COLLECTIVE COIN FLIPPING, ROBUST VOTING SCHEMES AND MINIMA OF BANZHAF VALUES

(Preliminary Report)

Michael Ben-Or and Nathan Linial

Institue of Mathematics and Computer Science
Hebrew University, Givat Ram
Jerusalem, Israel

ABSTRACT

The power of players in a collective decision process is a central issue in Mathematical Economics and Game Theory. Similar issues arise in Computer Science in the study of distributed, fault tolerant computations when several processes, some perhaps faulty, have to reach agreement.

In the present article we study voting schemes which are relatively immune to the presence of unfair players. In particular, we discuss how to perform collective coin flipping which is only slightly biased despite the presence of unfair players. Mathematically this corresponds to problems concerning the minima of Banzhaf values in certain n -person games. These are measures of power studied in Game Theory. It is quite remarkable that while dictatorial voting games are, of course, the most sensitive to the presence of unfair players, some voting schemes that we propose here are significantly more robust than majority voting.

Coin flipping was selected as a study case because of its simplicity and because collective coin flipping is widely used in randomized algorithms for distributed computations. It is our feeling that Game Theory has much to contribute to Computer Science and we are sure that further applications will be found.

1. Introduction

We study the following problem:

Consider an n -person game which proceeds according to the outcome of coin flips. It is assumed that every player has an unbiased coin and so the simplest procedure for flipping the coin is that one of the players flips his coin and announces the outcome. If not all players play the game fairly this simple procedure could be dangerous - that player may announce outcomes according to his interest in the game and not by flipping the coin. We need, then, a procedure for collective decision making or a voting scheme which is more robust, so that the collective coin is as unbiased as possible.

This problem turns out to be a natural problem in Game Theory which is related to the so called **Banzhaf-Coleman** value [Ow]. This is an index of power which in game theory is secondary in importance to the classical Shapley value. In these terms our problem can be stated formally as a quest for the least (in the l_∞ norm) Banzhaf value for a certain class of games.

A similar problem arises in the study of the Byzantine Generals problem. All the known probabilistic Byzantine General protocols try to generate a "global coin flip" that is later used to bring about decision. If the faulty processes cannot completely control the coin, we can use this "global coin" to construct fast Byzantine Agreement protocols [Be, Ra, CC, Br, CMS]. We are thus looking here too for a robust coin flipping procedure so that the outcome is as unbiased as possible.

The procedure by which one player flips the coin for all is a dictatorial voting scheme. This being the most sensitive to the presence of an unfair player it was only natural to conjecture that majority voting is the most robust voting scheme. Rather surprisingly, this is not the case. The normalized influence (normalized Banzhaf value) of an unfair player in the dictatorial voting

0272-5428/85/0000/0408$01.00 © 1985 IEEE

scheme is 1, while in the majority voting scheme it is $O(1/\sqrt{n})$, where n is the number of players. We present a voting scheme that reduces this influence to $O(\log n/n)$.

We also investigate the same question under the following natural symmetry condition: If every player changes his vote than the overall decision must also change. In this case we have a construction based on the Fano projective plane in which the influence of every player is $O(n^{-0.65..})$.

Two further aspects are dealt with in this report:

(1) What happens in multistage games? In this case there is always a player whose influence is $\Omega(1/n)$ and we describe a voting scheme where no player can influence the outcome by more than $O(1/n)$.

(2) What happens if there is a larger number of unfair players. Here our knowledge is more fragmentary. We consider in particular the issue of ε -control of a game: What is the least number of unfair players which can determine the outcome of the game in a positive fraction of the situations. We would like to make this number as large as possible to achieve robustness. Here again, quite surprisingly, the majority voting scheme is not optimal. We present voting schemes with n players which take $\varepsilon \cdot n^{0.63..}$ players to ε -control the game. This is better than the $O(\varepsilon n^{1/2})$ unfair players that could ε -control the majority scheme.

Combining these two problems we ask

(3) What are the bounds on the influence of a set of unfair players in multistage games. A lower bound that we have is that there is always a set of k players who, if playing unfairly, can bias the outcome by at least $\Omega(k/n)$. We can show that this bound is tight for $k < n^{0.63..}$.

