COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA 13 (2) (1993) 129–145

THE INFLUENCE OF LARGE COALITIONS

MIKLÓS AJTAI* and NATHAL LINIAL†

Received June 4, 1990
Revised June 3, 1992

This paper contains two results on influence in collective decision games. The first part deals with general perfect information coin-flipping games as defined in [3]. *Baton passing* (see [8]), an n−player game from this class is shown to have the following property: If S is a coalition of size at most $\frac{n}{3\log n}$, then the influence of S on the game is only $O\left(\frac{|S|}{n}\right)$. This complements a result from [3] that for every k there is a coalition of size k with influence $\Omega(k/n)$. Thus the best possible bounds on influences of coalitions of size up to this threshold are known, and there need not be coalitions up to this size whose influence asymptotically exceeds their fraction of the population. This result may be expected to play a role in resolving the most outstanding problem in this area: Does every n−player perfect information coin flipping game have a coalition of $o(n)$ players with influence $1-o(1)$? (Recently Alon and Naor [1] gave a negative answer to this question.) In a recent paper Kahn, Kalai and Linial [7] showed that for every n−variable boolean function of expectation bounded away from zero and one, there is a set of $\frac{n\omega(n)}{\log n}$ variables whose influence is $1-o(1)$, where $\omega(n)$ is any function tending to infinity with n. They raised the analogous question where $1-o(1)$ is replaced by any positive constant and speculated that a constant influence may be always achievable by significantly smaller sets of variables. This problem is almost completely solved in the second part of this article where we establish the existence of boolean functions where only sets of at least $\Omega\left(\frac{n}{\log^2 n}\right)$ variables can have influence bounded away from zero.

1. Introduction

This paper makes two contributions to the area of influences on collective decision procedures (see [3]). The most intriguing open problem in this area is whether in every n−player perfect information coin-flipping game (definitions will be given below) there is a coalition of $o(n)$ players whose influence on the game is $1-o(1)$. In other words, is it true that in every such game there is a negligible minority which, by deviating from random behavior can almost surely dominate the game. Consider for integers $n \geq k$ the largest number $\phi = \phi(n,k)$ such that in every n−player coin flipping game there is a coalition of k players with influence $\phi(n,k)$. A theorem of Ben-Or and Linial [3] asserts that $\phi(n,k) > c\frac{k}{n}$ for some constant

AMS subject classification code (1991): 68 R 05

* IBM Research, Almaden

† Hebrew University, Jerusalem, Israel; IBM Research, Almaden; and Stanford University. Work supported in part by grants from the Binational Science Foundation Israel-US and the Israeli Academy of Science.

c. In light of this remark we are essentially dealing with the question: Are there games in which the influence of every coalition is proportional to its fraction of the population of players? And if such games do not exist, at which coalition size does a disproportionate influence necessarily show up?

Now [3] introduced a game ("iterated majority of 3") the analysis of which shows that for $k=O(n^\alpha)$ where $\alpha=\log_3 2=0.63\ldots$ indeed $\phi(k,n)=\Theta(k/n)$. In the present paper it is shown, that the same holds for larger k and in fact $\phi(k,n)=\Theta(k/n)$ for all $k=O\left(\frac{n}{\log n}\right)$. For all that is known, this might be the largest $k=k(n)$ for which this statement holds. The proof is based on a detailed analysis of the so-called *baton passing* game (Saks [8]) whose description follows: Player P_1 is the first to hold the baton; a player receiving the baton should pass it at random to a player who had not held it yet. The last player to hold the baton is to flip a coin and this bit is the outcome of the game. Saks showed that influences in this game depend in a strong way on the relationship between the coalition size and $\frac{n}{\log n}$. In particular, coalitions of size $o\left(\frac{n}{\log n}\right)$ have influence $o(1)$, while those of size asymptotically bigger than $\frac{n}{\log n}$ have influence $1-o(1)$. In this paper the analysis is refined to show that if $k<\frac{n}{3\log n}$ then the influence of a size k coalition is only $O(k/n)$. The proof depends on a (fairly complicated) closed form formula for the probability of a coalition of a given size to win the game. An asymptotic analysis of this formula is than carried out to conclude that no disproportionate influence comes up as long as $k<\frac{n}{3\log n}$.

If indeed the answer to the above problem is positive, and small dominant coalitions always exist, this clearly resembles a result of Kahn, Kalai and Linial [7]. In that paper it is shown that in *simple* coin flipping games, or what is the same, in any boolean function a small dominant coalition (set of variables) must exist. Specifically, for any $n-$variable boolean function whose expected value is bounded away from zero and one there is a set of $\frac{n\omega(n)}{\log n}$ variables whose influence is $1-o(1)$, where $\omega(n)$ can be any function which tends to infinity with n. There is, however, a significant difference between the two situations, of simple and general games. In a simple game there always exists a player with influence $\Omega\left(\frac{\log n}{n}\right)$ that is asymptotically more than its $\frac{1}{n}$ fraction of the population of the players (this is the main theorem of [7]). More generally for $k=O\left(\frac{n}{\log n}\right)$, $k-$coalitions exist with influence $\Omega\left(\frac{k}{n}\right)$. In other words, disproportionate influence is present already for the smaller coalition size. Now if indeed $\phi(k,n)=1-o(1)$ for some $k=k(n)=o(n)$ (possibly $\frac{n}{\log n}$) then for general games a disproportion between a coalition's size and its influence occurs only for larger cardinalities, and rather suddenly (in terms of k). The explanation of this phenomenon may well differ from the one which was discovered in simple games.

If on the other hand, the answer to the question is negative, and perfect information games can be constructed with no small dominant coalitions, then it is reasonable to expect the baton passing game to be useful in such constructions, because this game exhibits the best possible behavior of restricting influences of small coalitions.

The other part of the paper concerns influences in simple games. Simple games and boolean functions are one and the same and the terminology of boolean functions is adopted. As mentioned already, Kahn, Kalai and Linial have shown for $n-$ variable boolean functions the existence of a set of $\frac{n\omega(n)}{\log n}$ variables with influence $1-o(1)$. This result is tight, except for the ω term. However, they pointed out that in all the examples known at that time, much smaller sets of variables existed whose influence was bounded away from zero. It was even speculated that a constant influence may always be achievable by sets of cardinality only n^c for some constant $c<1$. This is not the case, and indeed it is shown here that boolean functions exist where a constant influence can be achieved only by sets of at least $\Omega\left(\frac{n}{\log^2 n}\right)$ variables. Probably the best bound is closer to $\Omega\left(\frac{n}{\log n}\right)$ but the present proof does not yield that.

