New Lower Bounds for Median and Related Problems*

by

Chee-Keng Yap

Research Report #79

October 1976

This research was supported in part by the National Science Foundation under grant MCS-76-05744

*The results of this paper were announced at the Symposium on Algorithms and Complexity: New Directions and Recent Results, Carnegie-Mellon University, Pittsburgh, Pa. April 1976.

1. Introduction

One of the most widely studied problems in concrete complexity is the i-th Selection Problem [1,2,3,4,5,7,14,15]. In the problem, we are given a set of N elements which has an implicit total ordering, and we are to find the i-th largest element using only binary comparisons on the input elements. The important special case is when i = N/2, i.e., we want to find the median. We study the complexity in terms of the worst case number of comparisons. The Median Problem is the "hardest Selection Problem" in the sense that if the Median Problem has complexity $f(N) \geq N$, then finding the i-th largest element also has complexity $O(f(N))$. Efficient algorithms for the Median Problem find applications in many computational problems including sorting, minimum spanning tree [13] and geometry problems [12].

Surprisingly, the complexity of the Median Problem was found to be linear [1], closing off speculations that it may be $O(N\log N)$. Since then a very sophisticated algorithm had been developed which gives a 3N upper bound [6]. On lower bounds, no substantial progress had been made since Pratt and Yao [7] gave a lower bound of $7N/4-\log N-O(1)$. However, Schonhage [10] and Kirkpatrick [4] both gave independent simplified proofs of the slightly better bound of $7N/4$. It turns out that their independent formulations are essentially the same.

In this paper we present a general scheme for an Adversary Proof for the Median Problem. The basic concepts of the Adversary are as in [1] and [7]. We imagine a game played between the Adversary and the Algorithm. We call an Adversary in our scheme a State-Transition

Adversary. We illustrate our approach with a simple State-Transition version of the Kirkpatrick-Schonhage Adversary. A number of new techniques are used. The idea of state-claims and safe-boxes enable us to "remember" previous comparisons. Using color classes we are able to avoid a combinatorial explosion. It is implicit in previous proofs that the Adversaries have the property of Bounded Unbalance. We find sufficient conditions that allow our Adversary to violate the bounded unbalance constraint and still have a good lower bound. It is a kind of Church-Rosser Property of the Adversary that says that "if at any time during the game, property P is true, then we are guaranteed that at the end of the game, property P will be true." Note that during the intermediate stages of a game, property P need not hold. Here P is the property of having "bounded unbalance." All these ideas combine to give us the best known bound lower bound of 11N/6 for the Median Problem.

An Algorithm that finds the median may be viewed as a "factory" that produces a certain kind of "spider" structure (fig. 1) denoted by S_k^k. The median element is the "spider body." Imagine a "spider factory" that mass produces many copies of the same spider structure, assuming that it has an arbitrarily large set of elements to start with. The Algorithm makes comparisons as usual. Every now and then, it outputs a spider structure, S_k^k. The minimax complexity of producing m copies of S_k^k spiders is the usual comparison cost that is minimised over all spider-factories; call it $C_\infty(mS_k^k)$. The "mass-production cost" of a S_k^k spider is

$$\liminf_{m\to\infty} \left[\frac{C_\infty(mS_k^k)}{m}\right]$$

We would expect that the "mass-production cost" is cheaper than the cost of producing one spider individually. Indeed our results settled this question in the affirmative.

The Median Problem is closely related to the w-Fractile Problem, i.e. the problem of determining the i-th largest element for $i = \lceil wN \rceil$, $0 < w < 1/2$. We improve the lower bound for the w-Fractile Problem obtained by Schonhage [10] and Kirkpatrick [4]. The Bipartition Problem is the problem of partitioning a given set of N elements into two equal subsets such that each of the elements in one set is larger than all the elements in the other. Kirkpatrick [4] was the first to note the importance of this problem for obtaining lower bounds to the Median Problem. Our techniques for the Median Problem also work for the Bipartition Problem. Lower bounds for the Bipartition Problem in turn translate into lower bounds for a very general class of problems called General Partition Problems, first posed in [15]. Let $P(i_1, \ldots, i_k)$ be the $(i_1, \ldots, i_k)$-Partition Problem where we are given a set of N elements, $N = \sum_{j=1}^{k} i_j$. We want to partition it into k subsets $\{S_j\}_{j=1}^{k}$ such that $|S_j| = i_j$ $(j = 1, \ldots, k)$ and each element in S_j is larger than all the elements in S_{j+1} $(j = 1, \ldots, k-1)$. The complexity of $P(i_1, \ldots, i_k)$ is $C(P(i_1, \ldots, i_k))$ and is the usual minimax number of comparisons. Note that this class includes many of the comparison-type problems in the literature (e.g. Sorting, Selection Problem [2,4,15], Ordering Problem [2,4,15] and Bipartition Problem). Thus, $P(N/2,1,N/2)$ and $P(N/2,N/2)$ denote the Median Problem and the Bipartition Problem, respectively.