Recently several Byzantine Coin flipping protocols have been proposed by Dolev and Broder [BD], Yao [Y], Awerbuch et. al. [ACGM], Broder [BR], Ben-Or [BE], and others. These, rather complicated solutions assume, using cryptography or other assumptions, that the unfair players must act without having complete knowledge of the actions taken by other players. Such assumptions may not be necessary if our goal is only to prevent the faulty processes (or unfair players) from ε -controlling the coin. In this work we thus always assume that the unfair players act having complete knowledge of the actions taken by the other players.

2. Definitions and Basic Notions

A ***game***, as commonly defined in game theory [Ow], is a pair (N,v) where N is the set of players and v is a real function defined on all subsets of N (or ***coalitions*** in game theory). Unless otherwise stated our set of players is $[n] = \{1,..., n\}$. The meaning of the function $v(S)$ is the gain of S if it plays against the rest of the players. The game is called ***monotone*** if $A \subseteq B \subseteq N$ implies $v(A) \leq v(B)$. The game is ***simple*** if v takes only 0,1 values. (In this case $v(S) = 1$ is interpreted in that S is a winning coalition.)

A simple game will also be called a ***one round voting scheme.*** The interpretation is that every player can vote either 0 or 1 , and if S is the set of players voting 1 then $v(S)$ is the outcome of the poll, or the collective decision.

A ***Multistage game,*** or voting scheme, (N,T) with a set of players N is defined by a binary tree T where leaves are labeled 0 or 1 and internal nodes by elements of N . Starting from the root, the player that labels the current node makes his vote, either 0 or 1 . Accordingly, the game proceeds either to left or the right son, and so on. The label at the leaf at which the process ends is the outcome of the game.

In the games considered here a player can be ***fair*** or ***unfair***. A fair player always votes 0 or 1 based on the outcome of an unbiased coin. An unfair player may produce his vote in any way.

For a game G and a set of players T define $p_G^1(T)$ to be the largest probability that the outcome of G is 1, if the players of T play their best strategy to make the outcome 1 and the rest of the players play fairly. The quantity $p_G^0(T)$ is defined similarly. Note that $p_G^1 = p_G^1(\emptyset)$ and $p_G^0 = p_G^0(\emptyset)$ are the probabilities for the game G to end with 1 or 0 if all players play fairly. Usually it will be assumed that $p_G^1 = p_G^0 = \frac{1}{2}$. Thus the quantities

$$I_G^1(T) = p_G^1(T) - p_G^1$$

and

$$I_G^0(T) = p_G^0(T) - p_G^0$$

measure the amount of influence the coalition T has on the game T. We also set

$$I_G(T) = \max(I_G^1(T), I_G^0(T)).$$

For a one round game $G = (N,v)$ and $T = \{i\}$, a singleton, it is easily verified that

$$I_G(\{i\}) = I_G^0(\{i\}) = I_G^1(\{i\}) = \psi_i =$$

$$= \Sigma\, |\, v(S) - v(S \setminus i)\, | \cdot 2^{-n+1}.$$

This quantity has been studied in Game Theory under the name of Banzhaf Coleman index of the game. It is also worthwhile mentioning that essentially the same quantity was also studied in Threshold Logic [Wi] and in Information Theory [Mc].

One goal of this paper is to find games for which $I_G^1(T)$ and $I_G^0(T)$ are as small as possible for all sets T of cardinality bounded from above.

For $1 \le r \le n$ we denote

$$I_G(r) = \max\{I_G(T)\,|\,|T| = r\}$$

and $I_G(1)$ is denoted by I_G.

For a fixed $\varepsilon > 0$ we say that a set of players S ***ε-controls*** a game if

$$I_G(S) > \varepsilon.$$

This notion captures the idea that a set of players actually determines the outcome of the game in a positive fraction of the situations. Clearly, our goal is to find games for which the least number of players who ε -control the game is as large as possible.

Finally we recall some common definitions: In a ***Hypergraph*** $H = (V,E)$ V is a set of ***vertices***, and E is a collection of nonempty subsets of V called ***edges***. H is an ***ideal*** (a ***filter***) if $A \in E$ and $B \subseteq A$ ($A \subseteq B$) imply that $B \in E$.

Note that if $G = (N,v)$ is a simple monotone game, then $J_G = \{S \subseteq N \,|\, v(S) = 0\}$ is an ideal and $F_G = \{S \subseteq N \,|\, v(S) = 1\}$ is a filter. In this case the following lemma gives an alternative definition to the influence of single players.

