COMBINATORICA
Akadémiai Kiadó — Springer-Verlag

COMBINATORICA 9 (3) (1989) 269—287

SOME EXTREMAL PROBLEMS ARISING FROM DISCRETE CONTROL PROCESSES

D. LICHTENSTEIN, N. LINIAL and M. SAKS[1]

Received December 8, 1987
Revised September 5, 1988

We consider a simple abstract model for a class of discrete control processes, motivated in part by recent work about the behavior of imperfect random sources in computer algorithms. The process produces a string of n bits and is a "success" or "failure" depending on whether the string produced belongs to a prespecified set L. In an uninfluenced process each bit is chosen by a fair coin toss, and hence the probability of success is $|L|/2^n$. A player called the controller, is introduced who has the ability to intervene in the process by specifying the value of some of the bits of the string. We answer the following questions for both worst and average case: (1) how much can the player increase the probability of success given a fixed number of interventions? (2) in terms of $|L|$ what is the expected number of interventions needed to guarantee success? In particular our results imply that if $|L|/2^n = 1/\omega(n)$ where $\omega(n)$ tends to infinity with n (so the probability of success with no interventions is $0(1)$) then with $O(\sqrt{n \log \omega(n)})$ interventions the probability of success is $1-0(1)$.

Our main results and the proof techniques are related to well-known results of Kruskal, Katona and Harper in extremal set theory.

1. Introduction

A number of recent studies ([11], [12], [13], [4], [1]; see [3] for a survey) concern the following problem: Suppose we have a performance analysis for some randomized algorithm. How sensitive is the analysis to imperfections in the random source? Similar questions can be asked for any random process.

For instance consider the following discrete model of control. An uncontrolled object such as a thrown rock or a boat floating moves according to some random process. At each time unit we think of nature as taking a random step (e.g. a gust of wind or a wave) by sampling some distribution of possible steps.

The movement of the object is influenced by a player, called the *controller*. This player has a definite goal, such as navigating the object to some destination. At each time step the controller can make one move which he chooses from a given repertoire (e.g. he can change the angle between his sails and the wind). A typical question that arises is: what resources (e.g., energy, time) does the navigator need in order to reach his goal?

The analogy that we want to draw here is between the pairs

random source — uncontrolled movement
imperfect source — controlled movement.

The aforementioned references deal with questions such as: Given a quantitative bound on the nonrandomness of the source how much does the behavior of the

[1] Supported in part by NSF Grant DMS8703541 and Air Force Office of Scientific Research Grant AFOSR—0271.

AMS subject classification (1980): 68 R 10, 05 C 80

randomized algorithm driven by it diverge from the random case? What amount of nonrandomness will lead the algorithm astray, so that the desired witness is never (or almost never) found. These are completely analogous to questions such as: Given the amount of energy (or any other resources) that the controller has available how much can the controlled vehicle deviate from its random trajectory? What is the amount of energy that will (almost surely) guarantee that the controller can reach his goal?

Let us review some models used previously to capture the behavior of imperfect sources. In [11], [12], [13], [14], [1] an imperfect coin is modeled by a coin whose probability of heads is either δ or $1-\delta$, for some constant $0<\delta<1/2$. Before each coin flip the adversary sets the probability of heads, and may base the choice on the entire past history of the algorithm and previous coin flips. In [4] a more powerful adversary is postulated. The source provides random bits to the algorithm in fixed length blocks. Each block is selected according to a probability distribution chosen by the adversary, subject only to an upper bound on the probability of any particular block.

In this present paper we take a point of view that is much influenced by the analogy to problems of control we described. A sequence of n bits is generated by a source. Certain strings are "successes" and the others are "failures". The sources are random except that the player (or adversary, depending on your point of view) may intervene in some of them by deterministically deciding the outcome. The restriction comes in limiting the number of deterministic steps taken by the source in the course of the process.

The set of successful strings defines a language L of n bit words. In an uncontrolled process, the probability of success is just $|L|/(2^n)$. Of interest is how the probability of success can be altered by intervention.

The questions we answer here are:

1. How much can the player increase the probability of success given a fixed number of interventions? We give tight upper and lower bounds in terms of $|L|$.
2. What is the expected number of interventions needed to guarantee success? We give a tight upper bound in terms of $|L|$.
3. Questions 1 and 2 deal with bounds that hold for all languages L of a particular size. We also compute the expected value of these quantities over "random" languages.

In particular, we note the following asymptotic consequences of our main results (Theorem 3.2 and Theorem 4.3): If $|L|/2^n=1/w(n)$ where $w(n)$ tends to infinity with n (so that with no intervention the probability of success is $o(1)$) then with $O(\sqrt{n \log w(n)})$ interventions the probability of success is $1-o(1)$. Furthermore, the expected number of interventions needed to guarantee success is $O(\sqrt{n \log w(n)})$.

Two models which are related to the one studied here are "bit extraction" and "collective coin flipping". In the collective coin flipping model introduced by Ben Or and Linial ([2]), the adversary has a fixed number of interventions and must choose the positions in which he intervenes in advance. In the bit extraction problem studied by Chor, et al. ([5]), the adversary not only must choose the positions advance but also must decide the values of those positions in advance. These variations in the power of the adversary seem to be critical; the results in each case are very different. A comparison of these and other models in given in the survey paper ([3]).

2. Notation and terminology

Let B_n denote the set of strings over $\{0, 1\}$ of length n. B_0 consists of one string, $\emptyset$. A subset $L \subseteq B_n$ is called a *language* in B_n. If L is a language in B_n and $\sigma \in B_m$ for $m \leqq n$ then $L(\sigma)$ denotes the language in B_{n-m} consisting of all strings τ such that $\sigma\tau \in L$.

The i^{th} character in string σ is denoted by $\sigma(i)$. The support of σ, supp (σ) is the set of positions that are 1.

Consider a process that sequentially constructs a string of length n from $\{0, 1\}$, where each bit is assigned 0 or 1 with probability 1/2. Given a particular language $L \subseteq B_n$, the probability that $\sigma \in L$ for a string σ produced in this way is $|L|/2^n$. If the process produces a string in L we call the outcome a *success*, otherwise it is a *failure*.

Now consider the same process in the presence of a player who is allowed to determine some of the bits. An *influence strategy* is represented by a function s from the set of strings σ of length less than n to $\{0, 1, *\}$. The interpretation is that each successive bit produced by the process depends on the string σ produced thus far: the next bit is uninfluenced (randomly selected) if $s(\sigma) = *$ and is equal to $s(\sigma)$ otherwise. If σ is a string with $s(\sigma) \neq *$ then we say s *intervenes* on σ. An *influenced process* is therefore specified by a language L in B_n and an influence strategy s. The value of the process val (L, s) is the probability of producing a string in L when applying strategy s.

A sequence σ in B_n is said to be *admissible* with respect to a strategy s if it is a possible outcome of the influenced process, i.e. for every prefix $\sigma(1), \sigma(2), \ldots, \sigma(i)$ on which s intervenes, $s(\sigma(1), \sigma(2), \ldots, \sigma(i)) = \sigma(i+1)$. The strategy s is said to be *k-bounded* if for every admissible string the number of interventions that occurred is at most k. The strategy s *guarantees success* if every admissible string is in L.

3. Optimal k-bounded strategies

Let L be a language in B_n. We define $v_k(L)$ to be the maximum over all k-bounded strategies s of val (L, s), i.e., $v_k(L)$ is the probability of success if the best k-bounded strategy is employed. In particular $v_0(L) = |L|/2^n$.

