Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation

Michael Ben-Or
Shafi Goldwasser
Avi Wigderson

Abstract

Every function of n inputs can be efficiently computed by a complete network of n in such a way that:

1. If not faults occur, no set of size $t <n/2$ of players gets any additional information (other than the function value),
2. Even if Byzantine faults are allowed, no set of size $t<n/3$ can either disrupt the computation or get additional information.

Furthermore, the above bounds on t are tight!