Lemma 2.1: Let $G = (N,v)$ be a simple monotone game, $J = J_G$ its corresponding ideal, then for any $x \in N$

$$I_G(\{x\}) = (\,|J| - 2d(x)\,)2^{-n+1}$$

where $d(x) = |\{S \in J \,|\, x \in S\}|$.

Proof: For every $x \in N$

$$I_G(\{x\}) = 2^{-n+1} \Sigma\, |\, v(S) - v(S \setminus x)\, |.$$

But since v is monotone, the sum counts the number of sets S with $v(S) = 1$ and $v(S \setminus x) = 0$. This is the number of sets $A \in J$ with $A \cup x \in F$. Therefore

$$\begin{aligned} &I_G(\{x\}) = \\ &= 2^{-n+1}(\,|\{A \in J : x \notin A\}| - |\{A \in J : x \in A\}|\,) = \\ &= 2^{-n+1}(\,|J| - 2\,|\{A \in J : x \in A\}|\,) \\ &= 2^{-n+1}(\,|J| - 2d(x)). \quad \square \end{aligned}$$

We conclude this section by noting that in order to minimize the influence of players in one round voting schemes it is enough to consider monotone games. This follows immediately from

Lemma 2.2: Let $G = (N,v)$ be a one round voting scheme, there is a voting scheme $G' = (N,w)$ such that w is monotone, $|J_G| = |J_{G'}|$ and for every $i \in N$,

$$I_G(i) \ge I_{G'}(i).$$

Proof: During this proof $x \vee y$ and $x \wedge y$ denote the maximum and minimum of $x,y \in \mathbb{R}$. Select $i \in N$ and define, for $i \notin S$

$$\begin{aligned} w(S) &= v(S) \wedge v(S \cup i), \\ w(S \cup i) &= v(S) \vee v(S \cup i). \end{aligned}$$

We show that for every $j \in N$

$$\Sigma\, |\, w(S \cup j) - w(S)\, | \le \Sigma\, |\, v(S \cup j) - v(S)\, |.$$

For $j = i$ this is clear. For $j \neq i$ we show that if $i,j \notin S$,

$$|\, w(S \cup \{i,j\}) - w(S \cup i)\, | + |\, w(S \cup j) - w(S)\, | \le$$

$$\le |\, v(S \cup \{i,j\}) - v(S \cup i)\, | + |\, v(S \cup j) - v(S)\, |.$$

Denote $v(S) = \alpha$, $v(S \cup i) = \beta$, $v(S \cup j) = \gamma$, and $v(S \cup \{i,j\}) = \delta$. Then we want to show

$$|\gamma \vee \delta - \alpha \vee \beta| + |\gamma \wedge \delta - \alpha \wedge \beta| \le |\delta - \beta| + |\gamma - \alpha|,$$

where $\alpha, \beta, \gamma, \delta \in \{0,1\}$. This is easily verified. $\square$

3. One Round Games

In this section we present a one round voting scheme among n players that reduces the influence of any particular player to $O(\frac{\log n}{n})$.

Theorem 3: There are voting schemes $G = G_n$ where

$$I_G \le \frac{\log n}{n}(1 + O(1))$$

Proof: To describe the idea of this construction let us ignore for a while issues of integrality and divisibility. For given n let b be the (unique) solution of the equation

$$(2^b - 1)^{1/b} = 2^{1-1/n}.$$

We will later show that this b satisfies

$$b = \log n - \log \log n + O(1).$$

Now decompose $[n]$ with n/b blocks of size b and consider the ideal J of those subsets of $[n]$ which contain no block.

$$|J| = (2^b - 1)^{n/b} = 2^{n-1}.$$

So we consider the voting scheme where $v(A) = 0$ if $A \in J$ and $v(A) = 1$ if $A \notin J$. Stated simply the overall decision is one if and only if a whole block unanimously votes one and is zero otherwise. Now let us compute the influence of an individual player. Using Lemma 2.1 we have to find $d(x)$ which is the same for every $x \in [n]$. It is according to the definition of J

$$d(x) = (2^{b-1} - 1)(2^b - 1)^{\frac{n}{b}-1} = \\ = \frac{2^{b-1}-1}{2^b-1}(2^b-1)^{n/b} = \frac{2^{b-1}}{2^b-1}|J|.$$

Hence

$$I_G(\{x\}) = I_G = (|J| - 2d(x)) \cdot 2^{-n+1} = \\ = 1 - \frac{2^b-2}{2^b-1} = \frac{1}{2^b-1} = O(\frac{\log n}{n}).$$

