Simple and Efficient Leader Election in the Full Information Model

Rafail Ostrovsky* Sridhar Rajagopalan† Umesh Vazirani†

Abstract

In this paper, we study the leader election problem in the full information model. We show two results in this context. First, we exhibit a constructive $O(\log N)$ round protocol that is resilient against linear size coalitions. That is, our protocol is resilient against any coalition of size less then βN for some constant (but small) value of β. Second, we provide an easy, non-constructive probabilistic argument that shows the existence of $O(\log N)$ round protocol in which β can be made as large as $\frac{1}{2} - \epsilon$ for any positive ϵ. Our protocols are extremely simple.

* Computer Science Division, University of California at Berkeley, and International Computer Science Institute, Berkeley, CA 94720. Email: rafail@cs.Berkeley.EDU. Supported by an NSF Postdoctoral Fellowship and ICSI.

†Computer Science Division, University of California at Berkeley, CA 94720. Email: {sridhar, vazirani}@cs.Berkeley.EDU. Supported by NSF grant IRI 91-20074 and CCR-9310214.

1 Introduction

A central problem in distributed computing is that of generating a common coin or, equivalently, of electing a leader. We consider this problem in the setting where there is a coalition of malicious players who are trying to maximize the chances of one of them being elected as a leader. A protocol, on the other hand must guarantee that there is a reasonable chance that an honest player will be elected regardless of any devious plot hatched by the coalition. This problem has been extensively studied in the cryptographic setting, culminating in the constant expected time Byzantine Agreement algorithm of Feldman and Micali [FM-88]. In this paper, we consider this question in the full-information model introduced by Ben-Or and Linial [BL-85, BL-89]. This model is characterized by the following two "worst case" assumptions. First, that all communication is public and made via broadcast channels. That is, no two processors share a private communication channel. The second, is that dishonest players are capable of arbitrarily complicated computations. Honest players however, are required to work in polynomial time. There are two parameters of interest in this setting: *resilience* and *efficiency*.

Resilience deals with the number of dishonest players that a protocol can tolerate. Let us consider a system with N players. A protocol is β-immune if it can tolerate a coalition of size smaller than βN dishonest players. Clearly, the objective here is to make β as large as possible. A great deal of effort has been invested in designing protocols which can tolerate a constant value of β. A sequence of papers, [BL-85, BLS-87, BL-89, AR-89, S-89, AN-90, BN1-93, BN2-93] resulted in proof of the existence of a protocol that has optimal immunity (any $\beta < \frac{1}{2} - \epsilon$ for any positive ϵ).

We measure efficiency in terms of the number of *rounds* of communication. In each round, every player can send a single message. Players can send messages during the same round in an asynchronous manner. That is, the notion of a round models the effects of distributed asynchrony, and the beginning of each round represents a synchronization point in the protocol. Clearly, minimizing the number of rounds is crucial since we minimize the number of times the system needs to be synchronized. (For more complete definitions see section 2.) The non-constructive protocol which achieves optimal immunity [AN-90, BN2-93] requires a linear number of rounds. Cooper and Linial [CL-93] gave the first (and only previously known) protocol that runs in a sub-linear $O(\log^{17} N)$ number of rounds and simultaneously achieves a constant (but small) immunity. The Cooper-Linial protocol is constructive.

In this paper we exhibit simple protocols that improve upon best previous results in various ways:

- We first exhibit a constructive protocol which can tolerate a constant fraction βN (for any $\beta < .0045$) of malicious players and runs in $O(\log N)$ rounds. (This compares favorably to $O(\log^{17} N)$ constructive protocol of [CL-93] which also achieves linear resilience.)
- We then show, using an Erdös probabilistic argument, the existence of a protocol that also requires $O(\log N)$ rounds and can tolerate any $(\frac{1}{2} - \epsilon)N$ malicious players for all positive ϵ. (This compares favorably to the non-constructive protocol of [AN-90, BN2-93] which also achieves optimal resilience but runs in $O(N)$ number of rounds.)

