Coin-flipping games immune against linear-sized coalitions (Extended abstract)

Noga Alon
IBM Almaden Research Center, San Jose, CA 95120 and
Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel
Moni Naor
IBM Almaden Research Center, San Jose, CA 95120

Abstract

Perfect information coin-flipping and leader-election games arise naturally in the study of fault tolerant distributed computing and have been considered in many different scenarios. Answering a question of Ben-Or and Linial we prove that for every $c < 1$ there are such games on n players in which no coalition of cn players can influence the outcome with probability greater than some universal constant times c. We show that a random protocol of a certain length has this property and give an explicit construction as well.

1 Introduction

A fundamental problem of fault tolerant distributed computing is that of n processors wishing to agree on a random value. The problem becomes non-trivial when some of the processors are faulty. The problem has been considered in many different scenarios, depending on the assumptions made on the type of communication between the processors, the kind and number of faults, and the power of the adversary. See the surveys of Chor and Dwork [10] and Ben-or, Linial and Saks [7]. In the present paper we consider it in the natural model formulated by Ben-Or and Linial [6] (whose formal description is given in the next subsection): the processors have complete information, (i.e. the communication type is a public broadcast channel), the processors take turns broadcasting some random values and the outcome is a function of all the bits that were sent. The adversary is assumed to be computationally unlimited. The problem is to design protocols where the influence on the outcome of any set of faulty processors not exceeding a certain size is bounded.

A closely related problem is that of leader election: the processors take turns broadcasting messages. At the end of the protocol, as a function of the bits transmitted, one processor is considered the leader. The problem is to design protocols that have the property that for any coalition of faulty processors whose size does not exceed a certain threshold, the probability that a member of the coalition be elected is bounded.

Unlike the Byzantine case, where the exact thresholds for achieving an agreement were known [10, 11], for the perfect information scenario a gap existed: it was known that $\frac{n}{2}$ cheaters (out of n players) can completely control the protocol, yet the best known protocol [13, 1] (improving the one in [6]) has the property that only sets of cheaters of size less than $\frac{n}{3 \log n}$ have influence bounded away from 1.

In this paper we resolve this problem and show that there are protocols where even a linear number of cheaters have only bounded influence. We first show in Section 2, via a *probabilistic*

construction , the existence of an election protocol that can tolerate up to $\frac{1}{3}n$ cheaters (i.e. the elected leader will not be faulty with some non-zero probability). Then, in section 3, we show an *explicit construction* that works for a smaller (yet linear in n) threshold. This easily gives coin flipping protocols with a similar behaviour.

Our proofs combine probabilistic arguments with an iterative procedure based on the pseudo-random properties of projective and affine planes. The analysis requires a study of a game which we call faulty baton passing that is performed in each iteration of the procedure.

1.1 Preliminaries, background and results

A *perfect-information coin-flipping game* of n players is a rooted tree T whose leaves are labeled by 0 or 1 and whose internal vertices are labeled by the names of the players. In addition, each internal vertex v is associated with a probability distribution D_v on its children. Starting from the root, the player whose name labels the current vertex v chooses one of its children according to the distribution D_v, and the game proceeds to the chosen child. When a leaf is reached the game ends and its value is the label of the leaf. Note that the same player may have to make more than one choice in a game. It is sometimes assumed that the tree T is binary and that the probability distribution associated with each internal vertex is the uniform distribution on its two children. This makes no essential difference, and hence we use here the more general definition.

Let N denote the set of players. We say that a player $I \in N$ plays *fairly* if he makes his choice randomly (according to the corresponding probability distribution) whenever it is his turn to make a choice in the course of the game.