Lemma 3.1. *Let L be a labelling of B_n, and $k \geqq 1$. Then*

$$v_k(L) = \max\left\{v_{k-1}(L[1]),\ v_{k-1}(L[0]),\ \frac{v_k(L[1]) + v_k(L[0])}{2}\right\}.$$

Proof. The three terms of the maximum correspond to the three options at step 1: force a 1, force a 0 or don't intervene. ∎

Two important examples are:

Example 3.1. Suppose $L = B_n$ [1]. Then $v_0(L) = 1/2$ and $v_k(L) = 1$ for $k \geqq 1$ since the strategy that intervenes at the first step by forcing a 1 guarantees a successful outcome.

Example 3.2. Let $C_{n,t}$ denote the language consisting of all strings of length n with at least t 1's (a *threshold* language), and let $c(n, t) = |C_{n,t}| = \sum_{j=t}^{n} \binom{n}{j}$. It is easy to

show (using, for instance, Lemma 3.1 and induction) that an optimal k-bounded strategy is to force the first k bits to be 1. Then

$$v_k(C_{n,t}) = \begin{cases} c(n-k, t-k)/2^{n-k} & \text{if } k < t \\ 1 & \text{if } k \geq t \end{cases}$$

since for $k<n$, $C_{n,t}[1^k]$ is isomorphic to $C_{n-k,t-k}$.

In this section we will establish a tight lower bound on $v_k(L)$ for any language L in terms of $|L|$. We prove:

Theorem 3.2. *Let L be a language in B_n. If $t \leq n$ is an integer such that*

$$|L| \geq c(n, t)$$

then for all $k \geq 0$,

$$v_k(L) \geq c(n-k, t-k)/2^{n-k}.$$

In particular $v_k(L)=1$ for $k \geq t$.

Observe that this result is tight for threshold languages and thus the theorem can be interpreted as saying that among languages of a specified cardinality the threshold languages result in processes that are the hardest to influence.

We will actually prove a refinement of Theorem 3.2, that provides, for each $s \leq 2^n$ and $k \geq 0$, the minimum of $v_k(L)$ over all languages with $|L|=s$. Theorem 3.2 only does this when $s=c(n, t)$ for some n and t. We begin by defining a sequence of languages $B_n^0, B_n^1, \ldots, B_n^{2^n}$ such that $|B_n^i|=i$ for each i.

Define the following total order on B_n: all strings having r 1's precede those with $r-1$ 1's and for each r the strings having exactly r 1's are ordered by *reverse lexicographic order:* $\alpha < \beta$ if $\alpha_j < \beta_j$ where j is the last index in which they differ (so $\alpha_i=\beta_i$ for $i>j$). For example, B_4 is ordered by:

$$1111 \prec 1110 \prec 1101 \prec 1011 \prec 0111 \prec 1100 \prec 1010 \prec 0110$$
$$\prec 1001 \prec 0101 \prec 0011 \prec 1000 \prec 0100 \prec 0010 \prec 0001 \prec 0000.$$

For $s \leq 2^n$, the language B_n^s consists of the first s strings under this order.

Theorem 3.3. *Let L be a language in B_n and $s=|L|$. Then for any $k \geq 0$,*

$$v_k(L) \geq v_k(B_n^s).$$

Note that for $s=c(n, t)$, we have $B_n^s=C_{n,t}$ and Theorem 3.3 implies Theorem 3.2.

The proof of Theorem 3.3 is by induction on k. The basic idea is to use Lemma 3.1 to express $v_k(L)$ as a maximum of three terms and use the induction hypothesis and a technical lemma to show that one of those terms is at least $v_k(B_n^s)$. The proof depends heavily on the combinatorial properties of the sets B_n^s and we begin with a review of some of these properties (Lemmas 3.4—3.7), and a combinatorial characterization of $v_k(B_n^s)$ (Lemma 3.8).

The sets B_n^s play a central role in extremal set theory, particularly the celebrated theorem of Kruskal [10], Katona [9] and Harper [8] (see also [7], [6]). It is well known in this theory that B_n^s is obtained as follows:

1) Let t be the smallest integer such that $s \geq c(n, t+1)$. Then

$$C_{n,t} \supseteq B_n^s \supseteq C_{n,t+1}.$$

2) For $k=t, t-1, \ldots, 1$, let a_k be defined as the largest number a for which

$$s-c(n, t+1)-\sum_{j=k+1}^{t}\binom{a_j}{j} \geqq \binom{a}{k}.$$

(Note if the left hand side is 0 then $a_k=k-1$). Now define $A_k=\{\sigma\colon |\mathrm{supp}\,(\sigma)|=t$ and $\{1+a_{k+1}, \ldots, 1+a_t\} \subseteqq \mathrm{supp}\,(\sigma) \subseteqq \{1, \ldots, a_k, 1+a_{k+1}, \ldots, 1+a_t\}\}$.

Then we have,

$$B_n^s = C_{n,t+1} \cup A_t \cup \ldots \cup A_1. \tag{3.1}$$

The sequence $\{a_j\}$ constructed above from s is unique and its properties are summarized by the following well known:

Lemma 3.4. *Let n be a fixed positive integer. Then for each integer $s<2^n$ there is a unique sequence $a_n, a_{n-1}, \ldots, a_1$ such that*

(i) $$s = \binom{a_n}{n}+\binom{a_{n-1}}{n-1}+\ldots+\binom{a_1}{1}$$

(ii) $$n \geqq a_n \geqq a_{n-1} \geqq \ldots \geqq a_1 \geqq 0$$

(iii) $$\text{if } a_j \neq n \text{ then } a_j > a_{j-1}.$$

This representation of s will be called the *n-binomial expansion* of s. The proofs of the following two propositions are left to the reader.

Proposition 3.5. *Let $1 \leqq b < a \leqq 2^n$ and let*

$$a = \binom{a_n}{n}+\binom{a_{n-1}}{n-1}+\ldots+\binom{a_1}{1}$$

$$b = \binom{b_n}{n}+\binom{b_{n-1}}{n-1}+\ldots+\binom{b_1}{1}$$

be the n-binomial expansions. Then for any $j \geqq 1$

$$\sum_{i=j}^{n}\binom{a_i}{i} \geqq \sum_{i=j}^{n}\binom{b_i}{i}.$$

Proposition 3.6. *Suppose $s<2^n-1$ and*

$$s = \binom{a_n}{n}+\binom{a_{n-1}}{n-1}+\ldots+\binom{a_1}{1}$$

$$s+1 = \binom{b_n}{n}+\binom{b_{n-1}}{n-1}+\ldots+\binom{b_1}{1}$$

are n-binomial expansions. Let j be the smallest index such that either $a_{j+1}>a_j+1$ or $a_{j+1}=n$. Then $b_i=a_i$, for $i>j$, $b_j=1+a_j$, and $b_i=i-1$ for $i<j$. ∎

Let $s=\binom{a_n}{n}+\binom{a_{n-1}}{n-1}+\ldots+\binom{a_1}{1}$ be the n-binomial expansion of s and consider the set $B_n^s[1]$.

By (3.1),

$$B_n^s[1] = C_{n,t+1}[1] \cup A_t[1] \cup \ldots \cup A_1[1].$$

Now $C_{n,t+1}[1] = C_{n-1,t}$ and $A_j[1] = \{\sigma | \text{supp}(\sigma) = t-1$ and

$$\{a_{j+1}, a_{j+2}, \ldots, a_t\} \subseteq \text{supp}(\sigma) \subseteq \{1, 2, \ldots, a_j - 1, a_{j+1}, a_{j+2}, \ldots, a_t\}\}.$$

Hence

$$|B_n^s[1]| = \binom{a_n - 1}{n-1} + \binom{a_{n-1} - 1}{n-2} + \ldots + \binom{a_2 - 1}{1} + \binom{a_1 - 1}{0}.$$

Note that this is not an n-binomial expansion, because of the $\binom{a_1 - 1}{0}$ term. Observe also that $B_n^s[1]$ is an initial segment of B_{n-1} with respect to the total order that has been defined.