To show the last equality go back to the relation between b,n:

$$(2^b-1)^{1/b} = 2^{1-1/n}$$

or $n = -b/\log(1 - (\frac{1}{2})^b)$. We use

$$-\ln 2 \cdot (\frac{1}{2})^b \geq \log(1 - (\frac{1}{2})^b) \geq -(\frac{1}{2})^{b-1}$$

whence $b \cdot 2^b \cdot \log e \geq n \geq b \cdot 2^{b-1}$. These functions of b are increasing and therefore by evaluating them at the appropriate values of b the following bounds on b results

$$|b - (\log n - \log \log n)| < 2$$

It follows that

$$I_G = (2^b - 1)^{-1} = O(\frac{\log n}{n}).$$

To overcome the difficulties involved with b not being an integer we do as follows: We select any integer b and define the real α for which

$$(2^b - 1)^{\alpha} = 2^{\alpha b - 1}.$$

Next we define a to be the integer nearest to $\alpha, a = \alpha + \varepsilon$, $|\varepsilon| \leq \frac{1}{2}$, and set $n = ab$. J is defined as before and has size

$$|J| = (2^b - 1)^a = (2^b - 1)^{\alpha+\varepsilon} = 2^{\alpha b - 1} - (2^b - 1)^{\varepsilon}.$$

While $2^{n-1} = 2^{(\alpha+\varepsilon)b-1}$. So

$$\frac{|J|}{2^{n-1}} = (\frac{2^b-1}{2^b})^{\varepsilon} = 1 - \frac{\varepsilon}{2^b} + O(\frac{\varepsilon^2}{4^b}).$$

Therefore, by adding $2^{n-b-1} \cdot \varepsilon$ sets to J, still maintaining J's being an ideal the influence of every player can rise to at most $(1 + \varepsilon)/2^b = O(\frac{\log n}{n})$. □

4. *Symmetric Games*

The following symmetry condition is commonly imposed in the context of human voting games: If every player reverses his vote the collective decision has to change as well. If our voting scheme is described by a simple game the condition is that for every subset of players $S \subseteq N$

$$v(S) + v(N - S) = 1$$

It also turn out that robust symmetric games are useful building blocks for robust voting schemes that are not necessarily symmetric.

We would like to consider our general problem in the context of symmetric voting games:

1. Find symmetric game which minimize $I_G(r)$. Notice that the symmetry condition implies that for all $T \subseteq N$, $I_G^1(T) = I_G^0(T)$.
2. Find such games for which the least number of players which ε -control the game is as large as possible.

we have the following result for the symmetric case:

Theorem 4: (a) There exist symmetric games $G_n = G$ for which the influence function satisfies

$$I_G(r) \leq \frac{r}{2n^{\alpha}} \quad \text{for} \quad 0 \leq r \leq n^{\alpha}$$

where $\alpha = \log_3 2 \approx 0.6309...$.

(b) There exist symmetric games $G_n = G$ for which the individual influence function satisfies

$$I_G \leq \frac{1}{n^\beta}$$

where $\beta = \log_7(32/9) \approx 0.6518...$.

Proof: There are two preliminaries we have to make, the first of which is the notion of the ***composition of games***: Let $G = ([n],v)$ and $G_i = (P_i, w_i)$ be simple games, $(i = 1,...,n)$, where the sets of players P_i are mutually disjoint. The G -composition of $\{G_i\}$ is the game

$$G = (\overset{n}{\underset{1}{\cup}} P_i, w)$$

where

$$w(S) = 1 \quad iff \quad v(\{i \mid w_i(S \cap P_i) = 1\}) = 1.$$

Intuitively this means that the set of players is composed of n committees where the internal voting in the i -th committee is by the w_i rule, and the committee prime s votes are combined by v.

the second notion concerns hypergraphs. A hypergraph H is ***intersecting*** if any two edges have a nonempty intersection. H is ***two-colorable*** if there is a partition of the vertices $V = V_1 \dot{\cup} V_2$ such that no edge is contained in either V_1 or V_2 . It is called t ***-uniform*** if all edges have cardinality t .

Proposition:

(a) Let $H = (V,E)$ be an intersecting, non 2 -colorable hypergraph, then the voting scheme $G = (V,v)$ given by

$v(S) = 1$ *iff* there is an $A \in E$ such that $S \supseteq A$,

is symmetric.