2. Preliminaries

All background material may be found in [3], [4], [8] and [7]. For completeness' sake we repeat the fundamental definitions. Let f be a boolean function on a set of variables X and let S be a subset of X. Consider the following statistical experiment wherein all variables not in S are assigned a value, uniformly and independently. There are three possible outcomes: either the partial assignment forces f to be zero, or one or it leaves f undetermined. Call the probabilities of these events q_0, q_1 and q_2 respectively, also let p_1 be the expectation of f i.e., the probability that $f=1$ when all variables are set at random. The *influence of S on f towards one* (zero) is defined as $I_f^1(S) := q_1 + q_2 - p_1$ (resp. $I_f^0(S) := q_0 + q_2 - (1-p_1)$.) The *influence of S on f* may be defined in two equivalent ways $I_f(S) := q_2 = I_f^0(S) + I_f^1(S)$, the equivalence of the two definitions is easy to check.

A *perfect-information coin flipping game* can be specified as follows: As before let X be a set of *players* and consider a full binary tree T whose leaves are labeled zero and one and whose internal nodes are labeled by names of members in X. The interpretation is that the game proceeds, starting at the root of T and the player whose name appears in that node is to flip a coin, according to the outcome of which the game proceed to either the left or right child of that node in T. When a leaf is reached the game is over and the outcome is the label of that leaf. What a conspiring coalition can do is to supply the right-left instructions according to an optimal coordinated strategy and not by flipping coins.

Let $p_1 = p_1(T)$ be the probability of reaching a "1" leaf when all steps are taken at random and consider the situation where coalition S plays the best strategy to maximize the probability of a 1 outcome in the game. Say that by S playing this strategy the probability of a 1 outcome increases to $p_1 + \varepsilon$. This ε is defined as $I_T^1(S)$, the influence of S towards 1 in the game T. A similar definition is made for influence towards zero and the influence of S is defined as previously by $I_T(S) := I_T^0(S) + I_T^1(S)$. As remarked in [3] this class of games is broad enough to include apparently more general coin flipping protocols, in the sense that more general perfect information coin-flipping games may be simulated by this class of games. In the simulation the influence of any coalition will not increase by more than an arbitrarily small amount, though no guarantees are made, about the length of the simulation and games with a small number of rounds may have to be simulated by much longer games.

3. A formula for baton-passing

The first analysis of this game appears in Saks [8]. Here are its rules: Player P_1 receives the baton first, a player receiving the baton should pass it at random to a player who had not held it yet. The last player to hold the baton is to flip a coin and this coin flip is the outcome of the game. Consider the game when played by $s+t$ players, of which s abide by the rules, while the complementary coalition of t, called $\mathbf{C}$ plays a best strategy to bring about a desired outcome in the game. Thus members of $\mathbf{C}$ pass the baton according to some optimal rule, rather than at random. It is quite clear that $\mathbf{C}$ succeeds only by having one of its members come out last (and announce the desired bit, rather than flip a coin). A moment's reflection shows that the best strategy for $\mathbf{C}$ is to always pass the baton out to players not in $\mathbf{C}$. Let $f(s,t)$ be the probability of winning for $\mathbf{C}$ where it is assumed that the first player to hold the baton is chosen at random. In view of the optimal strategy for $\mathbf{C}$ as described above, it is easy to see that

$$f(s,t) = \frac{s}{s+t} f(s-1,t) + \frac{t}{s+t} f(s-1,t-1)$$

with boundary conditions $f(s,1) = \frac{1}{s+1}$ for $s \geq 0$ and $f(0,t) = 1$ for all $t \geq 1$.

In order to state the results, define for $n \geq r \geq 1$ the following sums, the first of which is the harmonic series:

$$h_r(n) := \sum_{1 \leq x_1 < \ldots < x_r \leq n} \prod \frac{1}{x_i}$$

and $h_0(n) = 1$ for $n \geq 0$, for all $n < r$ set $h_r(n) = 0$.

Theorem 3.1.

$$f(s,t) = \frac{1}{\binom{s+t}{s}} \sum h_r(s) h_j(r+j) \binom{s+t-r-i-1}{s} (-1)^j \frac{(r+i)!}{(i-j)!}$$

where the summation is over $r \geq i \geq j \geq 0$ subject to $t-1 \geq r+i$.

In particular, if $t \leq \frac{s+t}{3\log s}$ then $f(s,t) < c\frac{t}{s+t}$ for some absolute constant c.

Proof. Notice first that the h_r satisfy:

$$h_r(n) = h_r(n-1) + \frac{1}{n} h_{r-1}(n-1). \tag{1}$$

To facilitate the proof, some additional definitions are required. Set $g(s,t) := \binom{s+t}{s} f(s,t)$ and note that g satisfies:

$$g(s,t) = g(s-1,t) + \frac{s+t-1}{s} g(s-1,t-1)$$

with boundary conditions $g(s,1)=1$ for $s \geq 0$ and $g(0,t)=1$ for $t \geq 1$.

We will express g in the form:

$$g(s,t) = \sum_{0 \leq r \leq t-1} A_r(s,t)\, h_r(s), \tag{2}$$

and translate the recurrence and boundary conditions for g to be stated in terms of the A's. We rewrite the recurrence for g in these new terms, and obtain:

$$s \sum_{r=0}^{t-1} (h_r(s) A_r(s,t) - h_r(s-1) A_r(s-1,t)) =$$
$$(s+t-1) \sum_{r=0}^{t-2} h_r(s-1) A_r(s-1,t-1).$$

Replace $h_r(s)$ by $h_r(s-1) + h_{r-1}(s-1)/s$ and equate the coefficients of $h_r(s-1)$ on either side. The conclusion is that g can indeed be expressed as in equation 2, provided we can find A's satisfying:

$$A_{r+1}(s,t) = (s+t-1) A_r(s-1,t-1) - s(A_r(s,t) - A_r(s-1,t))$$

as well as $A_0(0,t)=1$ for $t \geq 1$ and $A_0(s,1)=1$ for $s \geq 0$.