The organization of the rest of this paper is as follows: Sections 2 and 3 state the results and their significance. Section 4-8 describe the ideas of a State-Transition Adversary. Section 6 gives a simple illustration of state-transition adversary to obtain the Kirkpatrick-Schonhage result. Section 9 gives the proofs for all the results. The appendix is a detailed description of the adversary which gives us the 11N/6-lower bound. All figures are given at the end of the paper.

2. Economies of Mass Production

Our main result is the following:

Theorem 1: Finding the median of N elements requires at least 11N/6-K (for some fixed K) comparisons in the worse case. (All proofs are in the final section.)

The rest of this paper is mainly devoted to describing the techniques used to prove Theorem 1. We remark that the result of Theorem 1 is not so much surprising as that its proof is hard. In fact, it is generally conjectured that the exact complexity for the Median Problem is 2N. We believe that our techniques are powerful enough to obtain a lower bound arbitrarily close to 2N. It is interesting to note that although the 7N/4 bound for median is relatively easy to obtain [4], any improvement of that bound seems to demand a more than proportionate increase in effort. We want to suggest a reason why 7N/4 may be a "natural" barrier for the Median Problem:

Our definitions here are influenced by the work of A. Schonhage [6,11]. Define a structure to be a partial ordering relation on a set. The identity of the elements in the structure is unimportant; in graph-theoretic terms, a structure is "unlabelled." For reference, the trivial structure of one element is called the singleton. If Q and P are partially ordered sets and there is an order preserving 1-1 map from P into Q, we say that Q contains a copy of P. If there are m such maps from P into Q such that the ranges of the maps are pairwise disjoint, we say that Q contains m disjoint copies of P. If P is any structure, let mP be m disjoint copies of P and $|P|$ = the number of elements in the set P. Define $C_n(mP)$ to be the usual minimax comparison complexity of building mP from an initial set containing $m|P| + n$ singleton elements $(n \geq 0)$. If $n = \infty$, then the initial set has infinitely many elements. Let S_k^k be a spider structure (fig. 1). Then the usual Median Problem when $N = 2k + 1$ is simply the cost of producing one S_k^k spider by itself.

Actually our result is stronger than that stated in Theorem 1. We have actually established the following:

Corollary 1: $C_\infty(S_k^k) \geq 11N/3 - K$, for some constant K and $N = 2k + 1$.

This says that the lower bound of 11N/6 for computing the median of N elements holds even if there are infinitely many other elements present and the algorithm is not a priori constrained to pick any particular set of N elements. This evidence continues to lend support to a conjecture of Yao [14] that $C_0(S_k^j) = C_\infty(S_k^j)$ for all $j, k \geq 0$. If the conjecture is true then a 2.5N Algorithm for the Median Problem is known to exist [6].

Let $\hat{C}(P) = \liminf_{m \to \infty} \left[\frac{C_\infty(mP)}{m}\right]$. In fact, Schonhage [11] has shown that this definition may be simplified because of the following identity:

$$\liminf_{m \to \infty} \left[\frac{C_\infty(mP)}{m}\right] = \liminf_{m \to \infty} \left[\frac{C_0(mP)}{m}\right] = \lim_{m \to \infty} \left[\frac{C_0(mP)}{m}\right]$$

We define $\hat{C}(P)$ to be the mass-production cost of P. Patterson, Pippinger and Schonhage [6] had shown the following:

$$\hat{C}(S_k^k) \leq 7k/2 \cong 7N/4 \qquad (1)$$

Combined with Corollary 1, we have:

Corollary 2: $C_\infty\ (S_k^k) > \hat{C}(S_k^k)$

Thus Corollary 2 is the first general evidence showing that there is economy in mass-production as opposed to individual production of structures. (Paterson [11] has a specific example to the same effect). This is another example of what Schnorr [9] calls "hidden" dependencies. That is, the cost of computing a number of somewhat similar problems simultaneously may turn out to be cheaper than the sum of the costs of computing them independently. We think that such a phenomena is a universal one and may warrant an independent investigation in our efforts to understand the nature of Intrinsic Complexity. In this case, one is tempted to conjecture that the upper bound in equation (1) is tight. (This was our allusion to the "natural barrier" in the beginning of this section). However, the best lower bound we have for $\hat{C}(S_k^k)$ is [16]:

$$\hat{C}(S_k^k) \geq 3N/2, \text{ where } N = 2k + 1$$

We thus know $\hat{C}(S_k^k)$ up to a gap of N/4, which is apparently better than the 7N/6 gap still remaining for the original median problem.

