The Logic of Large Enough

Eerke Boiten, Dan Grundy

School of Computing

University of Kent, UK

MPC 2010

Dan Grundy's PhD thesis (2008)

"Concepts and Calculation in Cryptography"

Available from www.cs.kent.ac.uk/~eab2/crypto/

Area with

- complex proofs (reduction, contradiction, probability);
- low confidence in proofs;
- little tradition of automation or calculation.

www.cryptoforma.org.uk

Large Enough

Asymptotic reasoning, complexity theory: properties hold "for large enough" numbers.

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

Assumption throughout: x and X are natural numbers.

Name this quantifier!
"Almost all", "all but finitely many"

$$\langle \diamondsuit\!\!\!\!\square\, x :: P \rangle \quad \equiv \quad \langle \exists X :: \langle \forall x : x > X : P \rangle \rangle$$

Intuition/notation: $\mathbb{N}$ as a timeline . . .

Known since 1970s, modal quantifiers since 1950s. (Emphasis: expressiveness, general class.)

Why useful?

- often left implicit in context – MPC "not done", real risks;
- where it *is* explicit: *two* dummies;
- its negation also interesting;
- basis for more notations (eliminate more dummies).

Basic properties (unsurprising)

If x does not occur free in P then

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

Proof:

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

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

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

$\equiv$ { $\forall$ not trivialised: non-empty range }

$\langle \exists X :: P \rangle$

$\equiv$ { $\exists$ not trivialised: non-empty range }

P

If x does not occur free in E then

$$\langle \diamondsuit x :: x > E \rangle \equiv \textbf{true}$$

From monotonicity of $\forall$ and $\exists$ we get:

$$\langle \forall\, x :: P \Rightarrow Q \rangle \;\Rightarrow\; (\langle \diamondsuit x :: P \rangle \Rightarrow \langle \diamondsuit x :: Q \rangle) \quad (0)$$

Intuitively

$$\langle \forall\, x :: P \rangle \quad \Rightarrow \quad \langle \diamondsuit x :: P \rangle$$

proved using (0):

$\langle \forall\, x :: P \rangle$

$\quad \equiv \;\{$ left identity of $\Rightarrow$, heading for (0) $\}$

$\langle \forall\, x :: \mathbf{true} \Rightarrow P \rangle$

$\quad \Rightarrow \;\{$ (0) with $P, Q := \mathbf{true}, P \;\}$

$\langle \diamondsuit x :: \mathbf{true} \rangle \;\Rightarrow\; \langle \diamondsuit x :: P \rangle$

$\quad \equiv \;\{$ x doesn't occur in $\mathbf{true}$ $\}$

$\mathbf{true} \;\Rightarrow\; \langle \diamondsuit x :: P \rangle$

$\quad \equiv \;\{$ left identity of $\Rightarrow$ $\}$

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

Conjunction

Conjunction distributes over $\langle\Diamond\!\!\!\!\Box\rangle$:

$$\langle\Diamond\!\!\!\!\Box\, x :: P\rangle \;\wedge\; \langle\Diamond\!\!\!\!\Box\, x :: Q\rangle \quad\equiv\quad \langle\Diamond\!\!\!\!\Box\, x :: P \;\wedge\; Q\rangle$$

Proof of $\Leftarrow$ from weakening;
$\Rightarrow$ starting with witnesses X_0 and X_1:

$\langle\forall\, x : x > X_0 : P\rangle \;\wedge\; \langle\forall\, x : x > X_1 : Q\rangle$

$\quad\Rightarrow\;\{\;$ arithmetic $\;\}$

$\langle\forall\, x : x > X_0 \uparrow X_1 :: P\rangle \;\wedge\; \langle\forall\, x : x > X_0 \uparrow X_1 : Q\rangle$

$\quad\equiv\;\{\;$ distributivity $\;\}$

$\langle\forall\, x : x > X_0 \uparrow X_1 :: P \;\wedge\; Q\rangle$

$\quad\Rightarrow\;\{\;\exists$-introduction, with $\;X := X_0 \uparrow X_1\;\}$

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

$\quad\equiv\;\{\;$ definition of $\langle\Diamond\!\!\!\!\Box\rangle\;\}$

$\langle\Diamond\!\!\!\!\Box\, x :: P \;\wedge\; Q\rangle$

From binary to general conjunction

Weakening also accounts for

$$\langle \forall\, y :: \langle \diamondsuit\!\!\!\!\cdot\, x :: P \rangle \rangle \;\Leftarrow\; \langle \diamondsuit\!\!\!\!\cdot\, x :: \langle \forall\, y :: P \rangle \rangle$$

but $\Rightarrow$ proof doesn't carry across: would need maximum of possibly infinite set. Indeed it doesn't hold: consider $x \geq y$ for P .