Let p_1^T be the probability of reaching a leaf labeled 1 if all players play fairly. T is a *fair* game if $p_1(T) = 1/2$. For a subset S of the set of players N, let $p_1^T(S)$ denote the probability of reaching a 1-leaf when the coalition S plays the optimal strategy trying to maximize the probability of reaching a 1-value. Here we assume that all the other players play fairly and that each player in S knows exactly which other players are in S. The *influence* $I_1^T(S)$ *of* S *towards* 1 *in the game* T is defined by $I_1^T(S) = p_1^T(S) - p_1^T$. The influence $I_0^T(S)$ of S towards 0 in T is defined similarly and the *(total) influence* $I(S) = I^T(S)$ is defined by $I(s) = I_1^T(S) + I_0^T(S)$. Therefore, $I(S)$ measures the capability of S to control the game, and a game is robust if $I(S)$ is small for every relatively small S. In [6] it is proved that for every perfect-information coin-flipping game T of a set N of n players, where p_1^T is bounded away from 0 and 1, and for every $k \leq n$ there is a subset $S \subset N$ of cardinality k whose influence $I(S)$ is at least $\Omega(k/n)$. In the same paper the authors construct a fair game of n players in which the influence of each set of k players, where $k \leq O(n^{log_3 2})$ is at most $O(k/n)$. Improving the estimates of Saks in [13], Ajtai and Linial [1] showed that there is a fair game on n players in which the influence of each set of $k \leq \frac{n}{3 \log n}$ is at most $O(k/n)$. These results lead to the following problem, raised in [6], and referred to as the most outstanding problem in this area in some of the more recent papers on the subject.

Problem ([6], see also [1]) Are there fair perfect-information coin-flipping games of n players in which for every $k \leq n$ the influence of every set of k players is at most $O(k/n)$? In particular, are there such games in which there is no set of size $o(n)$ whose influence is $1 - o(1)$?

In the present paper we show that the answer to both questions is "yes". We first present

a probabilistic proof of existence of such games. Afterwards we describe, for every positive $c < 1$, an explicit construction of perfect-information coin-flipping fair games of n players in which there is no set of cn players whose influence exceeds $O(c)$.

Our results are better formulated in terms of leader-election games. A *leader-election game* of n players is a rooted tree T whose vertices are labeled by the names of the players, and each internal vertex v is associated with a probability distribution D_v on its children. Starting from the root, the player whose name labels the current vertex v chooses one of its children according to the distribution D_v, and the game proceeds to the chosen child. When a leaf is reached the game ends and the chosen leader is the label of this leaf.

For a subset S of players, let $p^T(S)$ denote the probability that a leader from S is chosen, when the coalition S plays the optimal strategy trying to maximize the probability of such a choice, (and when all other players play fairly). For a constant $\delta > 0$ and for $t \leq n$ let us call, following [13], a leader-election game T *δ-robust against t-cheaters* if $p^T(S) \leq \delta$ for any subset S of at most t players. Let $t(n, \delta)$ denote the maximum t such that there exists a leader-election game of n players which is δ-robust against t cheaters. From any leader-election game T one can construct its associated coin-flipping fair game $C(T)$ obtained by letting the chosen leader flip a coin and decide the value of the game. Thus formally, $C(T)$ is the game obtained from the tree T by adding to each leaf v of T two children labeled 0 and 1, and by associating v with the uniform distribution on these two children. It is obvious that for a subset S of players, the influence of S towards 0 or towards 1 in $C(T)$ is precisely $p^T(S)/2$. Therefore, the existence of robust leader-election games implies the existence of robust coin-flipping games. This leads naturally to the problem of estimating $t(n, \delta)$.

In [13] Saks constructed a leader election game which is δ-robust against $c(\delta)n/\log n$ cheaters, for any $0 < \delta < 1$, where $c(\delta)$ is a positive constant depending only on δ. This shows that $t(n, \delta) > c(\delta)n/\log n$. Answering a question raised in [13] we show that in fact $t(n, \delta) > \Omega(\delta n)$ for all $0 < \delta < 1$. Moreover, for any $\epsilon < 1/3$ there is a $\delta < 1$ such that $t(n, \delta) > \epsilon n$. As noted in [13] there is a simple argument that shows that $t(n, \delta) < n/2$ for all $\delta < 1$. It would be interesting to close the gap between the two constants $1/2$ and $1/3$ here.

Our best lower bounds (in terms of the constants) for $t(n, \delta)$ are obtained by probabilistic arguments, described in the next section. However, we also give an explicit construction of leader-election games of n players which are δ-robust against $\Omega(\delta n)$-cheaters.