1.1 Previous work

The problem of leader election and collective coin-flipping has received much attention in the literature. (For example, as a good introduction, see surveys of Ben-Or, Linial and Saks [BLS-87], Chor, Dwork [CD-89] and Linial [L-92].) This problem is studied in principally two settings: the cryptographic setting and the information theoretic setting. In the cryptographic setting some cryptographic assumptions are made and the computational power of all players is limited. In the information theoretic setting, no such assumptions are made and faulty processors are assumed to be capable of arbitrarily complicated computation.

Under cryptographic assumptions [GMW-87] or assuming private channels between processors [BGW-88, CCD-88], it is possible to flip a common coin in a constant expected number of rounds if less than $\frac{1}{3}$ of the processors are faulty [FM-88]. Since this setting is not the focus of this paper, we will not review the rest of the extensive literature in this area. The interested reader is referred to the survey in Chor and Dwork [CD-89].

In the information-theoretic setting, and without the use of private channels, the problem was first formulated by Ben-Or and Linial [BL-85, BL-89]. In the first paper, Ben-Or and Linial propose a protocol that is $N^{(\log_3 2)-1}$-immune. The second paper improved upon this result and exhibited a one-round $1/\log N$-immune protocol. A widely known result due to Kahn, Kalai and Linial [KKL-88], implies that if each processor were restricted to providing one random bit, then $1/\log N$ is the largest possible value of β for any one round protocol.

Since then, protocols were designed that were resilient against larger and larger coalitions [S-89, AL-89, AN-90, BN1-93, BN2-93]. In particular, Saks [S-89], Ajtai and Linial [AL-89] designed so-called baton-passing protocols which are $1/\log N$-immune. Furthermore, Saks [S-89] also showed that no protocol can be immune against $\lceil \frac{N}{2} \rceil$ coalitions. Finally, Alon and Naor were able to exhibit a protocol which is β-immune for any $\beta < \frac{1}{3}$. This constituted major progress since it established that a very large number of dishonest players can be tolerated. Further analysis of the protocol of Alon and Naor was done by Boppana and Narayanan where they showed that the protocol of Alon and Naor is β-immune for all $\beta < 0.44$ in [BN1-93] and for all $\beta < \frac{1}{2} - \epsilon$ and positive ϵ in [BN2-93], establishing that the protocol of Alon and Naor [AN-90] has, in fact, optimal resilience. Notice, however, that Alon and Naor solution requires linear number of rounds.

A faster (in the number of rounds) solution was constructed by Cooper and Linial [CL-93], where they showed a fairly complicated protocol which requires $O(\log^{17} N)$ rounds and is c-immune for some small constant c.

2 Problem Statement

There are N players: in what follows we will use players and processors interchangeably. All communication is via broadcast and is public. Every processor has a unique name and the name of the sender of any message is explicitly known to all other processors. The goal is to choose one of the N players (a leader) in this setting. This seemingly simple matter becomes complicated if some βN of the players are involved in a dishonest coalition. This means that they do not necessarily adhere to any specified protocol. Further, given any protocol, they will behave in a way as to maximize the chances of one among themselves being elected leader. A protocol is said to be β-immune if regardless of which βN of the players are dishonest, the protocol chooses an honest leader with probability bounded away from 0 as N approaches infinity.

A *round* is a round of communication. It consists of a broadcast message of polynomial length transmitted by each player. In principle, all messages are to be transmitted and received in parallel. However, in a distributed system, there is no guarantee on the order in which messages are sent or delivered within a round. Thus, within any round, dishonest players may receive (or consciously wait until they receive), the messages of the honest players before they compose their own. The processors are synchronized between rounds. Thus, all messages in round i are received before any in round $i+1$ are transmitted. This models the effects of distributed asynchrony in the most pessimistic (and thus, the most difficult) case.

Finally, honest processors have to work in polynomial time. There is however no such computational limitation on the dishonest ones. This stipulation rules out the use of cryptographic assumptions.

3 The protocol

A *committee* is a subset of the processors [B-85]. The protocol first constructs a collection $\mathcal{C}$ of committees. The committees are constructed by choosing an explicit constant degree d expander graph on $N + o(N)$ vertices (for example, see [GG-79]). Each player is represented by some vertex in the expander graph. Each committee is composed of the players represented by different vertices in a $k \log N$ long walk on the expander graph where k is a fixed constant. A player can be a member of a committee a multiple number of times. It is easily verified that there are only a polynomial number M of such walks[1].