(b) If H is also t-uniform and there is a transitive group acting on V under which H is invariant, then

$$I_G \leq \frac{t}{n}.$$

(c) If $G = ([n],v)$ is a symmetric voting scheme and so are $G_1,...,G_n$ then the G composition of $\{G_i\}$ is also symmetric.

Proof: (a) and (c) are simple and their proofs are omitted.

(b) By transitivity it is enough to consider the average influence of a player. By dualizing lemma 1 we obtain:

$$I_G(\{i\}) = 2^{2-n} \cdot \bar{d}(i) - 1$$

where $\bar{d}(i)$ is the number of sets containing i and an edge form E. we have

$$I_G = \frac{2^{2-n}}{n} \sum \bar{d}(i) - 1 = \frac{2^{2-n}}{n} \sum |S| - 1$$

where the sum is taken over all $S \subseteq V$ which contain an edge from E . Denote by f_j the number of such sets S with $|S| = j$. Then $\Sigma f_j = 2^{n-1}$ and

$$I_G = \frac{2^{2-n}}{n} \sum_{j \geq t} j f_j - 1.$$

Denote by $g_j = \binom{n-t}{j-t}$ the number of j-sets which contain a given t-set. We shall show that

$$(1) \qquad \frac{\sum j f_j}{\sum f_j} \leq \frac{\sum j g_j}{\sum g_j} = \frac{n+t}{2}$$

Consequently $I_G \leq \frac{t}{n}$.

To prove (1) it is enough to show that for $i \geq t$, $g_{i+1}/g_i \geq f_{i+1}/f_i$ and since $g_{i+1}/g_i = (n-i)/(i-t+1)$ we want to show

$$(2) \qquad (n-i)f_i \geq (i-t+1)f_{i+1}.$$

The l.h.s. is the number of pairs (S,x) where $|S| = i$, S contains an edge in E and x is a vertex in $V - S$. Fix a numbering E_ν, $(\nu = 1,..., |E|)$ of the edges of H. The r.h.s. counts the number of pairs (T,y) where $|T| = i + 1$, T contains an edge of H, $y \in T$, such that if E_ν is the edge of lowest index such that $T \supseteq E_\nu$ then $y \notin E_\nu$. With (T,y) associate the pair $(T \setminus y, y)$. This is a 1:1 correspondence from the objects counted in the r.h.s. to these counted in the l.h.s. .□

Before we proceed let us point that a method for constructing robust symmetric voting schemes will follow if we can produce classes of hypergraphs with the properties as in (b) with t small with respect to n. Unfortunately our methods for finding such hypergraphs are still quite limited. Some examples are:

(1) Let $n = 2t - 1$ and consider the hypergraph of all t-sets of $[n]$ - It clearly satisfies (b).

(2) The hypergraph of lines in the Fano plane. It has 7 vertices and it is 3 -uniform. The edges are {(1,2,4), (2,3,5), (3,4,6), (4,5,7), (1,5,6), (2,6,7), (1,3,7)}. It is intersecting because every two lines in a projective plane intersect. The other properties in (b) are most easily derived directly.

(3) If $G = ([n],v)$ and $G_1 = \ldots = G_n$ are voting schemes as above then the G-composition of the G_i's satisfies (b) as well.

Using these three tools we can now prove our theorem.

Part (a): Let H_1 be the majority game of 3 players. Define H_k recursively as the H_1 composition of three copies of H_{k-1}. Denote by $n = 3^k$ the number of players in H_k and let $I(n,r) = I_{H_k}(r)$ be the largest influence that r unfair players can have in H_k. Clearly n^α unfair players control H_k so only $r < n^\alpha$ is of interest. We prove by induction on n that

$$I(n,r) \leq \frac{r}{2n^\alpha}.$$

This is true for n=3 as can easily be verified.

To proceed we consider the r unfair players and how they are split among the three H_{k-1} component of H_k. Say there are r_i unfair players in the i-th component $i = 1,2,3$. We are allowed to assume that for all i

$$0 \leq r_i \leq (\frac{n}{3})^\alpha = \frac{1}{2}n^\alpha,$$

since $(\frac{n}{3})^\alpha$ unfair players can have complete control over H_{k-1}. The condition $\Sigma r_i = r$ must clearly hold, too.

The best strategy for the unfair players in order to achieve an outcome of 1 in the game is for the r_i unfair players in the i-th component to play towards 1 in their component.