2 The existence of robust games

Let T be a full binary rooted tree of depth d. Put $N = \{1, \ldots, n\}$, and let us label each internal vertex v of T, randomly and independently, by a number in N chosen according to a uniform distribution on N. Observe that T is a leader-election game of n players. Our first result in this section is the following theorem, which demonstrates the existence of very robust leader-election games.

Theorem 2.1 *Let T be the leader-election game chosen randomly as above. Then, the probability that there is a set $S \subset N$ of cardinality ϵn, where $\epsilon < 1/3$, such that $p^T(S)$ is at least*

$$\epsilon + \frac{\epsilon^{3/2}}{\sqrt{2}(1 - \sqrt{1/2 + 3\epsilon/2})} + \gamma$$

does not exceed

$$\binom{n}{\epsilon n}\frac{\epsilon(1/2+3\epsilon/2)^d}{\gamma^2}.$$

In particular, there is an n-player leader-election game T of depth $O(n)$ in which for any set of $\epsilon n \leq \frac{1}{4}n$ players $p^T(S) \leq \epsilon + 12\epsilon^{3/2}$.

Note that even if all players in an n-players leader-election game play fairly, then for every ϵ (which is an integral multiple of $1/n$) there is a set S of ϵn players such that the leader is chosen among the members of S with probability of at least ϵ. This shows that the last estimate for $p^T(S)$ in the theorem above is sharp, up to the additive lower order term $12\epsilon^{3/2}$.

The theorem is proved by deriving estimates on the expectation and variance of the the value of $p^T(S)$ in a randomly chosen leader election game. Then, using Chebyschev's Inequality it is shown that with the required probability there is no set S where $p^T(S)$ is larger than the bound in the theorem. A similar strategy is used in the proof of the main result of [5], but the proof here contains several additional ideas.

First we establish the following two lemmas.

Lemma 2.2 *Let Y, Z be two independent random variables with equal expectations $E(Y) = E(Z) = E$ and equal variances $Var(Y) = Var(Z) = \sigma^2$. Let $\epsilon \leq 1$ be a positive constant and let X be the random variable defined as $\frac{Y+Z}{2}$ with probability $1-\epsilon$ and $Max\{Y, Z\}$ with probability ϵ. Then:*

$$E(X) = E + \frac{\epsilon}{2}E(|Y-Z|) \leq E + \frac{\epsilon\sigma}{\sqrt{2}} \qquad (1)$$

$$Var(X) \leq \sigma^2(\frac{1}{2} + \frac{3\epsilon}{2}). \qquad (2)$$

The proof is based on the fact that $Max(Y, Z) = \frac{Y+Z}{2} + \frac{|Y-Z|}{2}$ and applies Jensen's and Cauchy-Schwartz inequalities. The details appear in the full version [4].

In order to state the next lemma we need some more notation. Let T be, as before, a full binary rooted tree of depth d, whose vertices are labeled randomly and independently by the elements of $N = \{1, \ldots, n\}$. Let $a < 1$ be a positive number and let us choose, for every leaf v of T randomly and independently, a weight $w(v)$, where $w(v) = 1$ with probability a and $w(v) = 0$ with probability $1 - a$. Let $S \subset N$ be a fixed subset of cardinality $|S| = \epsilon n$. Define a weight function $w_{a,S}$ on the vertices of T as follows. If v is a leaf of T then $w_{a,S}(v) = w(v)$. If u is an internal vertex of T and v_1, v_2 are its two children then:
$w_{a,S}(u) = Max\{w_{a,S}(v_1), w_{a,S}(v_2)\}$ if u is labeled by an element of S, and
$w_{a,S}(u) = \frac{w_{a,S}(v_1)+w_{a,S}(v_2)}{2}$ otherwise.

Obviously, for fixed S, a and for every fixed vertex v of T, $w_{a,S}(v)$ is a random variable whose value depends on the random choices of the labels of the internal vertices of T and on the random choices of the weights $w(v)$ of the leaves of T.