The protocol works in two stages. In the first stage, a committee $C \in \mathcal{C}$ will be chosen. In the second stage, a leader is chosen in C. The second stage is accomplished by using the [AN-90, BN2-93] sequential protocol. Since $|C|$ is only logarithmic in N, the second stage runs in time $O(\log N)$. Henceforth, we will concentrate on the first stage[2].

The first stage works in a series of rounds. At the beginning, all M committees are marked 'eligible'. Let $\mathcal{E}_i$ be the collection of eligible committees at the inception of round i. In round i, each player publishes a list of size $\left\lceil \frac{|\mathcal{E}_i|}{N} \right\rceil$. Each entry in this list is the name of a committee in $\mathcal{E}_i$. In the case of honest players each entry is chosen independently and randomly from $\mathcal{E}_i$. Dishonest players may choose their lists in any arbitrary fashion. Every committee in the published lists are marked 'not eligible'. The protocol terminates when there are fewer than N committees left in the eligible set. At this point player 1 chooses an arbitrary committee C from among the remaining eligible committees. If there is no such committee, the protocol fails. In section 5 we prove the following theorem pertaining to this protocol:

Theorem 5.1: The protocol described here is an $O(\log N)$ round leader election protocol that is β-immune for every β smaller than .0045.

4 Committees

The notion of a *committee* was introduced by Bracha [B-85] in the context of the Byzantine agreement problem, and has since become an important tool for designing resilient protocols. It has been used in many of the earlier papers on leader election in the full-information model.

In our protocol, each committee was chosen by a $k \log N$ length walk on the expander graph. We say that a committee is *dangerous* if the fraction of bad processors in it exceeds $\beta + \delta$ for some fixed δ. Our choice of committees guarantees that the fraction of dangerous committees tends to zero rapidly as we increase the number of committees (by increasing k). There are various proofs of this kind of notion in the recent literature (see for instance [IZ-89]). We choose to state here a derivative of the theorem of Gillman [G-93]. Gillman provides a Chernoff style bound on the visit statistic for each subset S of vertices during a random walk on any expander graph.

[1] The number of committees is smaller $N \cdot d^{k \log N}$. The first factor represents the number of starting points and the second factor the number of walks from each starting point. Each walk is a committee.

[2] Alternately, one could elect a leader in C recursively. However, that complicates the analysis and we choose to state the protocol like this for simplicity. Moreover, notice that the second stage works on a problem instance of size $O(\log N)$ and hence is constructive even though we use the non-constructive algorithm of [AN-90, BN2-93].

Lemma 4.0.1 It is possible to choose a collection $\mathcal{C}$ of committees such that:

- $|\mathcal{C}| = M \leq \text{poly}(N)$. The degree of the polynomial depends on k and the out degree of the expander graph.
- If $\mathcal{B}$ is the set of all dangerous committees, then $|\mathcal{B}| \leq M^{1-\lambda\delta^2}$ for some fixed constant $\lambda < 1$. [3]

5 The proof

In this section we will address the two issues that arise in proving the main theorem in this paper. We first address the easier issue, and show that the protocol runs in $O(\log N)$ rounds. Then, we address the main issue, that of showing that the protocol described here has the required immunity.

5.1 Rounds

Consider an arbitrary committee $C \in \mathcal{C}$. The probability that C is eliminated in an arbitrary round i is at least the probability that C is eliminated by one of the votes cast by the honest players. There are roughly $(1-\beta)\,|\mathcal{E}_i|$ votes cast by honest players.[4] Each vote eliminates C with probability $\frac{1}{|\mathcal{E}_i|}$. Thus, we obtain

$$\begin{aligned} & Pr\,[C \text{ is not eliminated in round } i \mid C \in \mathcal{E}_i] \\ \leq\ & (1 - \frac{1}{|\mathcal{E}_i|})^{(1-\beta)|\mathcal{E}_i|} \\ \approx\ & e^{-(1-\beta)} \end{aligned}$$

Therefore, we have:

$$Pr[C \in \mathcal{E}_{i+1}] \leq e^{-i(1-\beta)}$$

So, we have the following lemma:

Lemma 5.1.1 With probability $1 - \frac{1}{N}$, the protocol completes in fewer than $\frac{\ln M}{1-\beta}$ rounds.