A similar analysis shows that $B_n^s[0]$ is the initial segment of B_{n-1} of cardinality

$$\begin{aligned} |B_n^s[0]| &= \binom{a_n - 1}{n} + \binom{a_{n-1} - 1}{n-1} + \ldots + \binom{a_1 - 1}{1} \\ &= \binom{a_{n-1} - 1}{n-1} + \binom{a_{n-2} - 1}{n-2} + \ldots + \binom{a_1 - 1}{1}, \end{aligned}$$

since $a_n - 1 < n$. This is essentially an $(n-1)$-binomial expansion (unless $a_1 = 0$ in which case we replace $a_1 - 1$ by 0).

Now we define

$$\omega_n(s) = |B_n^s[1]| = \binom{a_n - 1}{n-1} + \binom{a_{n-1} - 1}{n-2} + \ldots + \binom{a_2 - 1}{1} + \chi(a_1 \geqq 1), \tag{3.2}$$

$$\mu_n(s) = |B_n^s[0] = \binom{a_n - 1}{n} + \binom{a_{n-1} - 1}{n-1} + \ldots + \binom{a_2 - 1}{2} + \binom{\max(0, a_1 - 1)}{1}. \tag{3.3}$$

Observe that

$$\begin{aligned} \omega_{n-1}\omega_n(s) &= |B_n^s[11]|, \\ \omega_{n-1}\mu_n(s) &= |B_n^s[01]|, \\ \mu_{n-1}\omega_n(s) &= |B_n^s[10]|, \\ \mu_{n-1}\mu_n(s) &= |B_n^s[00]|, \end{aligned}$$

and for $k \leqq n$,

$$\omega_{n-k+1}\omega_{n-k+2} \ldots \omega_n(s) = B_n^s[1^k].$$

We write $\omega_n^k(s)$ for $\omega_{n-k+1}\omega_{n-k+2} \ldots \omega_n(s)$. We will need the following boring facts.

Proposition 3.7. *Let s be an integer between 1 and $2^n - 1$ with n-binomial expansion $\binom{a_n}{n} + \binom{a_{n-1}}{n-1} + \ldots + \binom{a_1}{1}$. Then*

(i) *The s^{th} string in B_n begins with a 1 if and only if $a_j = j$ where j is the smallest index with $a_j \geqq j$.*

(ii) *The $(s+1)^{\text{th}}$ string in B_n begins with a 1 if and only if $a_1 = 0$; hence $\omega_n(s+1) = \omega_n(s) + \chi(a_1 = 0)$.*

(iii) *The s^{th} string in B_n^s begins with a 10 if and only if $a_1 = 1$.*

(iv) $\mu_{n-1}\omega_n(s) = \omega_{n-1}\mu_n(s) + \chi(a_1 = 1)$.

(v) $\omega_n(s) \geqq \mu_n(s)$.

Proof. (i) In the partition of B_n^s given by (3.1), the s^{th} string is contained in A_j where j is the smallest index with $a_j \geqq j$, since A_i is nonempty if $a_i \geqq i$. The last string in B_n^s is the last string in A_j. By definition of A_j this is the string b with supp $(b)=\{a_j-(j-1), a_j-(j-2), \ldots, a_j, 1+a_{j+1}, 1+a_{j+2}, \ldots, 1+a_t\}$ and hence $1 \in$ supp (b) if and only if $a_j=j$.

(ii) Let $s+1=\binom{b_n}{n}+\binom{b_{n-1}}{n-1}+\ldots+\binom{b_1}{1}$ be the n-binomial representation. By (i), the $(s+1)^{\text{th}}$ string begins with a 1 if and only if $b_j=j$ where j is the smallest index with $b_j \geqq j$. By proposition 3.6, j is the first index such that either $a_{j+1}>a_j+1$ or $a_{j+1}=n$. If $a_1=0$, then the first such index has $a_j=j-1$ so $b_j=j$ and if $a_1 \geqq 1$, the first such index has $a_j \geqq j$ so $b_j \geqq j+1$.

(iii) Let j be the smallest index with $a_j \geqq j$. If $a_j>j$ then by (i), s begins with a 0. If $a_j=j$, then the s^{th} string begins with j 1's and the $j+1^{\text{th}}$ element is 0.

(iv) The successor of 10τ is 01τ. Hence

$$\mu_{n-1}\omega_n(s) = \omega_{n-1}\mu_n(s)+\chi(s^{\text{th}} \text{ string begins } 10)$$
$$= \omega_{n-1}\mu_n(s)+\chi(a_1 = 1),$$

by (iii).

(v) Every string 1τ precedes 0τ in the order.

Lemma 3.8. *For* $0 \leqq k \leqq n$, $v_k(B_n^s)=\omega_n^k(s)/2^{n-k}$.

Proof. By induction on k and $n-k$. If $k=0$, then $v_0(B_n^s)=s/2^n=\omega_n^0(s)/2^n$. If $n-k=0$ then $v_k(B_n^s)=\chi(s>0)=\omega_n^k(s)/2^{n-k}$. For k and $n-k>0$ we have, by Lemma 3.1 and the induction hypothesis:

$$v_k(B_n^s) = \max\{v_{k-1}(B_n^s[1]), v_{k-1}(B_n^s[0]), (v_k(B_n^s[1])+v_k(B_n^s[0]))/2\}$$
$$= \max\{\omega_n^k(s), \omega_{n-1}^{k-1}(\mu_n(s)), \omega_n^{k+1}(s)+\omega_{n-1}^k(\mu_n(s))\}/2^{n-k}.$$

Now by Proposition 3.7 (v) and the fact that ω_{n-1}^{k-1} is a nondecreasing function the first term is at least the second term. By repeated application of Proposition 3.7 (iv), $\omega_{n-1}^k\mu_n(s) \leqq \mu_{n-k}\omega_n^k(s)$. Hence

$$\omega_n^k(s) = \omega_{n-k}(\omega_n^k(s))+\mu_{n-k}(\omega_n^k(s)) \geqq \omega_n^{k+1}(s)+\omega_{n-1}^k\mu_n(s)$$

so $\omega_n^k(s)$ is the largest of the three terms and $v_k(B_n^s)=\omega_n^k(s)/2^{n-k}$. ∎

Proof of Theorem 3.3. Let $s_1=|L[1]|$ $s_0=|L[0]|$ and assume without loss of generality that $s_1 \geqq s_0$. By Lemma 3.8, $v_k(B_n^s)=\omega_n^k(s)/2^{n-k}$, so we need to prove

$$v_k(L) \geqq \omega_n^k(s)/2^{n-k}. \tag{3.4}$$

We proceed by induction on n. For $n=1$, the result is trivial. So let $n>1$ and assume the result holds for $n-1$. Now by Lemma 3.1,

$$v_k(L) = \max\{v_{k-1}(L[1]), v_{k-1}(L[0]), (v_k(L[1])+v_k(L[0]))/2\}.$$

By the induction hypothesis

$$v_{k-1}(L[1]) \geqq \omega_{n-1}^{k-1}(s_1)/2^{n-k}$$
$$v_{k-1}(L[0]) \geqq \omega_{n-1}^{k-1}(s_0)/2^{n-k}$$

and

$$(v_k(L[1])+v_k(L[0]))/2 \geqq (\omega_{n-1}^k(s_1)+\omega_{n-1}^k(s_0))/2^{n-k}.$$

We need to show that one of these three quantities is at least $\omega_n^k(s)/2^{n-k}$. It suffices to prove

Lemma 3.9. *Let n, k, s, s_0 and s_1 be nonnegative integers satisfying:*

(i) $$n \geqq k,$$

(ii) $$2^{n-1} \geqq s_1 \geqq s_0 \geqq 0.$$

(iii) $$s_0+s_1 \geqq s,$$

(iv) $$\omega_{n-1}^{k-1}(s_1) \prec \omega_n^k(s).$$

Then

(3.5) $$\omega_{n-1}^k(s_1)+\omega_{n-1}^k(s_0) \geqq \omega_n^k(s).$$

The statement of this lemma resembles the cascade inequalities of Katona [9] (see also [6]), but we see no way to deduce the lemma from these results. The proof does use similar ideas.