Lemma 2.3 *Let v be a vertex of T whose distance from the leaves is h. Then the expectation and the variance of the random variable $w_{a,S}(v)$ satisfy:*

$$E(w_{a,S}(v)) \leq a + \epsilon\frac{\sqrt{a}}{\sqrt{2}}\sum_{i=0}^{h-1}(\frac{1}{2} + \frac{3\epsilon}{2})^{i/2}$$

$$\leq a + \epsilon\frac{\sqrt{a}}{\sqrt{2}(1-\sqrt{1/2+3\epsilon/2})}$$

$$Var(w_{a,S}(v)) \leq a(\frac{1}{2} + \frac{3\epsilon}{2})^h.$$

The lemma is proved by induction on h. See the full version [4].

Returning, now, to our randomly-chosen leader-election game given by the randomly labeled tree T of depth d, let us fix a set S with $S = \epsilon n$, where

$\epsilon < 1/3$ and let us estimate the probability that for this specific set S, the inequality

$$p^T(S) > \epsilon + \frac{\epsilon^{3/2}}{\sqrt{2}(1-\sqrt{1/2+3\epsilon/2})} + \gamma$$

holds. For every vertex v, let T_v denote the subtree of T rooted at v. If the leader election game is played on T_v then the probability that a leader from S is chosen, when the coalition S plays the optimal strategy trying to maximize the probability of such a choice, is $p^{T_v}(S)$. Obviously, if v is a leaf of T, then $p^{T_v}(S)$ is 1 if the label of v is in S and is 0 otherwise. More interesting is the case that v is an internal vertex of T and u and w are its two children. It is not too difficult to check that in this case:
$p^{T_v}(S) = Max\{p^{T_u}(S), p^{T_w}(S)\}$ if v is labeled by an element of S, and
$p^{T_v}(S) = \frac{p^{T_u}(S)+p^{T_w}(S)}{2}$ otherwise.

Therefore, the random variables $p^{T_v}(s)$ are defined exactly as the random variables $w_{a,S}(v)$ discussed in Lemma 2.3, where here $a = \epsilon$. It follows that the expectations and variances of these random variables satisfy the bounds appearing in this lemma (with $a = \epsilon$). In particular, when we let v be the root of T we conclude that the expectation and the variance of $p^{T_v}(S) = p^T(S)$ satisfy

$$E(p^T(S)) \leq \epsilon + \epsilon\frac{\sqrt{\epsilon}}{\sqrt{2}}\sum_{i=0}^{d-1}(\frac{1}{2}+\frac{3\epsilon}{2})^{i/2}$$

$$\leq \epsilon + \frac{\epsilon^{3/2}}{\sqrt{2}(1-\sqrt{1/2+3\epsilon/2})},$$

and

$$Var(p^T(S)) \leq \epsilon(\frac{1}{2}+\frac{3\epsilon}{2})^d.$$

Combining this with Chebyschev's Inequality we obtain:

Lemma 2.4 *let S be a fixed set of $\epsilon n < \frac{1}{3}n$ players and let T be the leader-election game chosen randomly as above. Then, for every positive γ, the probability that*

$$p^T(S) \geq \epsilon + \frac{\epsilon^{3/2}}{\sqrt{2}(1-\sqrt{1/2+3\epsilon/2})} + \gamma$$

does not exceed

$$\frac{\epsilon(1/2+3\epsilon/2)^d}{\gamma^2}.$$

□

Proof of Theorem 2.1 By Lemma 2.4, for every fixed subset of players S of cardinality $|S| = \epsilon n < \frac{1}{3}n$, the probability that $p^T(S)$ exceeds

$$\epsilon + \frac{\epsilon^{3/2}}{\sqrt{2}(1-\sqrt{1/2+3\epsilon/2})} + \gamma$$

does not exceed

$$\frac{\epsilon(1/2+3\epsilon/2)^d}{\gamma^2}.$$

Since the number of choices for S is $\binom{n}{\epsilon n}$, the desired result follows. □

Theorem 2.1 shows that for every ϵ that satisfies

$$\epsilon + \frac{\epsilon^{3/2}}{\sqrt{2}(1-\sqrt{1/2+3\epsilon/2})} < 1$$

there is a $\delta < 1$ such that $t(n,\delta) \geq \epsilon n$; i.e., there are leader-election games on n players which are δ-robust against ϵn-cheaters. This does not suffice to prove the existence of such a δ for ϵ which is, e.g., at least 1/4. Still, one can modify the proof to show that such a δ exists for every $\epsilon < 1/3$. To do so, we need one of the simple properties of the *baton-passing game*, together with a randomized construction similar to the one given above. The somewhat complicated details are given in the full version [4].