We look for an expression for the A's of the form:

$$A_r(s,t) = \sum (-1)^i \alpha_{r,i} \binom{s+t-r-i-1}{s}, \tag{3}$$

where the summation is over $r \geq i \geq 0$ with $t-1 \geq r+i$.

Again, equation 3 will be justified in that the A's can indeed be presented this way, provided we can find α's which satisfy an appropriate recurrence and boundary conditions. The recurrences for the A's translate into the following conditions the α's need to satisfy for all $0 \leq r \leq t-1$:

$$\sum_{i=0}^{r+1} (-1)^i \alpha_{r+1,i} \binom{s+t-r-i-2}{s} = (t-1) \sum_{i=0}^{r} (-1)^i \alpha_{r,i} \binom{s+t-r-i-3}{s-1} + \tag{4}$$
$$+ s \sum_{i=0}^{r} (-1)^i \alpha_{r,i} \left(\binom{s+t-r-i-3}{s-1} + \binom{s+t-r-i-2}{s-1} - \binom{s+t-r-i-1}{s} \right).$$

The sum of the last three binomial coefficients simplifies to $-\binom{s+t-r-i-3}{s}$. Also, in the previous sum replace $\binom{s+t-r-i-3}{s-1}$ by $\binom{s+t-r-i-2}{s}-\binom{s+t-r-i-3}{s}$. After these steps the right hand side of equation 4 becomes

$$(t-1)\sum_{i=0}^{r}(-1)^i\alpha_{r,i}\binom{s+t-r-i-2}{s}+$$
$$+(s+t-1)\sum_{i=1}^{r+1}(-1)^i\alpha_{r,i-1}\binom{s+t-r-i-2}{s}.$$

Replace $t-1$ by $(t-r-i-2)+(r+i+1)$ in the first sum and change the index of summation in the second from i to $i-1$ thus obtaining

$$\sum_{i=0}^{r}(-1)^i\alpha_{r,i}((t-r-i-2)+(r+i+1))\binom{s+t-r-i-2}{s}-$$
$$-(s+t-1)\sum_{i=0}^{r}(-1)^i\alpha_{r,i}\binom{s+t-r-i-3}{s}=$$
$$\sum_{i=0}^{r}(-1)^i\alpha_{r,i}\,(s+t-r-i-2)\binom{s+t-r-i-3}{s}+$$
$$\sum_{i=0}^{r}(-1)^i\alpha_{r,i}\,(r+i+1)\binom{s+t-r-i-2}{s}-$$
$$\sum_{i=0}^{r}(-1)^i\alpha_{r,i}\,(s+t-1)\binom{s+t-r-i-3}{s}=$$
$$\sum_{i=0}^{r}(-1)^i\alpha_{r,i}\,(r+i+1)\binom{s+t-r-i-2}{s}-$$
$$\sum_{i=0}^{r}(-1)^i\alpha_{r,i}\,(r+i+1)\binom{s+t-r-i-3}{s}.$$

Again change the variable in the last sum to conclude the necessity of the condition:

$$\sum_{i=0}^{r+1}(-1)^i\alpha_{r+1,i}\binom{s+t-r-i-2}{s}=\sum_{i=0}^{r}(-1)^i\alpha_{r,i}\,(r+i+1)\binom{s+t-r-i-2}{s}+$$
$$+\sum_{i=1}^{r+1}(-1)^i\alpha_{r,i-1}\,(r+i)\binom{s+t-r-i-2}{s}.$$

We thus arrive at the recurrence for the α's:

$$\alpha_{r+1,i}=(r+i+1)\,\alpha_{r,i}+(r+i)\,\alpha_{r,i-1} \tag{5}$$

for all $r \geq i \geq 0$. The boundary conditions are not hard to establish, viz., $\alpha_{0,0}=1$ and $\alpha_{r,-1}=\alpha_{r,r+1}=0$ for all $r \geq 0$. We claim that for all r,i there holds $\alpha_{r,i}=\beta_{r,i}$, where

$$\beta_{r,i} = (r+i)! \sum_{j=0}^{i} \frac{(-1)^{i-j}}{(i-j)!} h_j\,(r+j)\,.$$

Let us verify the boundary conditions first. That $\beta_{0,0}=1$ and $\beta_{r,-1}=0$ are easily verified. Rather than showing directly that $\beta_{r,r+1}=0$, we show that $\beta_{0,i}=0$ for all $i \geq 1$ and observe that $\alpha_{0,i}=0$ for all $i \geq 1$ along with the recurrence (5), imply that $\alpha_{r,i}=0$ for all $i > r \geq 0$. To show $\beta_{0,i}=0$ note also that $h_j\,(j)=\frac{1}{j!}$ and so

$$\beta_{0,i} = i! \sum_{j=0}^{i} \frac{(-1)^{i-j}}{(i-j)!j!}.$$

which is zero if $i \geq 1$.

The only part left is to establish equation 5 for the β's. That is, we need to show:

$$(6) \quad (r+i+1)! \sum_{j=0}^{i} \frac{(-1)^{i-j}}{(i-j)!} h_j(r+j+1) =$$

$$= (r+i+1)! \sum_{j=0}^{i} \frac{(-1)^{i-j}}{(i-j)!} h_j(r+j) + (r+i)! \sum_{j=0}^{i-1} \frac{(-1)^{i-j-1}}{(i-j-1)!} h_j(r+j).$$

To prove this identity, divide out by $(r+i)!$ and consider the difference between the first two sums, using the recurrence 1 for the h's. The result is

$$(r+i+1) \sum_{j=1}^{i} \frac{(-1)^{i-j}}{(i-j)!} \cdot \frac{1}{r+j+1} h_{j-1}\,(r+j)$$

(note that the $j=0$ term vanished) which is split into two

$$\sum_{j=1}^{i} \frac{(-1)^{i-j}}{(i-j)!} h_{j-1}\,(r+j) + \sum_{j=1}^{i-1} \frac{(-1)^{i-j}}{(i-j-1)!} \frac{1}{r+j+1} h_{j-1}\,(r+j)$$

again the $j=i$ term in the last sum vanished. Return now to the third sum in (6), which becomes after dividing by $(r+i)!$ and a change in summation variable:

$$\sum_{j=1}^{i} \frac{(-1)^{i-j}}{(i-j)!} h_{j-1}\,(r+j-1) =$$

$$\sum_{j=1}^{i} \frac{(-1)^{i-j}}{(i-j)!} h_{j-1}\,(r+j) - \sum_{j=1}^{i} \frac{(-1)^{i-j}}{(i-j)!} \frac{1}{r+j} h_{j-2}\,(r+j-1)\,.$$

