

# ON THE MINIMUM EXPECTED DURATION OF A COIN TOSSING GAME

Inchi Hu\*     Santosh S. Venkatesh†

## ABSTRACT

The following coin tossing game is analysed: A store of  $N$  fair coins is given and it is desired to achieve  $M$  heads in a round of tosses of the coins. To allow for unfavourable sequences of tails, restarts are permitted at any epoch in the game where, in any restart, all coins are returned to store and tosses are begun anew from tabula rasa. A restart strategy is a prescription which specifies when a restart should be made. It is desired to estimate the minimum expected duration of the game over all restart strategies, and to find an optimal strategy which minimises the expected duration of the game. This simple coin tossing game, proposed by R. L. Rivest, has cryptographic roots and is linked to issues in the factoring of integers.

It is shown that there exists an optimal deterministic strategy which minimises the expected duration of the game, and a backward induction algorithm is derived which efficiently yields the optimal strategy. The properties of the optimal strategy are characterised, and some sub-optimal strategies analysed. In particular, it is shown that if the desired number of heads  $M$  is less than or equal to one-half the number of coins  $N$  in the store, then the minimum expected duration of the game grows linearly in  $N$ ; if, on the other hand,  $M$  exceeds one-half  $N$ , then the minimum expected duration of the game grows exponentially fast in  $N$ .

---

\*Department of Statistics, University of Pennsylvania, Philadelphia, PA 19104

†Department of Electrical Engineering, University of Pennsylvania, Philadelphia, PA 19104; *electronic mail*: venkatesh@ee.upenn.edu