Proof : By substituting $\frac{\ln M}{1-\beta}$ for i in the preceding discussion and applying Markov's inequality. □

5.2 Resilience

The proof of the resilience of this protocol is based on a simple but crucial trade-off that we elaborate upon next. As we increase β, the rate at which $\mathcal{E}$ decays becomes increasingly faster with respect to the rate at which $\mathcal{B}$ decays. The protocol works if β is small enough so that this increased decay rate of $\mathcal{E}$ is still not enough to overcome the initial size disadvantage that $\mathcal{B}$ had with respect to $\mathcal{E}$. In this case, all the bad

[3] The value of λ depends on the gap between the largest and next largest eigenvalues for the expander graph. The theorem of Gillman implies that λ can be taken to be roughly $\frac{1}{20}$th the eigenvalue gap. Expanders that have an eigenvalue gap arbitrarily close to 1 are known. We note that Gillman's bound is somewhat weaker then the standard Chernoff bound in the sense that λ should ideally be close to 1/2. An improvement in this direction will immediately yield an increase in the value of β in our main theorem (5.1). Nabil Kahale [K-94] has communicated to us that he can show such an improvement.

[4] It is easily verified that the approximation made here is justified.

committees will be eliminated before there are only N eligible committees left. The resilience figure, .0045 represents the value of β where the trade-off between the the decay rate and the initial size disadvantage is made.

If we choose δ so that $\beta + \delta < \frac{1}{2}$, then, it suffices to show that the probability that the committee C, is dangerous is small. Recall that C is the committee that is chosen after the first stage of the protocol. This is because of the following reasoning: Let δ be chosen to be such that $\beta + \delta < \frac{1}{2}$. Then, if C is not dangerous, by definition, the fraction of bad players in C is smaller than $\frac{1}{2}$. Thus, we can use the result of Boppana and Narayanan [BN2-93] to complete our proof immediately.

Lemma 5.2.1 If $\ell \geq \frac{\ln(N|\mathcal{B}|)}{(1-\beta)}$, then

$$Pr(\exists \text{ a dangerous committee in } \mathcal{E}_\ell) \leq \frac{1}{N}$$

Proof : Let $C \in \mathcal{B}$ be a dangerous committee. Consider a fixed round i in the first phase. Each vote cast by an honest player in this round eliminates C with probability $\frac{1}{|\mathcal{E}_i|}$. There are $(1-\beta)\,|\mathcal{E}_i|$ votes cast by honest players. Thus, the probability that C is not eliminated in the i^{th} round is at most $\left(1 - \frac{1}{|\mathcal{E}_i|}\right)^{(1-\beta)|\mathcal{E}_i|} \approx e^{-(1-\beta)}$. Therefore, the probability that C is not eliminated in rounds 1 through ℓ is $e^{-(1-\beta)\ell}$. Thus, we get

$$\mathrm{E}\ (|\mathcal{E}_\ell \cap \mathcal{B}|) \leq e^{-\ell(1-\beta)}\,|\mathcal{B}|$$

If we apply Markov's inequality and substitute the value of ℓ we obtain the lemma. □

Lemma 5.2.1 states that if the protocol runs for more than $\frac{\ln(N|\mathcal{B}|)}{(1-\beta)}$ rounds, then it is highly unlikely that any dangerous committee survives. In order to complete the proof, it would be sufficient to show that it is very likely that the protocol runs for at least $\frac{\ln(N|\mathcal{B}|)}{(1-\beta)}$ rounds. This is what we shall exhibit now. We begin with a lemma that is a simple form of what is sometimes called a Chernoff bound. It provides an exponentially small upper bound on the probability that the sum of i.i.d. random variables deviates significantly from the expected value.