Which is seen to be identical with the previous expression after a change of the summation variable. This concludes the derivation of the closed form formula. We now turn to the asymptotic analysis. ∎

4. Asymptotic analysis of the formula

It is not hard to show (e.g., by induction based on equation 1 that for $s>r\geq 1$, there holds:

$$h_r(s)\leq 3\frac{\log^r s}{r!}.$$

The analysis of the previous section now yields:

$$g(s,t)\leq 3\sum_{r=0}^{t-1}A_r(s,t)\frac{\log^r s}{r!}.$$

Since $\alpha_{r,i}$ are nonnegative for $r\geq i\geq 0$ the A's may be bounded:

$$\frac{A_r(s,t)}{\binom{s+t}{s}}\leq\sum_{i=0}^{r}\alpha_{r,i}\frac{\binom{s+t-r-i-1}{s}}{\binom{s+t}{s}}\leq\sum_{i=0}^{r}\alpha_{r,i}\left(\frac{t}{s+t}\right)^{r+i+1}.$$

An upper bound for the α's is easy to derive from either the recurrence they satisfy or from their closed form formula:

$$\alpha_{r,i}\leq(r+i)!h_i(r+i)\leq 3(r+i)!\frac{\log^i(r+i)}{i!}.$$

The straightforward derivation is omitted.

Putting everything together, we arrive at:

$$f(s,t)\leq 9\sum\binom{r+i}{r}\log^i(r+i)\left(\frac{t}{s+t}\right)^{r+i+1}\log^r s,$$

the summation being over all $r\geq i\geq 0$ with $t-1\geq r+i$. We overestimate the sum, replacing $\binom{r+i}{r}$ by 2^{r+i}, and $\log^i(r+i)$ by $\log^i s$, thus concluding that

$$f(s,t)\leq 9\frac{t}{s+t}\sum\left(\frac{2t\log s}{s+t}\right)^{r+i}.$$

As long as $\frac{2t\log s}{s+t}$ is bounded away from 1, the sum clearly converges and we get $f(s,t)=O\left(\frac{t}{s+t}\right)$, as desired. ∎

5. Boolean functions without small influential coalitions

Theorem 5.1. *There is a sequence of boolean functions f_n on $n=1,2,\ldots$ variables, having expectation 1/2, such that for every $\varepsilon>0$, for any large enough n, the influence of any set of $\frac{\varepsilon n}{\log^2 n}$ variables is $O(\varepsilon)$.*

Remark 5.1 The boolean function called *the tribes* introduced in [3] has n variables, its expectation is 1/2 and all individual variables have influence $O\left(\frac{\log n}{n}\right)$ and in this sense it is best possible by [7]. The functions considered here are somewhat related to that function.

Remark 5.2 At first we show that functions f_n as above exist, except their expectations are $\frac{1}{2}+o(1)$. This construction is then modified to yield the theorem.
Proof. Some definitions are required first: for a positive integer n let $[n]:=\{1,\ldots,n\}$. If b is a positive integer, let $n=n_b$ be the smallest multiple of b with $\left(1-2^{-b}\right)^{n_b/b} \leq \frac{\log 2}{n_b}$. Writing b in the form $b=\log_2 n - 2\log_2 \log_2 n + R$ and substituting it in the inequality $\left(1-2^{-b}\right)^{n/b} \leq \frac{\log 2}{n}$ it is easy to see that $b=\log_2 n_b - 2\log_2 \log_2 n_b + o(1)$ and $\left(1-2^{-b}\right)^{n_b/b} \geq \frac{\log 2}{n_b}\left(1-\frac{\log^2 n_b}{n_b}\right)$.

Fix an integer b and let $n=n_b$ as above. Let $\Theta=\Theta_n$ be the set of all partitions of $[n]$ into classes of size b. The collection of all sequences $\left(T^1,\ldots,T^n\right)$ where all $T^i \in \Theta$ is denoted $\mathcal{T}=\mathcal{T}_{\mathrm{n}}$. The j-th class of partition T^i is denoted T^i_j. Also Γ is the set of all mappings from $[n]$ to $\{0,1\}$. The collection of all $(g_1,\ldots,g_n)$ with $g_i \in \Gamma$ is denoted by $\mathcal{G}$.

For $\mathbf{T}\in\mathcal{T}$ and $\mathbf{g}\in\mathcal{G}$ let $F=F_{\mathbf{T},\mathbf{g}}$ be the boolean function defined by

$$F(x_1,\ldots,x_n) = \bigwedge_{1\leq i\leq n} \bigvee_{1\leq j\leq n/b} \bigwedge_{k\in T^i_j} \left(x_k = g_i(k)\right).$$

In other words $F(x)=1$ iff for all $1\leq i\leq n$ there is a class T^i_j of partition T^i so that x coincides with the function g_i on each element of T^i_j. Such a class is called a *strike* for the assignment x. For future reference, we also define

$$F^i(x_1,\ldots,x_n) = \bigvee_{1\leq j\leq n/b} \bigwedge_{k\in T^i_j} \left(x_k = g_i(k)\right).$$

We consider a probability space consisting of all functions $F_{\mathbf{T},\mathbf{g}}$ with a uniform probability distribution. Our goal is to show, via a probabilistic argument, that most functions in this collection have the property that no small sets of variables are influential. It is also shown that most members in this collection have expectation very close to 1/2, and consequently, can be slightly modified to make the expectation equal 1/2 without creating small influential sets.

Let Q be a set of variables of a given cardinality, and T a partition from Θ. For any $k\leq b$ let $a_k=a_k(Q,T)$ be the number of blocks in T which have k elements in common with Q. For fixed Q and a randomly selected T, (or vice versa, it does not matter), it is easy to find the distribution of the integers a_k. Skipping the details for the moment, Q and T are said to *match* if all integers a_k do not exceed their expectation by too much. Classes of T which have a nonempty intersection with Q are called *Q-classes*, others are *non-Q*. As usual, when we say that *almost all* members in a set have a certain property, it means that the family of sets is parameterized and when the relevant parameter tends to infinity the fraction of members having that property tends to 1. In the whole discussion $1/10>\varepsilon>0$ is kept fixed. We always assume n to be large enough so as to make all the inequalities needed valid.