As mentioned in the introduction, robust leader election games supply robust coin-flipping games by allowing the leader choose the random bit. Therefore, as a simple consequence of Theorem 2.1 and its improvement described in the full version [4] we obtain:

Theorem 2.5 *(i) There are fair n-players coin flipping games of depth $O(n)$ such that the influence of every set of $\epsilon n \leq \frac{1}{4}n$ players towards 0 or towards 1 is at most $\frac{1}{2}\epsilon + 6\epsilon^{3/2}$.*
(ii) For every $\epsilon < 1/3$ there are fair n-players coin flipping games such that the influence of every set of ϵn players towards 0 or towards 1 is bounded away from 1/2.

This theorem solves the problem mentioned in the introduction.

3 Explicit construction

In this section we show how to explicitly construct coin-flipping games where the influence of any set whose cardinality is smaller than some linear threshold is bounded away from 1. We use the idea put forth by Bracha [8] in the Byzantine context of forming virtual players from committees of actual players. Say that a committee is good if it has a certain ratio of good players to bad players. The advantage of an assignment to committees is that the ratio of good committees to bad committees can be much better than the ratio of good players to bad players.

Recall that baton passing is the game analyzed by Saks [13] and Ajtai and Linial [1] where a leader is chosen by passing a baton among the players. Initially the baton is held by some arbitrary player and each player that receives the baton picks a player that has not been selected so far and gives him the baton.

In our scheme, the committees formed play baton passing. When a committee gets the baton it elects a leader (recursively) and decides on the next committee to get the baton. The leader of the last committee to hold the baton is the global leader.

The advantage our game has over baton passing is that the bad players do not know in advance which committees will elect good leaders and which bad leaders. Thus, though the percentage of bad leaders is high, a bad leader does not necessarily choose a committee which elects a good leader (which is the optimal strategy in baton passing)

The committees are assigned using an affine plane: each player corresponds to a point in the plane and a committee is a line.

In the next subsection we analyze the variant of the baton passing game which is relevant to our scheme: a good player might turn bad when he receives the baton. (This corresponds to the case that a good committee elects a bad leader.) In subsection 3.2 we discuss the properties of the assignment to committees by affine planes. Finally in subsection 3.3 we analyze the resulting construction.

3.1 Faulty baton passing

In this subsection we analyze the baton passing game when even the good players have a certain probability ϵ of becoming faulty. We call this variant the faulty baton passing game.

In the regular baton passing game the best strategy for the bad participants is to select a good player to receive the baton. By the moment reflection argument of [1] (or by induction as in [13]) this is the best strategy in the faulty baton passing game as well. Thus we can assume that whenever a bad participant has the baton he selects a good participant to receive it and a good participant that becomes faulty also selects a good participant to receive the baton.

We would like to find bounds on $f(s,t) = f_\epsilon(s,t)$ the probability of the baton ending at a bad player starting from a good player when there are s (as yet unselected) good players, t (as yet unselected) bad players and a good player has probability ϵ of becoming faulty when he gets

the baton. (It is important that it not be known in advance whether a good player would become faulty when he will receive the baton.)

We assume $0 \leq \epsilon < \frac{1}{4}$.

Clearly, $f(0,t) = 1 \ \ \forall t \geq 1$ and $f(s,0) = 0 \ \ \forall s \geq 0$.