Lemma 5.2.2 (Chernoff bound) Let $X_1, X_2 \cdots X_{(1-\beta)t}$ be uniformly and independently chosen from $\{1, 2, \cdots t\}$. Let $Y_i = 1$ if $\exists j$ such that $X_j = i$. Let $Y = \sum_1^t Y_i$. Then, $\mathrm{E}\,(Y) = t(1 - e^{-(1-\beta)})$ and $Pr(|Y - \mathrm{E}\,(Y)| \geq \log t\sqrt{t}) \leq o\left(\frac{1}{\mathrm{poly}(t)}\right)$

Proof : Standard. □

Lemma 5.2.3 Let $Z_i = |\mathcal{E}_{i+1}|$. Let $p = e^{-(1-\beta)} - \beta$. If $\theta_i = \alpha i \log^2 N \sqrt{p^i\,|\mathcal{C}|}$, for $\alpha = \frac{1}{\sqrt{p}}$, then for any $i \leq N$,

$$Pr\left[Z_i < p^i\,|\mathcal{C}| - \theta_i\right] \leq o\left(\frac{1}{\mathrm{poly}(N)}\right)$$

Consequently, if $\ell \leq -\frac{\ln\left(\frac{|\mathcal{C}|}{N}\right)}{\ln\left(e^{-(1-\beta)} - \beta\right)}$, then

$$Pr\left[Z_\ell \geq N\right] \geq 1 - o\left(\frac{1}{\mathrm{poly}(N)}\right)$$

Proof : We will show the following conditional statement for every choice of k. The lemma and its consequence follow by simply taking a union bound over all k thereafter.

$$Pr\left[Z_k \leq p^k \left|\mathcal{C}\right| - \theta_k \middle| Z_{k-1} \geq p^{k-1}\left|\mathcal{C}\right| - \theta_{k-1}\right] \leq o\left(\frac{1}{\text{poly}(N)}\right)$$

This conditional statement follows immediately with the help of the following consequence of the Chernoff bound described above.

$$Pr\left[Z_k \leq pZ_{k-1} - \log N\sqrt{Z_{k-1}}\right] \leq o\left(\frac{1}{\text{poly}(N)}\right)$$

Conditioning on the value of Z_{k-1} we obtain the following.

$$Pr\left[Z_k \leq pZ_{k-1} - \log N\sqrt{Z_{k-1}} \middle| Z_{k-1} \geq p^{k-1}\left|\mathcal{C}\right| - \theta_{k-1}\right] \leq o\left(\frac{1}{\text{poly}(N)}\right)$$

Plugging in the value of θ_{k-1} and doing a little algebraic manipulation gives the the conditional statement and hence, the lemma. □

Theorem 5.1 The protocol described in section 3 is an $O(\log N)$ round leader election protocol that is β-immune for every β smaller than .0045.

Proof : The lemmas 5.2.1 and 5.2.3 together imply that if ℓ is chosen such that $\frac{\ln(N|\mathcal{B}|)}{(1-\beta)} < \ell < \frac{\ln\left(\frac{|\mathcal{C}|}{N}\right)}{-\ln\left(e^{-(1-\beta)}-\beta\right)}$, then after ℓ rounds, it is very likely that all the dangerous committees are gone and that the first phase is not yet complete. This in turn implies that the committee C is unlikely to be dangerous. We know that $|\mathcal{C}| = M$ and $|\mathcal{B}| = M^{1-\lambda\delta^2}$ where λ is 1/20th of eigenvalue gap for the expander graph of our choice. We also take note that there are explicit expander constructions that produce expanders with eigenvalue gap arbitrarily close to 1.

Substituting these values, we notice that if is sufficient if we can find an ℓ satisfying

$$\frac{\ln(NM^{1-\lambda\delta^2})}{(1-\beta)} < \ell < \frac{\ln\left(\frac{M}{N}\right)}{-\ln\left(e^{-(1-\beta)}-\beta\right)}$$

Notice further that as we increase the length of the walk on the expander in the construction of the committees by increasing k, and thus increase M relative to N, $\ln(NM^{1-\lambda\delta^2}) \approx (1-\lambda\delta^2)\ln M$ and $\ln(\frac{M}{N}) \approx \ln M$. Thus, we need to find a ℓ satisfying

$$\frac{(1-\lambda\delta^2)\ln(M)}{(1-\beta)} < \ell < \frac{\ln(M)}{-\ln\left(e^{-(1-\beta)}-\beta\right)}$$