The main steps of the proof are as follows:

(i) For all choices of $\mathbf{T}$, and almost all $\mathbf{g}$, the expectation of $F_{\mathbf{T},\mathbf{g}}$ is $\frac{1}{2}+o(1)$ (Proposition 5.4).

(ii) For almost all $\mathbf{T}$, and *every* set Q of $q=\frac{\varepsilon n}{\log^2 n}$ variables, at least $(1-o(1))\,n$ partitions T^i in $\mathbf{T}$ match Q (proposition 5.3).

(iii) Fix an arbitrary partition $T^i\in\Theta$, and $g_i\in\Gamma$. Then the influence any set Q of q variables can have on F^i is $\le\frac{1}{n}$ (Proposition 5.1).

(iv) If, moreover, T^i and Q match, then

$$I_{F^i}(Q)=O\left(\frac{\varepsilon}{n}\right),$$

(Proposition 5.2).

Proposition 5.1. *For any partition $T^i\in\Theta$, and a $g_i\in\Gamma$, the influence of any set Q of $q=\frac{\varepsilon n}{\log^2 n}$ variables, on F^i is $\le\frac{1}{n}$.*

Proof. Randomly assign values only to those variables which are in non-Q classes of T^i. We show that with probability $\ge 1-\frac{1}{n}$ such a partial assignment already determines that $F^i=1$. The number of Q-classes in T is at most q. So we have $n-q$ non-Q classes. For each fixed non-Q class from the 2^b possible assignments of the variables exactly one ensures that the class is a strike. So the probability that a fixed non-Q class is a strike is 2^{-b}, moreover these events are independent for different classes. Therefore, the probability that no non-Q class is a strike does not exceed:

$$\left(1-2^{-b}\right)^{\left(\frac{n}{b}-q\right)}\le\left(\frac{\log 2}{n}\right)^{1-\frac{bq}{n}}\le\frac{1}{n}.$$

as claimed. ∎

Definition 5.1 A partition $T\in\Theta$ and a set $Q\subseteq[n]$ are said to *match* if for each $1\le k\le b$ the number of classes J in T with $|Q\cap J|\ge k$ does not exceed

$$4nb^{-1}k^2\binom{b}{k}\left(\frac{|Q|}{n}\right)^k.$$

Proposition 5.2. *Let partition T^i match the set Q of q variables, and let $g_i\in\Gamma$ be arbitrary. The influence of Q on F^i is at most $\frac{9\varepsilon}{n}$.*

Proof. An assignment to all variables not in Q leaves F^i undetermined only if the following two conditions hold: (i) There is no strike among non-Q classes. (ii) There is a Q-class where the assignment completely agrees with g_i. These two events are independent, (i) occurs with probability $\le 1/n$ by Proposition 5.1, so let's consider (ii):

Let J be a fixed class of T^i with $|J \cap Q| = k$ for some $k \geq 1$. Obviously the probability that $x_s = g_i(s)$ for all $s \in J - Q$ equals $2^{-(b-k)}$. But T^i matches Q, so p, the probability under consideration is bounded as follows:

$$p \leq \sum_{1 \leq k \leq b} 4nb^{-1}k^2 \binom{b}{k} \left(\frac{q}{n}\right)^k 2^{-(b-k)} = \frac{4n}{b2^b} \sum k^2 \binom{b}{k} z^k,$$

where $z = \frac{2q}{n}$. (For each fixed k the fact that T^i matches Q gives an upper bound on the number of classes J with $|J \cap Q| = k$.) Note that $\sum k^2 \binom{b}{k} z^k = bz(1+z)^{b-2}(1+bz)$, hence

$$p \leq \frac{8q}{2^b}\left(1 + \frac{2q}{n}\right)^{b-2} \left(1 + \frac{2bq}{n}\right).$$

Using that $b = \log n - 2 \log\log n + o(1)$, $2^b \geq (1+o(1))n/(\log n)^2$ and $q = \varepsilon n/(\log n)^2$ we get

$$p \leq 8\varepsilon(1+o(1))\left(1 + \frac{2}{\log n}\right)\left(1 + \frac{2}{\log n}\right) \leq 9\varepsilon,$$

as claimed. ∎

In the following proposition we use Chernoff's inequality several times. The version of this theorem that we now state appears in [5], p. 13, (see also [6]).

Chernoff's inequality. *Let n independent trials be performed, each with probability p of success. Assume that $0 < p \leq 1/2$, that $0 < c \leq 1/12$, and that $cp(1-p)n \geq 12$. Let S_n be the number of successful trials, and let $M = pn$ be the expected number of successful trials. Then*

$$Pr\left(|S_n - M| \geq cM\right) \leq \left(c^2 M\right)^{-1/2} e^{-c^2 M/3}.$$

We will also use a second version (it is an immediate consequence of e.g. Corollary A. 7. in [2]).

For all $\varepsilon > 0, \varepsilon' > 0$ if m, i are sufficiently large then the following holds: if we repeat a trial independently i times and the expected number of successes is m and S is the actual number of successes then $Pr\left(|S - m| > m^{1/2+\varepsilon}\right) < \varepsilon'$.

Proposition 5.3. *Almost every $\mathbf{T} \in \mathcal{J}$ has the property that every set Q of q variables matches at least $(1 - o(1))n$ partitions in $\mathbf{T}$.*

Proof. Let $1 \leq k \leq b$ and $j \leq n/b$ be fixed. First we estimate the probability of $|T_j^i \cap Q| \geq k$. We may think of the partition T^i as given and the set Q (with q elements) being selected at random. Then

$$Pr\left(|T_j^i \cap Q| \geq k\right) \leq \binom{b}{k} \frac{q}{n} \frac{q-1}{n-1} \cdots \frac{q-k+1}{n-k+1} \leq \binom{b}{k} \left(\frac{q}{n}\right)^k.$$

So the expected number of classes with at least k elements in common with Q is at most $E_k = \frac{n}{b}\binom{b}{k}\left(\frac{q}{n}\right)^k$. The probability that the actual number is at least $4k^2$ times the expectation does not exceed $\left(1/4k^2\right)$. This is true for every k; for small numbers k we will need a better upper bound.