Proof. We proceed by induction on k. The difficult part of the proof is the basis, $k=1$, which we state as a separate lemma.

Lemma 3.10. *Let n, s_0, s_1 and s be integers satisfying $s_0+s_1 \geqq s$, $2^{n-1} \geqq s_1 \geqq s_0 \geqq 0$, and $s_1 < \omega_n(s)$.*

Then

(3.6) $$\omega_{n-1}(s_1)+\omega_{n-1}(s_0) \geqq \omega_n(s).$$

Assuming this for the moment, we prove the induction step of Lemma 3.9. Suppose $k>1$ and that hypotheses (i), (ii), (iii), and (iv) hold for n, k, s, s_0 and s_1. Let $s'=\omega_n(s)$, $s_0'=\omega_{n-1}(s_0)$ and $s_1'=\omega_{n-1}(s_1)$.

Claim. Hypotheses (i), (ii), (iii), and (iv) hold for $n-1$, $k-1$, s', s_0' and s_1'.

It is trivial that (i) holds. By applying the function ω_{n-1} to each term in the inequality (ii) for n, s_1 and s_0 we obtain the corresponding inequality for $n-1$, s_1' and s_0'. To establish (iii), note that by (iv) for n, k, s, s_1 and s_0, $\omega_{n-1}^{k-1}(s_1) < \omega_k^n(s) = \omega_{n-1}^{k-1}(\omega_n(s))$ so by the monotonicity of ω, $\omega_n(s) > s_1$. Thus n, s, s_1, s_0 satisfy the hypotheses of Lemmas 3.10 and we conclude $\omega_{n-1}(s_1)+\omega_{n-1}(s_0) \geqq \omega_n(s)$. Finally, for (iv) we have $\omega_{n-2}^{k-2}(s_1)=\omega_{n-1}^{k-1}(s_1) < \omega_n^k(s)=\omega_{n-1}^{k-1}(s')$.

By the claim and the induction hypothesis we conclude:

$$\omega_{n-1}^{k-1}(s_1')+\omega_{n-2}^{k-2}(s_0') \geqq \omega_{n-1}^{k-1}(s')$$

which is equivalent to

$$\omega_{n-1}^k(s_1)+\omega_{n-1}^k(s_0) \geqq \omega_n^k(s),$$

as required to prove Lemma 3.9. Thus it remains to prove the basis case, Lemma 3.10.

Proof of Lemma 3.10. By the monotonicity of ω we may assume that $s_0=s-s_1$. Let $s=\binom{a_n}{n}+\binom{a_{n-1}}{n-1}+\ldots+\binom{a_1}{1}$ be the n-binomial expansion. We proceed by in-

duction on s_0. The basis for the induction is $s_0=\mu_n(s)+1$ and $s_1=\omega_n(s)-1$. We must show

$$\omega_{n-1}(\mu_n(s)+1)+\omega_{n-1}(\omega_n(s)-1) \geqq \omega_n(s).$$

Now,

$$\begin{aligned}\omega_n(s) &= \mu_{n-1}(\omega_n(s))+\omega_{n-1}(\omega_n(s)) \\ &= \omega_{n-1}(\mu_n(s))+\omega_{n-1}(\omega_n(s))+\chi(a_1=1)\end{aligned}$$

by Proposition 3.7 (iv). So it is enough to show

$$\omega_{n-1}(\mu_n(s)+1)+\omega_{n-1}(\omega_n(s)-1) \geqq \omega_{n-1}(\mu_n(s))+\omega_{n-1}(\omega_n(s))+\chi(a_1=1). \tag{3.7}$$

As noted in (3.3), the n-binomial expansion of $\mu_n(s)$ is

$$\mu_n(s)=\binom{a_{n-1}-1}{n-1}+\binom{a_{n-2}-1}{n-2}+\ldots+\binom{a_2-1}{2}+\binom{\max(a_1-1,0)}{1}$$

so by Proposition 3.7 (ii),

$$\omega_{n-1}(\mu_n(s)+1)-\omega_{n-1}(\mu_n(s))=\chi(a_1=0)+\chi(a_1=1).$$

If $a_1=0$ then since $\omega_{n-1}(\omega_n(s)-1)\geqq\omega_{n-1}(\omega_n(s))-1$, (3.7) holds. If $a_1\geqq 1$, then (3.2) gives

$$\omega_n(s)-1=\binom{a_n-1}{n-1}+\binom{a_{n-1}-1}{n-2}+\ldots+\binom{a_2-1}{1}$$

and since $a_2>a_1$ we have $a_2-1\geqq 1$, so Proposition 3.7 (ii) gives $\omega_{n-1}(\omega_n(s))=$ $=\omega_{n-1}(\omega_n(s)-1)$ and again (3.7) holds, proving the basis step.

Now for the induction step. We may assume

$$\mu_n(s)+1 < s_0 \leqq s_1 < \omega_n(s)-1.$$

Let

$$s_1=\binom{b_{n-1}}{n-1}+\binom{b_{n-2}}{n-2}+\ldots+\binom{b_1}{1}$$

$$s_0=\binom{c_{n-1}}{n-1}+\binom{c_{n-2}}{n-2}+\ldots+\binom{c_1}{1}$$

be n-binomial expansions. If $\omega_{n-1}(s_0-1)+\omega_{n-1}(s_1+1)\leqq\omega_{n-1}(s_0)+\omega_{n-1}(s_1)$, then we can apply the induction hypothesis to prove (3.6). Hence assume $\omega_{n-1}(s_0-1)+$ $+\omega_{n-1}(s_1+1)>\omega_{n-1}(s_0)+\omega_{n-1}(s_1)$. Then the s_0^{th} string of B_{n-1} must begin with a 0 and the $(s_1+1)^{\text{th}}$ string of B_{n-1} begins with a 1. By Proposition 3.7 (i) and (ii), $b_1=0$ and $c_i\neq i$ for all $i<n$.