From the bad players strategy, for all $s, t \geq 1$

$$f(s,t) = \frac{s+\epsilon t}{s+t} \cdot f(s-1,t) + \frac{t-\epsilon t}{s+t} \cdot f(s-1,t-1). \tag{3}$$

Lemma 3.1 *For all $s, t \geq 0$, $0 \leq \epsilon < \frac{1}{4}$*

$$f(s,t) \leq 8 \cdot \frac{(t \log_2(t+1))^{\frac{1}{1-4\epsilon}}}{(s+1)^{1-\epsilon}} \tag{4}$$

The proof is by induction on $s+t$, which involves a technical computation and is given in the full version [4].

3.2 Amplification via affine planes

In this subsection we describe a pseudo-random property of projective planes which is applied in [2, 3] and show how affine planes have a similar property. Affine planes better fit our purposes here. The property we need can be proved by an eigenvalue argument and also more directly. We omit the details.

Lemma 3.2 *[2, 3] Let $\mathcal{P} = (P, L)$ be a projective plane of order p with a set P of $n = p^2+p+1$ points and a set L of n lines. If $A \subset P$, $|A| = \epsilon n$, then*

$$\sum_{\ell \in L} (|\ell \bigcap A| - \epsilon(p+1))^2 = \epsilon(1-\epsilon)p \cdot n$$

Corollary 3.3 *Let $\mathcal{A} = (\bar{P}, \bar{L})$ be an affine plane of order p, obtained by deleting a line from the projective plane of that order. Put $m = p^2 = |\bar{P}| = |\bar{L}|$ and recall that each $\ell \in \bar{L}$ has p points. Suppose that $A \subset \bar{P}$, $|A| = \epsilon m$ and suppose that $\delta > 0$. Then*

$$|\{\ell \in \bar{L} : |\ell \bigcap A| \geq (\epsilon + \delta) \cdot p\}|$$

$$\leq \frac{\epsilon(p^2+p+1)}{\delta^2 p} \leq \frac{\epsilon}{\delta^2}(\sqrt{m}+2)$$

Proof Let $x = \left|\{\ell \in \bar{L} : |\ell \bigcap A| \geq (\epsilon+\delta) \cdot p\}\right|$. Embed $\mathcal{A}$ in the projective plane of order p, $\mathcal{P} = (P, L)$. Observe that $\frac{|A|}{p^2+p+1} = \frac{\epsilon p^2}{p^2+p+1}$ and hence $\frac{|A|}{p^2+p+1}(p+1) = \frac{\epsilon p^2(p+1)}{p^2+p+1} \leq \epsilon p$. By Lemma 3.2

$$\sum_{\ell \in \bar{L}} (|\ell \bigcap A| - \frac{|A|}{p^2+p+1}(p+1))^2 \leq \epsilon p(p^2+p+1)$$

Each line among the x defined above contributes to the left hand side at least $\delta^2 p^2$. Thus $x\delta^2 p^2 \leq \epsilon p(p^2+p+1)$ implying the desired result. □

Remark: For every $p = 2^k$ there is an affine plane of order p. Our algorithm uses the planes of order 2^{2^k}. Note that the number of points in a plane of order 2^{2^k} is equal to the number of points in one line of a plane of order $2^{2^{k+1}}$. This is used for recursive application of the algorithm.

Remark The first author has suggested previously using projective planes as a construction meeting some of the requirements of [8]. (See [10] for details.) As we shall see, unlike the Byzantine case, for our purposes it is not essential that the size of the committees be small (logarithmic in n).

Remark The construction is an instance of graphs called *dispersers* that have many other applications. (See [9] for an extensive survey of constructions and applications.) There are several other constructions of dispersers that can be used for our purposes.

3.3 The construction

We are now ready to present the construction in detail. We can assume without loss of generality that n is of the form 2^{2^j}: otherwise let $n' = 2^{2^{\lceil \log \log n \rceil}}$ and make each of the n participants play the role of $\lfloor \frac{n'}{n} \rfloor$ or $\lceil \frac{n'}{n} \rceil$ in a game of n' participants. The ratio of bad players has not increased by more than $\frac{1}{n}$.