Assume that $1 \le k \le 1/\delta$ where $\delta > 0$ is a small constant. We will denote by Y_j the event $|T_j^i \cap Q| \ge k$ (with k fixed as above.) Whether or not Q and T^i match depends on the question if more than $4k^2 E_k$ of the events Y_j hold. We want to use Chernoff's inequality to prove that Q and T^i match with high probability, that is the probability that Y_j hold for too many numbers j is small. Unfortunately the events Y_j are not independent since the set Q is randomized with the condition $|Q| = q$. (If $x \in Q$ would be randomized independently for each x with a probability n/q then the events Y_j would be independent.)

To circumvent this problem we will do the following; we randomize Q in two steps, first we take a truly pointwise random set Q' where each elements will belong to Q' with a probability of q/n independently, then change Q'. Suppose that Q' has $q+r$ elements. (The second version of Chernoff's inequality implies that with a probability of higher than $1 - \frac{\delta^3}{2}$ we have $|r| \le n^{2/3}$). If r is positive we discard r random element from Q if r is negative we add r random elements to Q. The point is that in both cases we changed Q' in at most $n^{2/3}$ classes T_j^i. Let Y_j' be the analogue of Y_j defined by using Q' instead of Q. To use Chernoff inequality for the trials Y_j' we need a lower bound on the expected number of successful trials.

First we give a lower bound for $Pr\left(|T_j^i \cap Q'| \ge k\right)$ for an arbirary fixed j.

$$Pr\left(|T_j^i \cap Q'| \ge k\right) \ge Pr\left(|T_j^i \cap Q'| = k\right).$$

For each fixed j we have

$$Pr\left(|T_j^i \cap Q'| = k\right) = \sum_{W \subseteq T_j^i, |W| = k} Pr\left(T_j^i \cap Q' = W\right).$$

For a fixed W ocurring in the sum $Pr\left(T_j^i \cap Q' = W\right) = \frac{\binom{n-b}{q-k}}{\binom{n}{q}}$ which may be seen to be $\ge (q/2n)^k \ge \left(\frac{\varepsilon}{2\log^2 n}\right)^k$. Since the number of possible sets W is $\binom{b}{k} \ge \left(\frac{\log n}{2k}\right)^k$ we have that $Pr\left(|T_j^i \cap Q'| \ge k\right) \ge \left(\frac{\varepsilon}{4k\log n}\right)^k \ge \frac{1}{2}n^{-1/3}$ if n is sufficiently large.

This implies that the expected number M' of classes with $Pr\left(|T_j^i \cap Q'| \ge k\right)$ is greater than $2n^{2/3}$. Therefore Chernoff's inequality implies that the probability that the numnber of successes for Y_j' is more than twice its expected value is smaller than $\delta^3/2$.

This together with the bounds $Pr\left(|r|>n^{2/3}\right)<\delta^{3/2}$, $M'>2n^{2/3}$ and the fact that E_k is an upper bound for the number of successes for Y'_j, imply that Pr(for more than $4k^2E_k$ indices j the event Y_j holds) $\leq \delta^3$. That is in the range $1\leq k\leq 1/\delta$ for each fixed k the probability that the number of classes with at least k common elements with Q is at least $4k^2$ times the expectation is at most δ^3. Using our previous estimate for an arbitrary k we get that the probability that this does not occur for any $1\leq k\leq b$ is at least $1-\sum_{k\leq 1/\delta}\delta^3-\frac{1}{4}\sum_{k>1/\delta}^{b}1/k^2\geq 1-\delta/2$. Thus, for any fixed i the probability that T^i does not match Q is at most $\delta/2$. Since the different partitions T^i are independent, Chernoff's inequality implies that

$$Pr\left(|\{i|\ T^i\text{does not match}Q\}|\geq \delta n\right)<2^{-\delta^2 n/2}.$$

This inequality holds for every fixed Q. Since the number of possible sets Q is $\binom{n}{q}=\binom{n}{\frac{\varepsilon n}{\log^2 n}}$, the probability that there is a Q matching fewer than $(1-\delta)n$ partitions in $\mathbf{T}$ is $<2^{-\delta^2 n/2}\binom{n}{q}$. Select δ to be $o(1)$, but also asymptotically bigger than $\frac{\sqrt{\log\log n}}{\log n}$. This choice guarantees that this expression tend to zero as n tends to infinity and the proposition follows. ∎

Assume now that $\mathbf{T}\in\mathcal{J}$ is such that every set of $q=\frac{\varepsilon n}{\log^2 n}$ variables matches all but $o(n)$ of the T^i. Consider a function $F=F_{\mathbf{T},\mathbf{g}}$, and let us estimate the influence of a set Q of q variables on F. The fact that an assignment to some of the variables leaves the function h undetermined is denoted by the shorthand $h=*$. Consider a random assignment to variables not in Q. If all F^i are determined by this partial assignment, then F is determined and Q does not influence its value. Therefore,

$$I_F(Q)\leq Pr\left(\vee_i F^i=*\right)\leq\sum_i Pr\left(F^i=*\right)=\sum I_{F^i}(Q).$$

Break this sum into two parts according to whether T^i matches Q or not. There are only $o(n)$ indices i for which Q and T^i do not match. Each of the corresponding terms is at most $\frac{1}{n}$, by Proposition 5.1, for a total of $o(1)$. Those terms where T^i and Q do match are, of course, no more than n in number, each $\leq\frac{9\varepsilon}{n}$. The whole sum, thus, does not exceed $\leq 10\varepsilon$, as claimed.

Proposition 5.4. *For all sequences $\left(T^1,\ldots,T^n\right)$ in $\mathcal{J}_{\mathrm{n}}$ and almost all $(g_1,\ldots,g_n)\in\mathcal{G}$ the expectation of $F=F_{\mathbf{T},\mathbf{g}}$ is $\frac{1}{2}+o(1)$.*

Proof. The partitions $\left(T^1,\ldots,T^n\right)$ will be fixed once and for all. The function $F=F_{\mathbf{T},\mathbf{g}}$ under consideration, is thus uniquely defined by the choice of functions $\mathbf{g}$. We first reduce the problem to the proof of the following statement.