Case i. $c_1>0$. Let j be the largest index such that $c_j>b_j$. Define

$$s_1'=\binom{b_{n-1}}{n-1}+\binom{b_{n-2}}{n-2}+\ldots+\binom{b_{j+1}}{j+1}+\binom{c_j}{j}+\ldots+\binom{c_1}{1}$$

$$s_0'=\binom{c_{n-1}}{n-1}+\binom{c_{n-2}}{n-2}+\ldots+\binom{c_{j+1}}{j+1}+\binom{b_j}{j}+\ldots+\binom{b_1}{1}.$$

Then these are n-binomial expansions and $s_1'>s_1$, $s_0>s_0'$. We also claim that $s_0'>\mu_n(s)$. Let k be the largest index such that $c_k\neq a_k-1$. Then $c_k>a_k-1$ since otherwise

Proposition 3.5 would imply $s_0 < \mu_n(s)$. If $k > j$ then Proposition 3.5 implies $s_0' > \mu_n(s)$ as required, so assume $c_i = a_i - 1$ for all $i > j$. Since $c_j < c_{j+1}$, we have $c_j < a_{j+1} - 1$. Now $\binom{c_1}{1} + \ldots + \binom{c_j}{j} < \binom{c_j+1}{j} \leqq \binom{a_{j+1}-1}{j}$. Also since $s_1 < \omega_n(s)$ then by Proposition 3.5,

$$\binom{b_{n-1}}{n-1} + \ldots + \binom{b_{j+1}}{j+1} \leqq \binom{a_n-1}{n-1} + \ldots + \binom{a_{j+2}-1}{j+1}$$

so

$$s_1' < \binom{a_n-1}{n-1} + \ldots + \binom{a_{j+2}-1}{j+1} + \binom{a_{j+1}-1}{j} \leqq \omega_n(s),$$

which implies $s_0' > \mu_n(s)$ as claimed. Now apply induction to get

$$\omega_n(s) \leqq \omega_n(s_1') + \omega_n(s_0') = \omega_n(s_1) + \omega_n(s_0).$$

Case ii. $c_1 = 0$. Let j be the first index such that $c_j > j - 1$. Since $c_j \neq j$, we have $c_j \geqq j + 1$. Then

$$1 + \mu_n(s) < s_0 = \binom{c_{n-1}}{n-1} + \binom{c_{n-2}}{n-2} + \ldots + \binom{c_j}{j}.$$

Subcase a. $s_0 - \mu_n(s) \leqq \binom{c_{j-1}}{j-1}$. Then

$$\mu_n(s) \geqq \binom{c_{n-1}}{n-1} + \binom{c_{n-2}}{n-2} + \ldots + \binom{c_j}{j} - \binom{c_j-1}{j-1}$$

$$= \binom{c_{n-1}}{n-1} + \binom{c_{n-2}}{n-2} + \ldots + \binom{c_{j+1}}{j+1} + \binom{c_j-1}{j}$$

and we must have $c_i = a_i - 1$ for $i > j$ and $c_j = a_j$.

Thus

$$s_0 = \binom{a_{n-1}-1}{n-1} + \binom{a_{n-2}-1}{n-2} + \ldots + \binom{a_{j+1}-1}{j+1} + \binom{a_j}{j}.$$

Now

$$s_1 = s - s_0 = \binom{a_n}{n} + \ldots + \binom{a_{j+1}}{j+1} + \binom{a_j}{j} + \binom{a_{j-1}}{j-1} + \ldots + \binom{a_1}{1}$$

$$- \left(\binom{a_{n-1}-1}{n-1} + \binom{a_{n-2}-1}{n-2} + \ldots + \binom{a_{j+1}-1}{j+1} + \binom{a_j}{j} \right)$$

$$= \binom{a_n}{n} + \binom{a_{n-1}-1}{n-2} + \ldots + \binom{a_{j+1}-1}{j} + \binom{a_{j-1}}{j-1} + \ldots + \binom{a_1}{1}$$

$$= \binom{a_n-1}{n-1} + \binom{a_{n-1}-1}{n-2} + \ldots + \binom{a_{j+1}-1}{j} + \binom{a_{j-1}}{j-1} + \ldots + \binom{a_1}{1}$$

since $a_n = n$. Note this is a valid $(n-1)$-binomial expansion so by (3.2) and the binomial recurrence

$$\omega_{n-1}(s_0) + \omega_{n-1}(s_1) = \omega_n(s).$$

Subcase b. $s_0-\mu_n(s)>\binom{c_j-1}{j-1}$. Then let h be the smallest index such that $c_j-h>b_{j-h}$ (this holds or $h=j-1$) and define

$$s_0' = \binom{c_{n-1}}{n-1}+\cdots+\binom{c_{j+1}}{j+1}+\binom{c_j-1}{j}+\binom{c_j-2}{j-1}+\cdots+\binom{c_j-h}{j-h+1}+\binom{b_{j-h}}{j-h}+\cdots+\binom{b_1}{1}$$

$$s_1' = \binom{b_{n-1}}{n-1}+\cdots+\binom{b_{j-h+1}}{j-h+1}+\binom{c_j-h}{j-h}.$$

Then $s_0'+s_1'=s$, and

$$\mu_n(s) < s_0-\binom{c_j-h}{j-h} \leqq s_0' < s_0$$

so we may apply induction to obtain

$$\omega_{n-1}(s_0')+\omega_{n-1}(s_1') \geqq \omega_n(s).$$

Now the expressions for s_0' and s_1' above are $(n-1)$-binomial expansions. Applying (3.2) the binomial recurrence and the previous inequality yields

$$\omega_{n-1}(s_0)+\omega_{n-1}(s_1) = \omega_{n-1}(s_0')+\omega_{n-1}(s_1') \geqq \omega_n(s). \quad \blacksquare$$

This concludes the Proof of Lemma 3.10, which in turn completes the Proof of Lemma 3.9 and Theorem 3.3.

We conclude this section by noting an upper bound on $v_k(L)$.

Proposition 3.11. *For any language L in B_n, $v_k(L)\leqq|L|/2^{n-k}$.*

Proof. By induction on k. For $k=0$, the inequality is an equality by definition. For $k>0$, Proposition 3.1 and the induction hypothesis yield,

$$\begin{aligned} v_k(L) &= \max\{v_{k-1}(L[0]),\, v_{k-1}(L[1]),\, (v_k(L[0])+v_k(L[1]))/2\} \\ &\leqq \max\{|L[0]|/2^k,\, |L[1]|/2^{n-k},\, (|L[0]|+|L[1]|)/2^{n-k}\} \\ &= |L|/2^{n-k}. \quad \blacksquare \end{aligned}$$

4. The expected number of interventions needed to guarantee success

Let L be a language and consider strategies that guarantee that the string σ produced is in L. For a strategy s, let $e(L, s)$ be the expected number of interventions that occur when running strategy s. Let $e(L)$ be the minimum of $e(L, s)$ over all strategies s. In this section we find the maximum of $e(L)$ given $|L|$.

We begin with a simple inductive characterization of $e(L)$:

Lemma 4.1. *Let L be a language in B_n. Then*

$$e(L) = \min\{1+e(L[1]),\, 1+e(L[0]),\, (e(L[1])+e(L[0]))/2\}.$$

Proof. The three terms in the minimum correspond to the three choices at the first step: force a 1, force a 0, or don't intervene. $\blacksquare$

Let $d(n, t)$ denote 2^n minus the sum of the largest t binomial coefficients, i.e.

$$d(n, t) = 2^n - \sum_{j=[(n-t+1)/2]}^{[(n+t-1)/2]} \binom{n}{j}.$$

We need the following result, which can be proved easily by induction:

Proposition 4.2. *$d(n, t)$ is the unique solution of the recurrence*

$$f(n, t) = f(n-1, t-1)+f(n-1, t+1) \quad n > t \geqq 1$$

with the initial conditions

$$f(n, 0) = 2^n$$

$$f(n, n) = 1$$

$$f(n, n+1) = 0.$$

The main result of this section is:

Theorem 4.3. *Let L be a language in B_n. If $|L| \geqq d(n, t)$ then $e(L) \leqq t$. Furthermore, for each n and t there is a language $D_{n,t}$ with $|D_{n,t}| = d(n, t)$ and $e(D_{n,t}) = t$.*

Proof. For positive integers n and real numbers t, $0 \leqq t \leqq n+1$, define

$$\psi(n, t) = \begin{cases} \max(|L|: L \subseteq B_n, e(L) \geqq t) & \text{if } t \leqq n \\ 0 & \text{if } t > n \end{cases}.$$

It is easy to see that $\psi(n, t)$ is a nonincreasing function of t and $\psi(n, 0)=2^n$, $\psi(n, n)=1$ and $\psi(n, n+1)=0$. We will show that for integers $t \geqq 0$

$$\psi(n, t) = d(n, t)$$

from which the theorem follows.

