Verification of the Miller-Rabin Probabilistic Primality Test

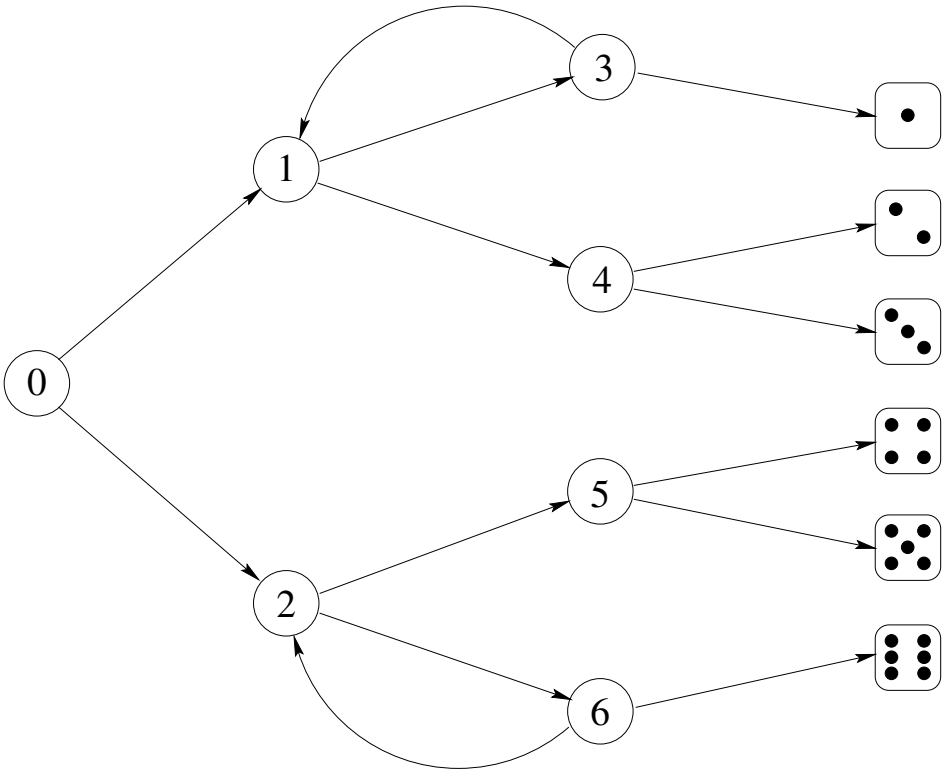
Joe Hurd

University of Cambridge

1. HOL Probability Theory
2. Miller-Rabin Verification
3. Composite Prover

HOL Probability Theory

In HOL we can model a probabilistic program $\hat{f} : \alpha \to \beta$ with a deterministic equivalent $f : \alpha \to \mathbb{B}^\infty \to \beta \times \mathbb{B}^\infty$ that passes around an infinite sequence of fair coin flips.



Miller-Rabin Verification

We define in HOL a probabilistic function miller_rabin, and prove the following two properties of it:

$$\vdash \quad \forall\, n, t, s.$$
$$\mathsf{prime}\ n \ \Rightarrow$$
$$\mathsf{fst}\ (\mathsf{miller\_rabin}\ n\ t\ s) = \top$$

$$\vdash \quad \forall\, n, t.$$
$$\neg(\mathsf{prime}\ n) \ \Rightarrow$$
$$1 - 2^{-t} \leq \mathbb{P}\,\{s : \mathsf{fst}\ (\mathsf{miller\_rabin}\ n\ t\ s) = \bot\}$$

The Miller-Rabin algorithm is a probabilistic primality test, used by commercial software such as Mathematica.

Composite Prover

By defining a pseudo-random number generator in HOL, we can execute the Miller-Rabin algorithm in the logic (using Barras' `computeLib`).

This allows us to prove that large numbers are composite, without needing to know their factors. For example, the following Fermat numbers can be shown to be composite in this way:

$$\vdash \quad \neg\mathsf{prime}(2^{2^6}+1)$$
$$\vdash \quad \neg\mathsf{prime}(2^{2^7}+1)$$
$$\vdash \quad \neg\mathsf{prime}(2^{2^8}+1)$$