Claim 5.1. *Let the functions $\mathbf{g}$ be selected at random, thus defining F. Consider randomly chosen inputs, x and y for F. The probability for these selections to satisfy $F(x)=F(y)$ is $\frac{1}{2}+o(1)$.*

That the claim proves our proposition is shown as follows: For a boolean f and two randomly selected inputs z_1,z_2, it is easily verified that $Pr(f(z_1)=$

$f(z_2)) = \frac{1}{2} + 2\left(E(f) - \frac{1}{2}\right)^2$, where $E(f)$ stands for f's expectation. Therefore the probability considered in the claim equals $\frac{1}{2}+2E\left(\left(E(F)-\frac{1}{2}\right)^2\right)$, where the internal expectation refers to random selection of inputs to F, while the external one refers to the random selection of F, via a choice of $\mathbf{g}$. If indeed $E\left(\left(E(F)-\frac{1}{2}\right)^2\right)=o(1)$, as stated in the claim, then for almost all choices of $\mathbf{g}$ it holds that $|E(F)-\frac{1}{2}| = o(1)$, as the proposition says.

It is easily verified that the claim follows if we can show $Pr(F(y)=1|F(x)=\tau) = \frac{1}{2}+o(1)$, for any $\tau \in \{0,1\}$, with F,x,y randomly chosen, as in the proposition. Actually, we'd like to pass to a more restrictive conditioning. First observe that the mapping which replaces y by $y \oplus x$, each g_i by $g_i \oplus x$, and x itself by 0 (where $\oplus$ stands for mod 2 sum) is an isomorphism of our probability space. Therefore no generality is lost if we assume $x=0$. Let S^i be the (random) set of classes in T^i which $x=0$ strikes. Not only would we like to condition on $F(0)=\tau$, but on a much more detailed condition, viz., the collection of all $S^i\,(n \geq i \geq 1)$. (Clearly, the list of all S^i, determines $F(0)$.) We'd like to maintain that despite the conditioning, it still holds that for each i the probability for $F^i(y)=1$ is close to $1-\frac{\log 2}{n}$ and that these equalities for varying i are independent. Of course, neither claim is correct as it stands. However, we notice, that with the exception of a certain rare event the previous statements are almost correct. We start by considering this rare event U in Ω, the space defined by random choice of y and g_i for $i=1,\dots,n$.

Definition 5.2 A class $J \in T^i$ is a *zero class* if g_i is identically zero on it. It's a *y class* if y restricted to it is all zeros. If T^i has a class which is both a zero and a y-class, we say that i is *exceptional.*

Consider the following three events in Ω:

(P1) No T^i has more than $\rho = 10\log^2 n$ y-classes.

(P2) No T^i has more than ρ zero classes.

(P3) There are $\leq \rho$ exceptional indices.

Let $U = \neg P1 \cup \neg P2 \cup \neg P3$. First we prove that $Pr(U)=o(1)$. Since $Pr(U) \leq Pr(\neg P1)+Pr(\neg P2)+Pr(\neg P3)$ it is enough to prove that all of the three events separately has a probability of $o(1)$.

Let $Z(J)$ be the event that J is a zero class and $Y(J)$ is the event that J is a y class. For any fixed class J we have $Pr(Z(J)) \leq 2^{-b} \leq 2\varepsilon/q$ and $Pr(Y(J)) \leq 2^{-b} \leq 2\varepsilon/q$. Inside a fixed T^i all of the events $Z(J), Y(J)$ where J is a class are mutually independent. Using these remarks we get:

$$Pr(\neg P1) \leq \sum_{i=1}^{n} \sum_{k \geq \rho} \binom{q}{k} \left(\frac{2\varepsilon}{q}\right)^k \leq n \sum_{k \geq \rho} \frac{1}{k!} q^k \left(\frac{1}{q}\right)^k \leq 2n\frac{1}{\rho!} \leq o(1).$$

The same calculation shows that $Pr(\neg P2)=o(1)$. The probability that a fixed class is both a zero class and a y class is at most $\left(\frac{2\varepsilon}{q}\right)^2$ therefore the probability that a fixed index i is exceptional is at most $q\left(\frac{2\varepsilon}{q}\right)^2 \leq \frac{4\varepsilon^2}{q} \leq \frac{4(\log n)^2 \varepsilon}{n}$. For different indices i the events that T^i are exceptional are independent therefore Chernoff's inequality implies that the probability that the number of such indices is more than ρ (more than twice their expected number) is $o(1)$.

Let Σ be the set of all sequences $y, S^1, S^2, \ldots, S^n$, where y is an input to F and for each $i = 1, \ldots, n$, S^i is a set of classes in T^i so that: (i) y satisfies condition (P1), (ii) all S^i have cardinality $\leq \rho$ (this corresponds to (P2)), (iii) for no more than ρ indices i does T^i have a y-class which belongs to S^i (for P3).

For each $\sigma \in \Sigma$ let $U_\sigma \equiv$ "for each $i = 1, \ldots, n$ the set of zero-classes of T^i is S^i."

The events U, U_σ, $\sigma \in \Sigma$ clearly partition our probability space Ω. Moreover, $F(0)$ is fixed on each U_σ and therefore our task reduces to showing that $Pr(F(y)=1) = \frac{1}{2} + o(1)$ on each U_σ. The only randomization left unspecified is that of g_i $i = 1, \ldots, n$ subject to the conditions given in U_σ. Since each condition "the set of zero-classes of T^i is S^i" restricts only the choice of g^i the events $\Phi_i \equiv$ "y has a strike in T^i" for $i = 1, \ldots, n$ are independent within each U_σ. We turn to estimate the probability of Φ_i:

Condition U_σ implies that g_i must be identically zero on J iff $J \in S^i$. That is, g_i is already determined on each $J \in S^i$. On T^i classes, not in S^i there are $2^b - 1$ possibilities (all choices but for the all zero function) for g_i among which to select with uniform distribution.

If i is exceptional, a property which y and the set S^i already determine, then clearly $Pr(\Phi_i) = 1$.