Consequence: can't have universally *and* large-enough quantified variables implicit in context at the same time. Worse, . . .

Multiple large enough

Definition for two simultaneous dummies:

$$\langle \diamondsuit\!\!\!\!\square\, x, y :: P \rangle \quad \equiv \quad \langle \exists\, X, Y :: \langle \forall\, x, y : x > X \wedge y > Y : P \rangle \rangle$$

Equivalently:

$$\langle \diamondsuit\!\!\!\!\square\, x, y :: P \rangle \;\equiv\; \langle \exists\, Z :: \langle \forall\, x, y : x > Z \wedge y > Z : P \rangle \rangle$$

Nesting property:

$$\langle \diamondsuit\!\!\!\!\square\, x, y :: P \rangle \quad \Rightarrow \quad \langle \diamondsuit\!\!\!\!\square\, x :: \langle \diamondsuit\!\!\!\!\square\, y :: P \rangle \rangle$$

(Proof next slide)

Proof:

$\langle \diamondsuit\!\!\!\!\diamondsuit\, x, y :: P \rangle$

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

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

$\quad \equiv \quad \{ \quad$ nesting of $\forall$ and of $\exists \quad \}$

$\langle \exists X :: \langle \exists Y :: \langle \forall x : x > X : \langle \forall y : y > Y : P \rangle \rangle \rangle \rangle$

$\quad \Rightarrow \quad \{ \quad \exists \forall \Rightarrow \forall \exists \quad \}$

$\langle \exists X :: \langle \forall x : x > X : \langle \exists Y : \langle \forall y : y > Y : P \rangle \rangle \rangle \rangle$

$\quad \equiv \quad \{ \quad$ definition of $\diamondsuit\!\!\!\!\diamondsuit$, twice $\quad \}$

$\langle \diamondsuit\!\!\!\!\diamondsuit\, x :: \langle \diamondsuit\!\!\!\!\diamondsuit\, y :: P \rangle \rangle$

$\Leftarrow$ does not hold: $y > x$ for P . (Same counterexample stops swapping $\diamondsuit\!\!\!\!\diamondsuit\, x$ and $\diamondsuit\!\!\!\!\diamondsuit\, y$.)

Consequence: if multiple $\diamondsuit\!\!\!\!\diamondsuit$ quantified variables in context, have to be explicit about their order (or lack of).

Infinitely many

The dual of $\langle\!\boxed{\diamond}\!\rangle$:

$$\langle \boxed{\diamond}\, x :: P \rangle \quad \equiv \quad \neg\langle \langle\!\diamond\!\rangle\, x :: \neg P \rangle$$

Consequently,

$$\langle \boxed{\diamond}\, x :: P \rangle \quad \equiv \quad \langle \forall\, X :: \langle \exists\, x : x > X : P \rangle \rangle$$

and also

$$\langle \boxed{\diamond}\, x :: P \rangle \quad \equiv \quad \langle x : P : x \rangle \text{ is infinite}$$
$$\langle \langle\!\diamond\!\rangle\, x :: P \rangle \quad \equiv \quad \langle x : \neg P : x \rangle \text{ is finite}$$

(Contradiction proofs of "large enough" via "infinitely many"!)