We first show that $\psi(n, t) \geqq d(n, t)$ by constructing the family of languages $D_{n,t}$ in B_n promised by the theorem. Define $D_{n,0}=B_n$, $D_{n,n}=\{1^n\}$, and $D_{n,n+1}=\emptyset$. For $1 \leqq t \leqq n$, defined $D_{n,t}$ inductively by

$$D_{n,t}[1] = D_{n-1,t+1},$$

$$D_{n,t}[0] = D_{n-1,t-1}.$$

Then $|D_{n,t}|$ satisfies the recurrence in Proposition 4.2 so $|D_{n,t}| = d(n, t)$. To show $e(D_{n,t})=t$ we proceed by induction on n. The basis, $n=1$ is immediate. The induction step follows from Lemma 4.1, which yields $e(D_{n,t})=\min\{t+2, t, t\}=t$.

$D_{n,t}$ has the following explicit description: a string b is in $D_{n,t}$ if and only if for some initial segment of b the number of 1's exceeds the number of 0's by at least t.

Next we want to show that $\psi(n, t) \leqq d(n, t)$. By Proposition 4.2, it would suffice to show that

$$\psi(n, t) \leqq \psi(n-1, t+1)+\psi(n-1, t-1)$$

holds for all integers t with $1 \leqq t \leqq n$. We begin with a weaker inequality.

Lemma 4.4. *For all real t such that $0 \leqq t \leqq n$,*

$$\psi(n, t) \leqq \max_{0 \leqq u \leqq \min(t,1)} \psi(n-1, t+u)+\psi(n-1, t-u).$$

Proof. Let L be a language in B_n with $e(L) \geqq t$ and $|L|$ maximum. Then

$$\psi(n, t) = |L| = |L[1]|+|L[0]| \tag{4.1}$$
$$\leqq \psi(n-1, e(L[1]))+\psi(n-1, e(L[0]))$$

by definition of ψ. By Lemma 4.1,

$$t = e(L) = \min\{1+e(L[1]), 1+e(L[0]), e(L[0])+e(L[1])\}$$

and so,

$$e(L[1]) \geqq t-1,$$
$$e(L[0]) \geqq t-1,$$
$$e(L[0])+e(L[1]) \geqq 2t.$$

Assuming, without loss of generality, $e(L[1]) \geqq t$, and setting $e(L[1])=t+v$, $e(L[0])=t-u$ we have $u \leqq \min(1, t, v)$. Hence by (4.1)

$$\psi(n, t) \leqq \psi(n-1, t+v)+\psi(n-1, t-u)$$
$$\leqq \psi(n-1, t+u)+\psi(n-1, t-u)$$

for some $0 \leqq u \leqq \min(1, t)$. ∎

Now $\psi(n, t) \leqq d(n, t)$ would follow from Lemma 4.4 and Proposition 4.2, if we can show that for integral t, $\psi(n-1, t+u)+\psi(n-1, t-u)$ is maximized for $0 \leqq u \leqq 1$ by $u=1$. To do this it would be enough to show that, for fixed n, $\psi(n, t)$ is a convex function t. This, however, is not true. To get around this we introduce the function $\hat{\psi}(n, t)$ to be equal to $\psi(n, t)$ if t is an integer and to be piecewise linear on each interval $[t, t+1]$ for fixed n. Precisely

$$\hat{\psi}(n, t) = \psi(n, \lfloor t \rfloor)(\lceil t \rceil - t)+\psi(n, \lceil t \rceil)(t-\lfloor t \rfloor)$$

where $\lfloor t \rfloor$ denotes the greatest integer $\leqq t$ and $\lceil t \rceil$ denotes the least integer $\geqq t$.

We now complete the Proof of Theorem 4.3 by using induction on n to prove

Lemma 4.5.

(i) $\psi(n, t)=d(n, t)$ *for all integers* $1 \leqq t \leqq n$

(ii) $\psi(n, t) \leqq \hat{\psi}(n, t)$ *for all real* t, $0 \leqq t \leqq n+1$

(iii) $\hat{\psi}(n, t)$ *is a convex function of* t, *i.e.*, $\hat{\psi}(n, t+u)+\hat{\psi}(n, t-u)$ *is a non-decreasing function of* u *for* $0 \leqq u \leqq t$.

Proof. By induction on n. For $n=1$,

$$\psi(1, t) = \begin{cases} 2 & \text{if} \quad t = 0 \\ 1 & \text{if} \quad 0 < t \leqq 1 \\ 0 & \text{if} \quad 1 < t \leqq 2 \end{cases}$$

so (i) holds. Also $\hat{\psi}(1, t)=2-t$ for $0 \leqq t \leqq 2$ so (ii) and (iii) hold.

Now assume $n>1$ and that (i), (ii) and (iii) hold for $n-1$. By Lemma 4.4, and (ii) and (iii) for $n-1$, we have that for $1\leqq t\leqq n$

$$\begin{aligned}(4.2)\qquad \psi(n,t) &\leqq \max_{0\leqq u\leqq 1}\psi(n-1,t+u)+\psi(n-1,t-u)\\ &\leqq \max_{0\leqq u\leqq 1}\hat{\psi}(n-1,t+u)+\hat{\psi}(n-1,t-u)\\ &=\hat{\psi}(n-1,t+1)+\hat{\psi}(n-1,t-1).\end{aligned}$$

If t is an integer then by definition of $\hat{\psi}$ and (i) for $n=1$ we get

$$\psi(n,t)\geqq d(n-1,t+1)+d(n-1,t-1).$$

Since we have already established $\psi(n,t)\leqq d(n,t)$, Proposition 4.2 yields $\psi(n,t)=d(n,t)$, establishing (i).

To prove (ii), we need to consider two cases.

Case a. $0\leqq t\leqq 1$. Then

$$\begin{aligned}\hat{\psi}(n,t) &= (1-t)\hat{\psi}(n,0)+t\hat{\psi}(n,1)\\ &= (1-t)2^n+t\psi(n,1)=(1-t)2^n+td(n,1)\\ &= 2^n+t\binom{n}{\lfloor n/2\rfloor}\end{aligned}$$

and

$$\begin{aligned}\psi(n,t) &\leqq \max_{0\leqq u\leqq t}\psi(n-1,t-u)+\psi(n-1,t+u)\\ &\leqq \max_{0\leqq u\leqq t}\hat{\psi}(n-1,t-u)+\hat{\psi}(n-1,t+u)\\ &=\hat{\psi}(n-1,0)+\hat{\psi}(n-1,2t)\\ &=2^{n-1}+\hat{\psi}(n-1,2t).\end{aligned}$$

If $t\leqq 1/2$ then $2^{n-1}\leqq(1-t)2^n$ and $\hat{\psi}(n-1,2t)=2t\hat{\psi}(n-1,1)=2td(n-1,1)$ which is less than or equal to $td(n,1)$ when $n\geqq 2$. If $1/2<t\leqq 1$, then

$$\begin{aligned}2^{n-1}+\hat{\psi}(n-1,2t) &= 2^{n-1}+(2-2t)\hat{\psi}(n-1,1)+(2t-1)\hat{\psi}(n-1,2)\\ &= 2^{n-1}+(2-2t)d(n-1,1)+(2t-1)d(n-1,2)\\ &= 2^n-2t\binom{n-1}{\lfloor n/2\rfloor-1}\\ &= 2^n-t\binom{n}{\lfloor n/2\rfloor}\end{aligned}$$

which is less than or equal to $\hat{\psi}(n,t)$.