The probability for the game to end with a 1 under such strategy is the probability that at least two of the components end with 1. The probability is, therefore,

$$(\tfrac{1}{2} + I(n/3, r_1))(\tfrac{1}{2} + I(n/3, r_2))(\tfrac{1}{2} + I(n/3, r_3)) +$$

$$(\tfrac{1}{2} + I(n/3, r_1))(\tfrac{1}{2} + I(n/3, r_2))(\tfrac{1}{2} - I(n/3, r_3)) +$$

$$(\tfrac{1}{2} + I(n/3, r_1))(\tfrac{1}{2} - I(n/3, r_2))(\tfrac{1}{2} + I(n/3, r_3)) +$$

$$(\tfrac{1}{2} - I(n/3, r_1))(\tfrac{1}{2} + I(n/3, r_2))(\tfrac{1}{2} + I(n/3, r_3)) +$$

$$= \frac{1}{2} + \frac{1}{2}\Sigma I(n/3, r_i) - 2\,\Pi I(n/3, r_i) \leq$$

$$\leq \frac{1}{2} + \frac{1}{2}\Sigma I(n/3, r_i).$$

Therefore

$$I(n,r) \leq \frac{1}{2}\max \Sigma I(n/3, r_i)$$

where the maximum is over all choices of r_1, r_2, r_3 with $0 \leq r_i \leq (\frac{n}{3})^\alpha = \frac{1}{2}n^\alpha$, $\Sigma r_i = r$.

By induction

$$I(n/3, r_i) \leq \frac{r_i}{2(n/3)^\alpha} = \frac{r_i}{n^\alpha}$$

and so

$$I(n,r) \leq \frac{1}{2}\Sigma\frac{r_i}{n^\alpha} = \frac{r}{2n^\alpha}$$

as claimed. The conclusion about ε-control follows by solving $I(n,r) \geq \varepsilon$ for r.

Part (b): The construction here is similar to the construction above with the building block being the Fano game rather than the majority of three game. Details are omitted.

To deal with values of n which are not powers of 3 or 7 one can modify the above mentioned games slightly and still achieve the same asymptotic bounds. □

5. *Multistage Games*

In this section we consider multistage games as defined in section 2. It can be shown, (details omitted) that no gain in generality is achieved by letting the decision at each node depend on a general one round game.

Unlike the one stage games, or voting schemes, that were studied in Game Theory and in the early days of Computer Science (i.e. Threshold Functions [Wi]), the power of players in these games, to the best of our knowledge, have not been studied before. In particular, the following important question has not been answered before:

Can we approximate an unbiased coin as good as we wish by a long enough game, or using our notation, given n and $\varepsilon > 0$, is there an n players game G with $p(G) = 1/2$, such that for all $i \geq 1$, $p_G(\{i\}) < 1/2 + \varepsilon$.

In the following theorem we answer this question negatively, by showing that in any n players game, for any k, $1 \leq k \leq n$, there is always a set S of k players that can bias the coin by at least $O(k/n)$. We wonder whether this natural result follows easily from some more general principle.

Theorem 5: Let $G = (N,T)$ be an n players game with $p = p(G)$. For any k, $1 \le k \le n$ there is a set S of k players such that

$$p_G(S) > p\cdot(1 + c(p)\frac{k}{n})$$

where $c(1/2) = \log_e 2 \approx 0.6931...$.

Proof: In this report we give a the proof for the case $k = 1$. The general case is treated in a similar way.

For a node in the game tree we consider the game of the subtree below it. We denote $p_G^1(\{i\})$ by a_i - the largest probability that this game ends with a 1 under i's best strategy and $a = p_G^1$ is this probability under fair play of all players. We prove

Lemma 5.1: For every node in a game tree

$$a_1...a_n \ge a^{n-1}.$$

Proof: We prove this by induction on the height in the tree. In a leaf all a_i and a are either zero or one. Let u be the father of v and w and say wlog that u is controlled by player 1. We use b_i, c_i to denote the appropriate quantities at v, w. We have

$$b_1...b_n \ge b^{n-1},$$

$$c_1...c_n \ge c^{n-1}.$$

$$a_1 = \max(b_1, c_1), \quad \text{say} \quad a_1 = b_1.$$

$$a_i = \frac{1}{2}(b_i + c_i) \quad n \ge i \ge 2$$

$$a = \frac{1}{2}(b + c).$$

We wish to show

$$a_1...a_n \ge a^{n-1}.$$

That is

$$b_1(\frac{b_2 + c_2}{2})...(\frac{b_n + c_n}{2}) \ge (\frac{b + c}{2})^{n-1}$$

or

$$b_1(b_2 + c_2)...(b_n + c_n) \ge (b + c)^{n-1}.$$

Expand the product $\prod_{i=2}^{n}(b_i + c_i)$ and consider the $\binom{n-1}{t}$ terms with t b's and $(n - t - 1)$ c's factors. This gives

$$\sum_{\substack{A\subseteq\{2..n\}\\ |A|=t}} \prod_{i\in A} b_i \cdot \prod_{j\notin A} c_j$$