Application: Limits of sequences

$$\lim_{x\to\infty} f.x = a \;\equiv\; \langle \forall\, \epsilon : \epsilon > 0 : \langle \diamondsuit\!\!\!\!\!\!\square\; x :: |f.x - a| < \epsilon \rangle \rangle$$

(one less dummy)

E.g., for fixed $c > 0$,

$\lim_{x\to\infty} f.x = a$

$\equiv$ { definition of $\lim_{x\to\infty}$ }

$\langle \forall\, \epsilon : \epsilon > 0 : \langle \diamondsuit\!\!\!\!\!\!\square\; x :: |f.x - a| < \epsilon \rangle \rangle$

$\equiv$ { arithmetic }

$\langle \forall\, \epsilon : \epsilon > 0 : \langle \diamondsuit\!\!\!\!\!\!\square\; x :: |c \cdot f.x - c \cdot a| < c \cdot \epsilon \rangle \rangle$

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

$\langle \forall\, \epsilon' : \epsilon' > 0 : \langle \diamondsuit\!\!\!\!\!\!\square\; x :: |c \cdot f.x - c \cdot a| < \epsilon' \rangle \rangle$

$\equiv$ { definition of $\lim_{x\to\infty}$ }

$\lim_{x\to\infty} c \cdot f.x = c \cdot a$

Every converging sequence is bounded.

First:

$$\lim_{x \to \infty} f.x = a$$

$$\equiv \quad \{ \quad \text{definition of } \lim_{x \to \infty} \quad \}$$

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

$$\Rightarrow \quad \{ \quad \text{instantiation, with } \quad \epsilon := \ 1 \quad \}$$

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

$$\Rightarrow \quad \{ \quad \text{arithmetic} \quad \}$$

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

Now we can prove boundedness of f :

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

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

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

$\quad \Leftarrow \{$ predicate calculus $\}$

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

$\equiv \{$ $\uparrow$ exists: complement of cofinite set $\}$

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

$\equiv \{$ one point rule: take $b >$ both bounds $\}$

true

Towards calculational asymptotics

Asymptotics: "at extremes things get very close".
$\langle\Box\rangle$ eliminates quantification of "how extreme" but not of "how close" (ϵ).

Asymptotic comparisons (based on absolute differences):

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

$$f \triangleleft g \quad \equiv \quad \langle \forall\, \epsilon : \epsilon > 0 : \langle \langle\Box\rangle\, x :: 0 \leq g.x - f.x < \epsilon \rangle \rangle$$

Properties . . .

Asymptotic comparisons (relative differences):

$$
\begin{array}{lcl}
f \prec g & \equiv & f/g \leftrightarrow 0 \\
f \ll g & \equiv & \langle \exists\, C :: \langle \diamondsuit\!\!\!\!\!\!\square\; x :: |f.x| \leq C \cdot |g.x| \rangle \rangle \\
f \asymp g & \equiv & f \ll g \;\wedge\; g \ll f \\
f \sim g & \equiv & f/g \leftrightarrow 1
\end{array}
$$

Properties: order-like, and

$$
\begin{array}{rcll}
f \leftrightarrow g \;\wedge\; \neg(f \leftrightarrow 0) & \Rightarrow & f \sim g \\
\sim & \subseteq & \asymp \\
\asymp & \subseteq & \ll \\
\asymp \;\frac{9}{9}\; \prec & \subseteq & \prec \\
\prec \;\frac{9}{9}\; \asymp & \subseteq & \prec
\end{array}
$$

Big Oh

$$f \in O(g) \quad \equiv \quad f \ll g$$

Known properties of $\ll$ lead to

$$\begin{array}{lll} & & f \in O(f) \\ f \in O(g) \ \wedge \ g \in O(h) & \Rightarrow & f \in O(h) \end{array}$$

and unfold $\ll$ for

$$\begin{array}{rcl} f \in O(g) & \Rightarrow & C \cdot f \in O(g) \\ f_1 \in O(g_1) \wedge f_2 \in O(g_2) & \Rightarrow & f_1 + f_2 \in O(|g_1| + |g_2|) \\ f_1 \in O(g_1) \wedge f_2 \in O(g_2) & \Rightarrow & f_1 + f_2 \in O(g_1 \uparrow g_2) \\ f_1 \in O(g_1) \wedge f_2 \in O(g_2) & \Rightarrow & f_1 \cdot f_2 \in O(g_1 \cdot g_2) \end{array}$$

$f \in O(g)$ from each asymptotic equivalence.

What next?

- expand these calculational theories; explore $\limsup$

- more big proofs;

- more algebraic theory for one-way functions.