The scheme is as follows: form committees by treating each player a as a point $a \in \bar{P}$ in the affine plane $\mathcal{A} = (\bar{P}, \bar{L})$ of order $2^{2^{j-1}}$. Each committee ℓ corresponds to a line $\ell \in \bar{L}$, i.e. a player a is in committee ℓ iff $a \in \ell$.

- Set $m \leftarrow$ threshold
- If $n \leq m$ than choose leader by baton passing. Otherwise:
  1. Construct committees via affine planes.
  2. $\ell \leftarrow$ first committee
  3. Repeat
     (a) Let ℓ choose a leader recursively.
     (b) Let the leader of ℓ choose a committee ℓ' as yet unselected.
     (c) $\ell \leftarrow \ell'$

     Until there are no unselected committees.
  4. The leader of the last chosen committee ℓ is crowned as the leader of all players.

The value of threshold is a function of ϵ. We let it be the smallest number of the form 2^{2^r}, where r is an integer, such that $2^{2^r} \geq (\frac{1}{\epsilon})^{100}$. (Note that for this choice $(\frac{1}{\epsilon})^{100} \leq m \leq (\frac{1}{\epsilon})^{200}$.)

Observe that the total amount of work done by each player is polynomial in n, since at each stage of the recursion every two players are together in exactly one committee.

The next theorem implies that no set smaller than some linear threshold can control the leadership, and hence shows that our construction gives a leader election game which is immune against linear sized coalitions.

Theorem 3.4 *There exists a positive constant c such that for every positive $\epsilon < 1$ the protocol specified above with an appropriately chosen threshold (as a function of ϵ) is $c\epsilon$ robust against ϵn cheaters.*

The theorem is established by proving two lemmas that combine the pseudo-random properties of affine planes described in Corollary 3.3 with the analysis of faulty baton passing summarized in Lemma 3.1. Due to space limitations we omit the details, which appear, together with some related remarks in the full version [4].

References

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

[2] N. Alon, *Eigenvalues, geometric expanders, sorting in rounds, and Ramsey Theory*, Combinatorica 6(1986), pp. 207-219.

[3] N. Alon and Z. Füredi, *Legitimate colorings of projective planes*, Graphs and Combinatorics 5(1989), 95-106.

[4] N. Alon and M. Naor, *Coin-flipping games immune against linear-sized coalitions*, IBM Research Report, RJ 7491, May 1990.

[5] N. Alon and M. O. Rabin, *Biased coins and randomized algorithms*, in "Advance in Computing Research" (Silvio Micali, ed.), Vol. 5 (1989), JAI Press, pp. 499-507.

[6] M. Ben-Or and N. Linial, *Collective coin flipping, robust voting schemes and minima of Banzhaf values*, Proc. 26^{th} FOCS, IEEE(1985), 408-416.

[7] M. Ben-Or, N. Linial and M. Saks, *Collective coin flipping and other models of imperfect information*, Coll. Math. Soc. János Bolyai 52 (1987), 75-112.

[8] G. Bracha, *An $O(\log n)$ expected rounds randomized Byzantine generals protocol*, Journal of the ACM, 34(1987), pp. 910-920.

[9] A. Cohen and A. Wigderson, *Multigraph amplification*, submitted to Random Structures and Algorithms.

[10] B. Chor and C. Dwork, *Randomization in Byzantine Agreement*, in "Advance in Computing Research" (Silvio Micali, ed.), Vol. 5 (1989), JAI Press.

[11] R. L. Graham, A. C. Yao, *On the improbability of reaching Byazantine agreements*, Proc. of the 21st annual ACM Symposium on Theory of Computing, Seattle, 1989, pp. 467-478.

[12] J. Kahn, G. Kalai and N. Linial, *The influence of variables on boolean functions*, Proc. 29^{th} FOCS, IEEE(1988), 68-80.

[13] M. Saks, *A robust non-cryptographic protocol for collective coin flipping*, SIAM J. Discrete Math. 2(1989), 240-244.

[14] U. V. Vazirani and V. V. Vazirani, *Random polynomial time is equal to slightly random polynomial time*, Proc. 26^{th} FOCS, Portland, Oregon (1985), 417-428.