By the arithmetic geometric inequality this is $\ge$

$$\binom{n-1}{t}[\prod_{\substack{A\subseteq\{2..n\}\\ |A|=t}} \prod_{i\in A} b_i \cdot \prod_{j\notin A} c_j]^{1/\binom{n-1}{t}} =$$

$$= \binom{n-1}{t}[(\prod_{i=2}^{n} b_i)^{\binom{n-1}{t-1}}(\prod_{i=2}^{n} c_i)^{\binom{n-2}{t}}]^{1/\binom{n-1}{t}} =$$

$$= \binom{n-1}{t}(\prod_{2}^{n} b_i)^{t/(n-1)}(\prod_{2}^{n} c_i)^{(n-t-1)/(n-1)}$$

So we have

$$b_1(b_2 + c_2)...(b_n + c_n) \ge$$

$$\ge b_1 \sum_{t=0}^{n-1}\binom{n-1}{t}(\prod_{2}^{n} b_i)^{t/(n-1)}(\prod_{2}^{n} c_i)^{(n-t-1)/(n-1)}$$

$$\ge \sum_{t=0}^{n-1}\binom{n-1}{t}(\prod_{1}^{n} b_i)^{t/(n-1)}(\prod_{1}^{n} c_i)^{(n-t-1)/(n-1)} \ge$$

$$\ge \sum_{t=0}^{n-1}\binom{n-1}{t}b^t c^{n-t-1} = (b + c)^{n-1}.$$

Where $\Pi b_i \ge b^{n-1}$ and $\Pi c_i \ge c^{n-1}$ were used. The derivation of the theorem is easy now: We conclude from the lemma that

$$\max a_i \ge a^{1-1/n} = a(1 + \frac{\log(1/a)}{n} + O(n^{-2})). \square$$

Remark: Our lower bound shows that there is always a player that can bias the coin by $O(1/n)$ toward the value 1. A similar result holds of course if we are interested in bias towards 0. We note however that this lower bound is optimal as for any p_i and p between 0 and 1 satisfying $\Pi p_i \ge p$ we can construct a game G such that $p = p_G^1$, $p_i = p_G^1(\{i\})$. (Details omitted from this report). Unfortunately in our construction any player can bias the outcome toward 0, though the bias towards 1 is bounded. In the following section we give a construction where in influence of any player (towards 0 or 1) is only $O(1/n)$.

6. Multistage games - Upper Bounds

In this section we describe how to construct multistage games such that the power of each player is bounded by $O(1/n)$.

Theorem 6.1: There are multistage games $G = G_n$ such that $p(G) = 1/2$ and the influence of any player satisfies

$$\max \{p_G^1(\{i\}), p_G^0(\{i\})\} \leq \frac{1}{2} + O(\frac{1}{n}).$$

Proof: We can describe one simple solution as 2-stage game. First each player announces his bit. We view the sequence of bits as a number between 1 and 2^n, and take its remainder modulo n. The player whose number came up flips his coin and this coin flip determines the outcome of the game. It is quite easy to verify that this construction satisfies our claim. □

Remark: Other constructions we know bring the bias down to exactly $1/n$. We omit the details of these constructions from this report.

For the case of many unfair players we have the following

Theorem 6.2: There are multistage games $G = G_n$ such that for all k, $k < n^{0.63}$, the influence of any set of players S, $|S| = k$, satisfies

$$\max \{p_G^1(S), p_G^0(S)\} \leq \frac{1}{2} + O(\frac{k}{n}).$$

Proof:(Scketch) Assume $n = 2^r$. For $k \leq n^\alpha/2r$, $\alpha = \log_3 2$, unfair players we can build a game G for which the influence of any set of k players will be at most $O(k/n)$. Let G_0 be the n-player game of theorem 4(a). Define the game G To be the following: We play the game G_0 for $r = \log n$ times and let b_i be the i-th outcome. The sequence $b = b_1, ..., b_r$ identifies one of the n players. This selected player now flips his coin again to set the outcome of the game G. Note that the only way the unfair players can bias the coin is by trying to have one of them selected to flip the final coin. As the influence of the k players on the G_0 game is bounded by $k/2n^\alpha$, the probability that one of these k players will be reached is bounded by

$$k(\frac{1}{2} + \frac{k}{2n^\alpha})^r \leq \frac{k}{n}(1 + \frac{1}{2r})^r < \frac{2k}{n}$$

