + \frac{(-1)}{a.x/x})^{a.x/x})^{-x} \\ \sim & \quad \{ \text{ above with } C := -1 \text{ , and (41) } \} \\ & (e^{-1})^{-x} \\ = & \quad \{ \text{ exponents } \} \\ & e^x \\ \succ & \quad \{ \ c^x \prec d^x \ \text{ for } \ 1 < c < d \ \} \\ & 2^x \end{array}$$

Using properties (37) to (40) we conclude from this calculation that

$$(1 - \tfrac{x}{a.x})^{-a.x} \ \succ \ 2^x$$

and using the definition of $\prec$ thus also

$$\langle \diamondsuit x :: (1 - \tfrac{x}{a.x})^{a.x} < 2^{-x} \rangle$$

as required.

We can also express so-called "Big Oh" notation using these relations. As stated in [6], this notation is usually defined in a particular context, e.g., for all arguments to the function, or near a fixed argument value, or for "large enough" arguments. In keeping with our application area, we assume the last case here. Thus, for functions on natural numbers, we have[1]

$$f \in O(g) \quad \equiv \quad f \ll g \tag{42}$$

Because $\ll$ is used but not given a separate notation in [6], this observation is missing there. The consequence that Θ (the intersection of "Big Oh" with

[1] Despite all the good reasons cited in [6] for writing "$f(x) = O(g(x))$" etc ("tradition [...] tradition [...] tradition [...] for our purposes it's natural."), we can't bring ourselves to do so. We do stick with a more traditional way of denoting the application of the O function though.

its converse) corresponds to $\asymp$ is included, and so is the link between $\prec$ and Landau's "little oh". An alternative characterisation we may use and explore further is finiteness of limsup $|f/g|$.

We now consider a number of the well-known properties of O , and how they may be proved in this set-up. Since $\ll$ is a preorder we have:

$$f \in O(f) \tag{43}$$

$$f \in O(g) \ \wedge \ g \in O(h) \quad \Rightarrow \quad f \in O(h) \tag{44}$$

Properties relating O to arithmetic operators would generally require unfolding the definition of $\ll$, for example:

$$f \in O(g) \ \Rightarrow \ C \cdot f \in O(g) \quad \text{for constant} \quad C \tag{45}$$

$$f_1 \in O(g_1) \wedge f_2 \in O(g_2) \ \Rightarrow \ f_1 + f_2 \in O(|g_1| + |g_2|) \tag{46}$$

$$f_1 \in O(g_1) \wedge f_2 \in O(g_2) \ \Rightarrow \ f_1 + f_2 \in O(g_1 \uparrow g_2) \quad \text{for positive} \quad g_1, g_2 \tag{47}$$

$$f_1 \in O(g_1) \wedge f_2 \in O(g_2) \ \Rightarrow \ f_1 \cdot f_2 \in O(g_1 \cdot g_2) \tag{48}$$

Finally, properties (36) to (38) allow all three kinds of asymptotic equivalence between f and g to be transformed into $f \in O(g)$.

Further applications

The original motivation for this work was found in cryptography. The second author's PhD thesis [7] explores calculational approaches to proofs in cryptography, which, in addition to traditional correctness notions and logic, contain elements of probabilism, number theory, complexity theory, and —through the latter— asymptotics.

Algebraic and symbolic reasoning has always been common in number theory, and typical proofs in this area are calculational and elegant. However, typical proofs in modern cryptography contain quantifications over algorithms and polynomials, with some of the quantifiers left implicit, and all of them changing between existential and universal in every (possibly nested) proof by contradiction. For the particular proof explored in detail in [7] (a demonstration proof from [5]), the "large enough" quantifier helped in the housekeeping of quantifications "in the context" and their acceptable manipulations. Notations explored in the previous section helped to structure and clarify a lemma based on asymptotics.

In general, this paper makes a small contribution to making modern cryptographic proofs more structured and manageable, with the ultimate goal of correctness by construction in modern cryptography. Our work in this area continues in the context of the UK EPSRC-funded CryptoForma network of excellence [8].

Acknowledgements

We would like to thank our colleagues in the TCS group, especially Stefan Kahrs and Simon Thompson, for fruitful discussions, and the MPC reviewers for many interesting and relevant suggestions.

References

0. E. Adams. The logic of 'almost all'. Journal of Philosophical Logic **3** (1974) 3–17
1. D. Marker and T. Slaman. Decidability of the natural numbers with the almost-all quantifier (2006) Available from `http://arxiv.org/abs/math/0602415v1`
2. A. Mostowski. On a generalization of quantifiers. Fundamenta Mathematicae **44** (1957) 12–36
3. N. Alechina and M. van Lambalgen. Correspondence and completeness for generalized quantifiers. Bulletin of the Interest Group in Pure and Applied Logic **3** (1995) 167–190
4. N. Alechina and J. van Benthem. Modal quantification over structured domains. In M. de Rijke, editor: Advances in Intensional Logic. Kluwer (1997) 1–27
5. O. Goldreich. Foundations of Cryptography: Volume I Basic Tools. Cambridge University Press (2001)
6. R. Graham, D. Knuth, and O. Patashnik. Concrete Mathematics. Second Edition. Addison-Wesley (1994)
7. D. Grundy. Concepts and Calculation in Cryptography. PhD thesis, Computing Laboratory, University of Kent (2008)
   Available from `www.cs.kent.ac.uk/∼eab2/crypto/thesis.web.pdf`
8. EPSRC CryptoForma network: `http://www.cryptoforma.org.uk`