Case b. $1 \leqq t \leqq n$. Let $a = \lfloor t \rfloor$ and write $t = a + \lambda$. Then by (i) for n,

$$\begin{aligned}\hat{\psi}(n, a+\lambda) &= (1-\lambda)\hat{\psi}(n, a) + \lambda\hat{\psi}(n, a+1) \\ &= (1-\lambda)d(n, a) + \lambda d(n, a+1)\end{aligned}$$

while by (4.2) (i) for $n-1$, and Proposition 4.2,

$$\begin{aligned}\psi(n, a+\lambda) &\leqq \hat{\psi}(n-1, a+\lambda-1) + \hat{\psi}(n-1, a+\lambda+1) \\ &= (1-\lambda)\hat{\psi}(n-1, a-1) + \lambda\hat{\psi}(n-1, a) \\ &\qquad + (1-\lambda)\hat{\psi}(n-1, a+1) + \lambda\hat{\psi}(n-1, a+2) \\ &= (1-\lambda)\big(d(n-1, a-1) + d(n-1, a+1)\big) \\ &\qquad + \lambda\big(d(n-1, a) + d(n-1, a+1)\big) \\ &= (1-\lambda)d(n, a) + \lambda d(n, a+1),\end{aligned}$$

establishing (ii) in this case.

Finally to show that $\hat{\psi}(n, t)$ is convex it is enough (by piecewise linearity between integers) to show $\hat{\psi}(n, t-1) + \hat{\psi}(n, t+1) \geqq 2\hat{\psi}(n, t)$ for integral $1 \leqq t \leqq n$. By (i), this is equivalent to

$$d(n, t-1) + d(n, t+1) \geqq 2d(n, t)$$

or

$$d(n, t-1) - d(n, t) \geqq d(n, t) - d(n, t+1)$$

which is obvious from the definition of $d(n, t)$. ∎

5. Random languages

In the previous sections we obtained tight bounds on the quantities $v_k(L)$ and $e(L)$ for arbitrary languages. The bounds are "worst case" in the sense that they hold for any language. In this section we investigate the behavior of $v_k(L)$ and $e(L)$ for random languages in B_n. We consider the distribution on languages of B_n which for fixed p independently assigns each string b to L with probability p. We denote this distribution by $RL(n; p)$. If L is chosen from $RL(n; p)$ we write $L \sim RL(n; p)$ and say L is *random with parameter p*.

We define $E(n, p)$ to be the expected value of $e(L)$ where $L \sim RL(n; p)$.

Theorem 5.1. *For integers* $n \geqq 1$ *and* $0 \leqq p \leqq 1$

$$E(n, p) \leqq 2(1-p)/p,$$

and there exists an $e(n) > 0$ *such that for* $0 < p < e(n)$,

$$E(n, p) \leqq \log 1/p.$$

Proof. Let L be a random language in B_n with parameter p. With probability $(1-p)^{2^n}$, L is empty and so $e(L)$ is, by definition, $n+1$. So we consider random languages subject to L being nonempty and analyze the strategy that intervenes at a step only if one of the possible outcomes guarantees a failure.

Let $E'(n,p)$ be the expected number of interventions using this strategy on a random language L conditioned on L nonempty. Now the probability of intervention at step 1 is equal to

$$\begin{aligned}&\text{prob}\{L[1]=\emptyset \text{ or } L[0]=\emptyset \mid L\neq\emptyset\}\\&=2(1-p)^{2^{n-1}}(1-(1-p)^{2^{n-1}})/(1-(1-p)^{2^n})\\&=2(1-p)^{2^{n-1}}/(1+(1-p)^{2^{n-1}}).\end{aligned}$$

Whether or not an intervention occurs, the problem is reduced to a random nonempty language in B_{n-1}. Hence

$$E'(n,p)=E'(n-1,p)+2(1-p)^{2^{n-1}}/(1+(1-p)^{2^{n-1}})$$

$$E'(n,p)=2\sum_{i=1}^{n}(1-p)^{2^{i-1}}/(1+(1-p)^{2^{i-1}}).$$

From this we obtain

$$E(n,p)=(1-p)^{2^n}(n+1)+(1-(1-p)^{2^n})2\sum_{i=1}^{n}(1-p)^{2^{i-1}}/(1+(1-p)^{2^{i-1}}).$$

The bounds in the theorem are obtained from this by routine analytic estimates. ∎

Next we want to investigate $V_k(n,p)$, defined to be the expected value of $v_k(L)$ where $L\sim RL(n;p)$. Since we can always choose not to intervene at step 1 we have

$$V_k(n,p)\geqq V_k(n-1,p).$$

Thus, $V_k(n,p)$ is monotone and bounded as a function of n so $\lim_{n\to\infty} V_k(n,p)$ exists; call it $V_k^*(p)$. We will prove:

Theorem 5.2. *For all* $p<1$ *and* $k\geqq 0$, $V_k^*(p)<1$.

In other words, a bounded number of interventions is not enough to almost surely produce a success.

On the other hand, since $V_k(n,p)\geqq 1-(1-p)^k$ (using the strategy that intervenes in the last k steps), if $k(n)$ is any function that goes to infinity with n then $\lim_{n\to\infty} V_{k(n)}(n,p)=1$.

Lemma 5.3. *For any* k *and* p,

$$V_k^*(p)\leqq p2^k.$$

Proof. We show that for all n, $V_k(n,p)\leqq p2^k$. $V_k(n,p)$ is the expected value of $V_k(n,p)$ where L is chosen from $RL(n;p)$. Now by Proposition 3.11 $E(v_k(L))\leqq E(|L|/2^{n-k})=$ $=p2^k$. ∎

Proof of Theorem 5.2. Let $h(L)$ be the minimum number of interventions that guarantee a success. Let $\alpha(n,k,p)$ be the probability that $h(L)\leqq k$ if $L\sim RL(n;p)$. Trivially $\alpha(n,0,p)=p^{2^n}$ and $\alpha(n,n,p)=1-(1-p)^{2^n}$. The result we want follows from two lemmas.

Lemma 5.4. *For any* $n \geqq m \geqq k \geqq 0$ *and* $0 \leqq p \leqq 1$,

$$V_k(n, p) \leqq 1-(1-2^k\alpha(m, k, p))2^{-m}.$$

Lemma 5.5. *For fixed* k *and* $p<1$,

$$\lim_{n\to\infty} \alpha(n, k, p) = 0.$$

To deduce the theorem, note that Lemma 5.5 implies that we can find m such that $\alpha(m, k, p)<2^{-k}$. Then Lemma 5.4 implies that for any $n \geqq m$, $V_k(n, p)$ is bounded away from 1, so $V^*(n, p)<1$.

It remains to prove the lemmas.