Thus the probability of outcome 1 (or 0) is at most

$$\frac{2k}{n} + \frac{1}{2}(1 - \frac{2k}{n}) = \frac{1}{2} + \frac{k}{n}$$

and so the influence of any k players is bounded by $O(k/n)$. □

7. Final Remarks and Open Questions

As quite evident this study is rather preliminary and many interesting questions remain open. Let us single out first some of the questions that were mentioned along this report:

1) One unfair player one round: How small can I_G be made for one round voting schemes? We presented an n player scheme for which

$$I_G < c \cdot \frac{\log n}{n}$$

On the other hand, it can easily be shown [DS], that even the average of the Banzhaf values is at least $1/n$. We tend to conjecture that the upper bound gives the correct answer. See [F] for relevant work.

2) How many players are needed to ε control a one round game ? The best we know is $O(n^{0.63...})$ and we tend to believe that $O(n^{1-\delta})$ can be achieved for any $\delta > 0$.

3) The symmetric case: Here we have the particularly appealing problem of finding new, uniform, symmetric, intersecting and 3-chromatic hypergraphs.

4) As explained in the introduction the present study tacitly assumes that the unfair players are determined before the game starts. The unfair players are picked in the worst possible way and their identity remains unknown to the rest of the players. It is of interest to consider also the case where unfair players are determined by an adversary during the course of the game. For the one round case, it can be shown that the most robust scheme against such an adversary is the majority voting scheme. This follows from the isoperimetric inequality of Harper (see [H]). We have no similar results for multistage games.

Acknowledgement: We acknowledge useful discussions with A. Broder, N. Megiddo, A. Neyman, L. Stockmeyer and U. Vazirani.

References

[ACGM] Awerbuch B., Chor B., Goldwasser S. and Micali S., Constructive and Provably Fair Coin Flip in Byzantine Networks, Manuscript, 1984.

[Be] Ben-Or, M., Another Advantage Of Free Choice: Completely Asynchronous Byzantine Agreement, 2nd PODC, 1983.

[BE] Ben-Or, M., Fast Asynchronous Byzantine Agreement, 4th PODC, 1985.

[BD] Broder A. and Dolev D., Flipping Coins in Many Pockets, 25th FOCS, 1984.

[Br] Bracha, G., An $O(\log n)$ Expected Rounds Randomized Byzantine Generals Algorithm, 17th STOC 1985.

[BR] Broder A., A Provably Secure Polynomial Approximation Scheme for the Distributed Lottery Problem, 4th PODC, 1985.

[CC] Chor B. and Coan B., A Simple and Efficient Randomized Byzantine Agreement Algorithm, 4th IEEE Symp. on Reliability in Distributed Software and Database Systems, 1984.

[CMS] Chor B., Merritt M. and Shmoys D., Simple Constant-Time Consensus Protocols in Realistic Failure Models, 4th PODC, 1985.

[DS] Dubey, P. and Shapley, L.S., Mathematical Properties of the Banzhaf Power Index, Math. Oper. Res. 4, 1979, 99-131.

[F] Frankel, P., On The Trace of Finite Sets, Journal of Combinatorial Theory ser. A, Vol. 34, 1983, 41-45.

[H] Harper, L., Optimal Numberings and Isoperimetric Problems on Graphs, Journal of Combinatorial Theory ser. A, 1966, 385-393.

[Mc] MacWilliams, F.J. and Sloane, N.J.A., The Theory of Error-Correcting Codes, North Holland, 1977.

[Ow] Owen, G., Game Theory, 2nd Ed., Academic Press, 1982.

[Ra] Rabin, M.O., Randomized Byzantine Generals, 24th FOCS, 1983, 403-409.

[Ya] Yao, A.C., On the Succession Problem for Byzantine Generals, TR, to appear, 1984.

[Wi] Widner, R.O., Chow Parameters in Threshold Logic, JACM, Vol. 18, 1971, 265-289.