Finally, we notice that if β is small enough, then such an ℓ exists. The largest possible value of β is easily computed as the solution the equation

$$\frac{(1-\lambda\delta^2)}{(1-\beta)} = \frac{1}{-\ln\left(e^{-(1-\beta)}-\beta\right)}$$

where $\delta = \frac{1}{2} - \beta$ and λ is $\frac{1}{20}$. It is easily verified that the solution to the above equation is at least .0045. This completes the proof of the main theorem. □

6 Non Uniform protocols

In this section we study non-uniform protocols. We assume, in this case, that we design our protocol probabilistically. It is easy to see that this situation implies the non-uniform case. The part of the protocol that we single out for attention is the construction of committees. Suppose we replace the expander based deterministic construction by a random construction as follows. A collection $\mathcal{C} = \{C_i : 1 \leq i \leq M\}$ of committees is chosen with $|C_i| = k \log N$. Each member of each committee is chosen independently and uniformly at random from $\{1, 2, \cdots N\}$.

Let X, $|X| = \beta N$ be any subset of $\{1, 2, \cdots N\}$. We wish to view X as the set of dishonest players. An immediate consequence of the Chernoff bound is that for any i

$$Pr\left[|X \cap C_i| \geq (\beta + \delta)\,|C_i|\right] \leq 2^{\frac{-\delta^2 k \log N}{4}}$$

Here, the probability is taken over all possible choices of C_i. Thus, if k is chosen to be $\frac{4\mu}{\delta^2}$ where μ is an yet un-chosen constant, then,

$$Pr\left[|X \cap C_i| \geq (\beta + \delta)\,|C_i|\right] \leq N^{-\mu}$$

Let $\mathrm{Bad}(X)$ be the sets in $\mathcal{C}$ such that $|C_i \cap X| \geq (\beta + \delta)\,|C_i|$. Then, clearly, the expected size of $\mathrm{Bad}(X)$ is at most $N^{-\mu}M$. Additionally, for any α, the probability that the size of $\mathrm{Bad}(X)$ exceeds αM is at smaller than $\left(\begin{array}{c} M \\ \alpha M \end{array} \right) N^{-\mu\alpha M}$. Using the fact that $\left(\begin{array}{c} M \\ \alpha M \end{array} \right) < M^{\alpha M}$ and choosing $\alpha = N/M$, we obtain,

$$Pr(|\mathrm{Bad}(X)| \geq N) \leq \left(\frac{M}{N^{\mu}}\right)^N$$

If we choose μ to be a large enough constant so that $M \leq N^{\mu - 1}$, we observe that

$$Pr(|\mathrm{Bad}(X)| \geq N) \leq N^{-N}$$

Since there are at most 2^N possible choices for X, we get the following lemma,

Lemma 6.0.4 There exists a collection $\mathcal{C} = \{C_i : 1 \leq i \leq M\}$ of committees such that for any X of size βN, $|\mathrm{Bad}(X)| \leq M^{1-\lambda}$ for any $\lambda < 1$. The size of M is polynomial in N. The degree of the polynomial depends only on λ. And so that the size of any committee C_i is $O(\log N)$. The size of committees depends polynomially on λ^{-1} and $(\frac{1}{2} - \beta)^{-1}$.

Proof : Consider the union bound over the possible choices of X in the previous discussion. □

It is now easily seen that by choosing the value of $\lambda = 4/5$, the root of the equation

$$\frac{(1-\lambda)}{(1-\beta)} = \frac{1}{-\ln\left(e^{-(1-\beta)} - \beta\right)}$$

is larger than $\frac{1}{2}$. Thus, showing the existence of a protocol that is $\frac{1}{2}$-immune and runs in $O(\log N)$ rounds. This completes the proof of the second main theorem:

Theorem 6.1 For every $\epsilon > 0$, there exists an $O(\log N)$ round leader election protocol that is β-immune for $\beta = \frac{1}{2} - \epsilon$.

