Abstract

In a multi-party *fair* coin-flipping protocol, the parties output a common (close to) unbiased bit, even when some corrupted parties try to bias the output. In this work we focus on the case of dishonest majority, i.e. at least half of the parties can be corrupted. Cleve [STOC 1986] has shown that in *any* m-round coin-flipping protocol the corrupted parties can bias the honest parties' common output bit by $\Theta(1/m)$. For more than two decades the best known coin-flipping protocols against majority was the protocol of Awerbuch, Blum, Chor, Goldwasser and Michali [Manuscript 1985], who presented a t-party, m-round protocol with bias $\Theta(t/\sqrt{m})$. This was changed by the breakthrough result of Moran, Naor, and Segev [TCC 2009], who constructed an m-round, *two*-party coin-flipping protocol with optimal bias $\Theta(1/m)$. Recently, Haitner, and Tsfadia [STOC 14] constructed an m-round, *three*-party coin-flipping protocol with bias $O(\log^3 m/m)$. Still for the case of more than three parties, against arbitrary number of corruptions, the best known protocol remained the $\Theta(t/\sqrt{m})$-bias protocol of Awerbuch et al. We make a step towards eliminating the above gap, presenting a t-party, m-round coin-flipping protocol, with bias $O(\frac{t^3 \cdot 2^t \cdot \sqrt{\log m}}{m^{1/2+1/(2^{t-1}-2)}})$. This improves upon the $\Theta(t/\sqrt{m})$-bias protocol of Awerbuch et al. for any $t \leq 1/2 \cdot \log\log m$, and in particular for $t \in O(1)$, this yields an $1/m^{\frac{1}{2}+\Theta(1)}$-bias protocol. For the three-party case, this yields an $O(\sqrt{\log m}/m)$-bias protocol, improving over the the $O(\log^3 m/m)$-bias protocol of Haitner, and Tsfadia. Our protocol generalizes that of Haitner and Tsfadia, by presenting an appropriate "defense protocols" for the remaining parties to interact in, in the case that some parties abort or caught cheating Haitner, Tsfadia, only presented a two-party defense protocol, which limits their final protocol to handle three parties). We analyze our new protocols by presenting a new paradigm for analyzing fairness of coin-flipping protocols. We map the set of adversarial strategies that try to bias the honest parties outcome in the protocol to the set of the feasible solutions of a linear program. The gain each strategy achieves is the value of the corresponding solution. We then bound the the optimal value of the linear program by constructing a feasible solution to its dual.