If i is not exceptional then no $J \in S^i$ is a strike for y. Therefore Φ_i may hold only if some T^i class $J \notin S^i$, is a strike for y. The probability of this event is $1 - \left(1 - \frac{1}{2^b - 1}\right)^{\frac{n}{b} - |S^i|}$. Since $|S^i| \leq \rho$, for all nonexceptional i we have

$$1 - \left(1 - \frac{1}{2^b - 1}\right)^{\frac{n}{b}} \geq Pr(\Phi_i) \geq 1 - \left(1 - \frac{1}{2^b - 1}\right)^{\frac{n}{b} - \rho}$$

Using the independence of the events Φ_i and the fact that the number of exceptional numbers i is at most ρ we have

$$\left(1 - \left(1 - \frac{1}{2^b - 1}\right)^{\frac{n}{b}}\right)^{n - \rho} \geq Pr(\exists i\ \Phi_i) \geq \left(1 - \left(1 - \frac{1}{2^b - 1}\right)^{\frac{n}{b} - \rho}\right)^{n}.$$

As we noted earlier, our choice of n implies $\left(1 - 2^{-b}\right)^{n/b} = \frac{\ln 2}{n}(1 + o(1))$, therefore

$$Pr(\exists i\ \Phi_i) = \frac{1}{2} + O\left(\frac{\log^4 n}{n}\right)$$

as claimed. ∎

We complete the proof, supplying functions with similar bounds on influences, whose expectation equals $1/2$. To simplify matters we speak of functions with $2n$, rather than n variables. The first n bits are called x and the last ones y. Consider a function F, as above, defined on x, whose expectation equals $\frac{1}{2} + \delta = \frac{1}{2} + O\left(\frac{\log^4 n}{n}\right)$

and where any coalition of size $c\frac{n}{\log^2 n}$ has influence $O(c)$. We need another function F' defined on y with the following properties: The expectation of F' is $1-\mu$, where $\mu = o(1)$ and $\delta = o(\mu)$ and also, that all coalitions of size $c\frac{n}{\log^2 n}$ have influence $O(c)$. (We prove the existence of such an F' at the end of the proof.) We also need a function h on $2n$ variables, whose only relevant property is its expectation as we soon explain. Our function $\Psi(x,y)$ is defined as follows:

$$\Psi(x,y) = F'(y)\, F(x) \vee \left(\neg F'(y)\, h(x,y)\right),$$

and its expectation,

$$E(\Psi) = (1-\mu)\left(\frac{1}{2}+\delta\right) + \mu E\left(h | F'(y) = 0\right).$$

This number ranges between $(1-\mu)\left(\frac{1}{2}+\delta\right)$ and $(1-\mu)\left(\frac{1}{2}+\delta\right)+\mu$, depending on the choice of h. This interval includes our desired value of $\frac{1}{2}$ iff $\mu \geq \frac{2|\delta|}{1+|\delta|}$. Since this condition is assumed to hold, there is a choice of h for which $E(\Psi) = \frac{1}{2}$.

To estimate influences on Ψ, note that a coalition Q which consists of subsets Q_1, Q_2 of x, y, respectively, can have influence at most $\mu + I_F(Q_1) + I_{F'}(Q_2)$. Therefore, if $|Q| = c\frac{n}{\log^2 n}$, then $I_\Psi(Q) = O(c)$, as claimed.

We show that there exists a function F' with the necessary properties. Let P be a subset of $[n]$ and define

$$F_P(x_1, \ldots, x_n) = \bigwedge_{i \in P} \bigvee_{1 \leq j \leq n/b} \bigwedge_{k \in T_j^i} (x_k = g_i(k)).$$

Using the same argument as earlier we get that if Q is any coalition we get

$$I_{F_P}(Q) \leq \sum_{i \in P} I_{F^i}(Q).$$

If $|Q| \leq \frac{\varepsilon n}{\log^2 n}$ then according to Proposition 5.1 $I_{F^i}(Q) \leq 1/n$ for all $1 \leq i \leq n$ and therefore $I_{F_P}(Q) \leq |P|/n$. So if we define $F' = F_P$ for any P with $|P| = o(n)$ then F' meets the requirements concerning $I_{F'}(Q)$.

We give a lower bound on $E(F_P)$. $E(F_P) = E\left(1-\max_{i \in P}\left(1-F^i\right)\right) \geq E\left(1-\sum_{i \in P}\left(1-F^i\right)\right) = 1-\sum E\left(1-F^i\right) \geq 1-c'|P|/n$ where c' is an absolute constant.

We give an upper bound on $E(F_P)$ only for certain subsets P. Let $P_1, \ldots, P_k$ be a partition of $[n]$ into subsets of size roughly n/k, (say $\frac{n}{2k} \leq |P_j| \leq \frac{2n}{k}$). $1/4 \leq (1-E(F)) \leq \sum_{1 \leq j \leq k} E\left(1-F_{P_j}\right) \leq k \max_j E\left(1-F_{P_j}\right)$.

Therefore there is a $P' = P_{j_0}$ with $E(F_{P'}) \leq 1-\frac{1}{4k}$. So if we pick k so that δ is sufficiently small with respect to $\frac{1}{k}$ and $\frac{1}{k} = o(1)$ then all of the requirements are met with $F' = F_{P'}$. ∎

References

[1] N. Alon, and M. Naor: Coin-flipping games immune against linear-sized coalitions, FOCS 1990, 46–54, to appear in *SIAM J. on Computing.*

[2] N. Alon, and J.H. Spencer: *The Probabilistic Method*, Wiley-Interscience Publication, John Wiley and Sons, 1992.

[3] M. Ben-Or, and N. Linial: Collective coin flipping, in: Randomness and Computation (S. Micali ed.) Academic Press, New York, 1990, 91–115.

[4] M. Ben-Or, N. Linial, and M. Saks: Collective coin flipping and other models of imperfect randomness, in: *Combinatorics (Eger 1987)*, Colloq. Math Soc. János Bolyai **52**, 75–112.

[5] B. Bollobás: *Random Graphs*, Academic Press, 1982.

[6] H. Chernoff: A measure of asymptotic efficiency for tests of hypothesis based on the sum of observations, *Ann. Math. Stat.* **23** (1952), 493–507.

[7] J. Kahn, G. Kalai, and N. Linial: The influence of variables on Boolean functions, *FOCS* (1988) 68–80.

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

Miklós Ajtai

IBM Almaden Research Center
San Jose, CA
ajtai@almaden.ibm.com

Nathan Linial

Hebrew University
Jerusalem, Israel
IBM Research, Almaden Research Center
San Jose, CA
nati@hujics.huji.ac.il