7 Further Research and Open Problems

We remark that due to the inherent simplicity of our solution it is conceivable that our technique can be parallelized in order to reduce the number of rounds even further. Moreover, it is conceivable that our technique might find other applications. For example, it might be useful in the [GGL-91] setting. Another open problem is based on the fact that our constructive protocol, while achieving a constant value of β, only works for β small enough. Thus, the question whether one can constructively achieve optimal value of β is still open for faster (i.e. sub-linear) protocols.

Acknowledgements

We thank Nati Linial for a helpful discussion, Ravi Boppana and Babu Narayanan, for providing us with a manuscript of their paper and Nabil Kahale, for telling us about his recent work on random walks on expander graphs.

References

[AL-89] M. Ajtai, N. Linial The influence of large coalitions. *IBM Research Report 7133* (67380), Nov. 1989.

[AN-90] N. Alon, M. Naor Coin-flipping games immune against linear-sized coalitions. *FOCS-90* pp. 46-54. Journal version in *SIAM Journal on Computing* 22:403-417, 1993.

[AR-89] N. Alon, M. Rabin Biased coins and randomized algorithms. *Advances in Computing Research, JAI Press* (Silvio Micali, ed.) 5:499-507,1989.

[BGW-88] Ben-Or M., S. Goldwasser, A. Wigderson Completeness Theorem for Non-cryptographic Fault-tolerant Distributed Computing, STOC 88, pp. 1-10

[BL-85] M. Ben-Or, N. Linial Collective coin flipping, robust voting schemes and minima of Banzhaf values. *FOCS-85* pp. 408-416.

[BL-89] M. Ben-Or, N. Linial Collective coin flipping. *Advances in Computing Research, JAI Press* (Silvio Micali, ed.) 5:91-116,1989.

[BLS-87] M. Ben-Or, N. Linial, M. Saks Collective coin flipping and other models of imperfect randomness. *Colloq. Math. Soc. Janós Bolyai No., 52 Combinatorics Eger* pp. 75-112, 1987. North-Holland Publ.

[BN1-93] R. Boppana, B. Narayanan. The biased coin problem *STOC 93*

[BN2-93] R. Boppana, B. Narayanan. Collective Coin Flipping and Leader Election with Optimal Immunity., *manuscript.*

[B-85] G. Bracha An $O(\log n)$ expected rounds randomized Byzantine Generals protocol. *STOC-85* pp. 316-326.

[CCD-88] D. Chaum, C. Crepeau and I. Damgard Multiparty Unconditionally Secure Protocols. *STOC 88*, pp. 11-19.

[CD-89] B. Chor, C. Dwork Randomization in Byzantine agreement. *Advances in Computing Research, JAI Press* (Silvio Micali, ed.) Vol. 5, 1989.

[CL-93] J. Cooper, N. Linial Fast Perfect-Information Leader-Election Protocol with Linear Immunity. *STOC-93* pp. 662-671.

[FM-88] P. Feldman, S. Micali Optimal algorithms for Byzantine Agreement. *STOC-88* pp. 148-161.

[GG-79] O. Gabber, Z. Galil Explicit construction of linear sized super-concentrators. *FOCS-20* pp. 364,370. Also see the journal version,*JCSS***22** (1981), pp. 407-420.

[G-93] D. Gillman A Chernoff bound for random walks on expanders. *FOCS-93.*

[GGL-91] O. Goldreich, S. Goldwasser, N. Linial Fault-tolerant Computation in the Full Information Model. *FOCS 91* pp. 447-457.

[IZ-89] R. Impagliazzo, D. Zuckerman How to recycle random bits. *FOCS 89* pp. 248-253.

[KKL-88] J. Kahn, G. Kalai, N. Linial The influence of variables on boolean functions. *FOCS 88*, pp. 68-80.

[K-94] N. Kahale. Private Communication, February 1994.

[GMW-87] O. Goldreich, S. Micali, A. Wigderson How to Play any Mental Game. *STOC 87*, pp. 218-229.

[L-92] N. Linial Games Computers Play: Game-Theoretic Aspects of Computing *C.S. Tech. Report 92-5, The Hebrew University of Jerusalem*, February 1992.

[S-89] M. Saks A robust noncryptographic protocol for collective coin flipping. *SIAM Journal of Discrete Mathematics*, 2:240-244, 1989.