Proof of Lemma 5.4. Let L be a language in B_n and consider $L' \subseteq B_{n-m}$ with $L' = \{\sigma \in B_{n-m} | h(L[\sigma]) \leqq k\}$, i.e., σ is in L' if, starting from σ, a string of L can be forced using at most k interventions. If L is random with parameter p, then L' is random with parameter $\alpha(m, k, p)$. By Lemma 5.2, the probability of producing a string in L' using k interventions is at most $2^k\alpha(m, k, p)$. Hence with probability at least $1-2^k\alpha(m, k, p)$, the first $n-m$ bits yield a string not in L' which means that in the last m bits there is a nonzero probability of producing a string not in L even with k interventions. This probability must be at least 2^{-m}. Thus

$$V_k(n, p) \leqq 1-(1-2^k\alpha(m, k, p))2^{-m}$$

as required. ∎

Proof of Lemma 5.5. We first obtain a recurrence for $\alpha(n, k, p)$. Success for L is guaranteed by k interventions if and only if $k-1$ interventions guarantee success for either of $L[1]$ and $L[0]$ or k interventions guarantee success for both of them. Thus

$$\alpha(n, k, p) = \alpha(n-1, k, p)^2+2\alpha(n-1, k-1, p)(1-\alpha(n-1, k, p)).$$

Now we show that $\alpha(n, k, p)\to 0$ as $n\to\infty$ by induction on k. For $k=0$, $\alpha(n, 0, p)=p^{2^n}$ which tends to 0. Now let $k>0$. By induction, for any $\varepsilon>0$ there is an index $n(k-1, \varepsilon)$ such that $\alpha(n, k-1, p) \leqq \varepsilon$ for $n \geqq n(k-1, \varepsilon)$. So for $n-1 \geqq n(k-1, \varepsilon)$ we have

$$\alpha(n, k, p) \leqq \alpha(n-1, k, p)^2+2\varepsilon(1-\alpha(n-1, k, p)). \tag{5.1}$$

Let $\beta(n, k, p)=1-\alpha(n, k, p)$ then we get that for $n \geqq n(k-1, \varepsilon)$,

$$\beta(n, k, p) \geqq (2-2\varepsilon-\beta(n-1, k, p))\beta(n-1, k, p).$$

Now if $\beta(n-1, k, p) \leqq 1-3\varepsilon$ then for $n>n(k-1, \varepsilon)$

$$\beta(n, k, p) \geqq (1+\varepsilon)\beta(n-1, k, p)$$

so since $\beta(n(k-1, \varepsilon), k, p)>0$, eventually $\beta(n, k, p) \geqq 1-3\varepsilon$, i.e., $\alpha(n, k, p) \leqq 3\varepsilon$. Once this happens, then (5.1), implies that for $\varepsilon<1/9$ that $\alpha(n, k, p)$ stays below 3ε. Since ε can be taken arbitrarily small, this shows that $\lim_{n\to\infty} \alpha(n, k, p)=0$. ∎

6. An open problem on generalized influence strategies

We conclude this paper with a discussion of a generalization of the influence strategies studied above. We have assumed a model where the value of an influenced bit is completely determined by the player. More generally, we can look at strategies where the player can only impart a limited amount of bias to the influenced bits, i.e. influencing a bit towards 1 increases the probability of a 1 to $1/2+\varepsilon$. This more general influence process is specified by a triple (L, s, ε) where L is a language, s a strategy and ε a fixed number indicating the bias of each influenced bit. (The case we have considered is $\varepsilon=1/2$, which we call a *pure influence process.*) We define $\mathrm{val}(L, S, \varepsilon)$ to be the probability that the process produces a word in L.

It is natural to ask if the results of Section 3 generalize to partial influence processes. Let $v_k(L, \varepsilon)$ be the maximum of $\mathrm{val}(L, s, \varepsilon)$ over k-bounded strategies s. We have seen that for $\varepsilon=1/2$ and any k, the "hardest" languages to influence are threshold languages and the "easiest" are languages where membership is decided by a small number of bits.

First of all it is easy to show that for any 1-bounded strategy.

$$\mathrm{val}(L, s, \varepsilon) = |L|+2\varepsilon(\mathrm{val}(L, s)-|L|)$$

and hence the value of the optimal 1-bounded strategy is linearly related to ε. Hence the results of Section 3 for $k=1$ generalize to the case of arbitrary ε.

However the results of Section 3 do not generalize when $k>1$. Consider the case $j=n$. Then the model is equivalent to the slightly random source introduced in [11]. Suppose, for example, that $|L|=2^{n-1}$. Then for any constant $\varepsilon>0$, since we can bias each toss by ε we can virtually guarantee success if L is a threshold language. In fact, it was observed in [1] that threshold languages are the easiest to influence in this case. If $L=B_n$[1], our influence is still limited to $1/2+\varepsilon$ since only the outcome of the first bit matters, and [11] prove that this is the hardest language to influence. Hence for small ε, the hardest language to influence for $k=1$ becomes the easiest for $k=n$ and vice versa!

We do not know what languages are the hardest to influence when ε is small and k is somewhere between 1 and n and it would be interesting to understand how the transition that occurs.

Acknowledgement. We thank Noga Alon for useful discussions regarding Theorem 5.2, and a referee for helpful suggestions.

References

[1] N. ALON and M. O. RABIN, On the random properties of a weakly random source, in Advances in Computing Research (Silvio Micali, ed.), *to appear.*

[2] M. BEN-OR and N. LINIAL, Collective Coin Flipping, robust voting schemes and minimal of Banzhaf values, *Proceedings of the 26th Annual IEEE Symposium on Foundations of Computer Science,* 1985, 408—416.

[3] M. BEN-OR, N. LINIAL and M. SAKS, Collective collective coin flipping and other models of imperfect randomness, Proceedings of edi.

[4] B. CHOR and O. GOLDREICH, Unbiased bits from sources of weak randomness and probabilistic communication complexity, *Proceedings of the 26th Annual IEEE Symposium on Foundations of Computer Science,* 1985, 429—442.

[5] B. CHOR, O. GOLDREICH, J. HASTAD, J. FRIEDMANN, S. RUDICH and R. SMOLENSKY, The bit extraction problem or t-resilient functions, *Proc. 26th IEEE Symposium on Foundations of Computer Science* (1985), 396—407.
[6] D. E. DAYKIN, Ordered ranked posets, representations of integers and inequalities from extremal ranked posets, *in Graphs and Order (I. Rival, ed.), D. Reidel Publishing*, 1985, 395—412.
[7] C. GREENE and D. J. KLEITMAN, Proof techniques in the theory of finite sets, *in Studies in Combinatorics* (G.-C. Rota, ed.), MAA Studies in Mathematics, **17** (1978), 22—79.
[8] L. HARPER, Optimal numberings and isoperimetric problems on graphs, *J. Comb. Th.*, **1** (1966), 385—393.
[9] G. KATONA, A theorem for finite sets, in *Theory of Graphs* (P. Erdős and G. Katona, eds.), Hungarian Academy of Science, Budapest, 1966, 187—207.
[10] J. B. KRUSKAL, The number of simplices in a complex, in *Mathematical Optimization Techniques* (R. Bellman, ed.), University of California Press, Berkeley, 1963, 251—278.
[11] M. SANTHA and U. V. VAZIRANI, Generating quasi random sequences from slightly random sources, *J. Comp. Sys. Sci.*, **33** (1986), 75—87.
[12] U. V. VAZIRANI, Towards a strong communication complexity theory or generating quasi-random sequences from two communicating slightly-random sources, *Combinatorica*, **7** (1987), 375—392.
[13] U. V. VAZIRANI, Randomness, Adversaries and Computation, *Ph. D. dissertation*, U. C. Berkeley, 1986.
[14] U. V. VAZIRANI and V. V. VAZIRANI, Random polynomial time is equal to semi-random polynomial time, *Proc. 26th IEEE Symp. on Foundations of Computer Science* (1985), 417—428.

D. Lichtenstein

Bell Laboratories
Holmdel, NJ 07733
U. S. A.

N. Linial

Department of Computer Science
Hebrew University
Givat Ram, Jerusalem, Israel

M. Saks

Department of Computer Science and Engineering
University of California at San Diego
La Jolla, Calif. 92122
U. S. A.