3. Related Results

In the well known i-th Selection Problem [e.g. 2,3,4], whose comparison complexity is denoted by $V_i(N)$, it is usually assumed that i is fixed as N gets arbitrarily large. For example, finding the second largest element. However, even though we may think of the Median Problem as $V_i(N)$ where $i = N/2$, this notation is awkward and confusing (isn't i supposed to be fixed?). There is a large class of problems where the i-th element being selected is such that i is a fixed fraction of N. Thus i gets arbitrarily large with N. We define the w-Fractile Problem $(0 < w < 1/2)$ to be the i-th Selection Problem where $i = \lceil wN \rceil$. Let $F_w(N)$ be the minimax complexity of the w-Fractile Problem. Clearly, this is the appropriate general setting to view the Median Problem since it is just $F_w(N)$. Despite the superficial similarities between the Selection Problem and the Fractile Problem, the techniques for obtaining upper and lower bounds for the two problems are quite different. In what follows, we warn the reader that we have adapted the results in the literature to fit into our new notation. As a pedagogical note, we think that the new notation helps overcome some initial confusion many people have in viewing the results of the Selection and Fractile Problems by making the dichotomy notationally transparent.

Upper bounds for fractiles is 3N and follows at once from the linear median algorithm of [6]. For lower bounds, Schonhage [10] improved the original result of Pratt and Yao [7] by an additive factor of log N, using a simplified proof. He obtained

$$F_w(N) \geq N + \min\{2\lceil wN \rceil, \lceil N(1 + w) \rceil/2\} - 3, \text{ for } 0 < w < 1/2 \qquad (2)$$

Kirkpatrick [4] also obtained the same result using a different proof. However, Kirkpatrick also showed that:

$$F_w(N) \geq N - 1 + (\lceil wN \rceil - 1)(s + 1) + k \qquad (3)$$

$$\text{where } \lfloor (1 - w)N \rfloor + 1 \geq 2^S \cdot (\lceil wN \rceil + k),\ 0 \leq k < i - 1,\ s > 0$$

The lower bound of equation (3) is a strict improvement of equation (2) for $0 < w < 1/3$. The combined lower bound of (2) and (3) is illustrated in fig. 2. Our improvement of (2) and (3) comes from the following theorem:

Theorem 2: If $(1 + R)N - K$ is a lower bound for the Median where $R > 0$, and K is a fixed constant, Then $F_w(N) \geq (1 + 2wR)N - K$.

Corollary 3: $F_w(N) \geq (1 + 5w/3)N - K$, for some fixed constant K.

Note that corollary 3 supplements the Schonhage result (2) since for the range $3/7 < w < 1/2$, ours is a strict improvement. The effect of · corollary 3 on the lower bounds for Fractiles is indicated in fig. 2.

Kirkpatrick was the first to note that the Bipartition Problem was the key to all known proofs of lower bounds for the Median Problem. In fact the lower bound for Median follows from a lower bound for the Bipartition Problem according to the following equation which is easily derivable (e.g. see [4]):

$$C(P(N,1,N)) \geq C(P(N+1, N+1)) + 1 \qquad (4)$$

(Note that $P(N,1,N)$ is the Median Problem for $2N + 1$ elements and $C(P(N,1,N))$ denote its minimax complexity). The import of Kirkpatrick's observation is that all known proofs are unable to exploit any property which is peculiar to the Median Problem but which is not already available in the Bipartition Problem. The observation would not be very significant if a conjecture of Hadian and Sobel [2] is true. They conjectured that equation (4) is a strict equality. Our new proof is no different from previous ones in the sense that it also works for the Bipartition Problem:

Corollary 4:

$C(P(N/2,N/2)) \geq 11N/6 - K$, for some fixed K.

In general, we obtain the following lower bound for the General Partition Problem:

Theorem 3: Let $C(P(N/2,N/2)) \geq (1+R)N-K$, where $R \leq 1$ and K is a constant. Let $\sum_{j=1}^{k} i_j = N$, and $h = \max\{(i_j + i_{j+1}): \ j = 1, \ldots, k - 1\}$. Then $C(P(i_1, \ldots, i_k)) \geq 2N - h(1 - R) - K$.

Theorem 3 is a very general lower bound on the General Partition Problem, based on a lower bound on the Bipartition Problem. In fact, the Bipartition Problem is a special case of the General Partition Problem and the proof proceeds by induction from the Bipartition Case. However, we remark that the constant R has to be ≤ 1 in order for the proof to go through. An example of applying theorem 3 is the problem of partitioning a set of N elements into three equal parts which are linearly ordered in the induced order [15], $P(N/3,N/3,N/3)$. We get from theorem 3 that $C(P(N/3,N/3,N/3)) \geq 17N/9$. Another example is $C(P(N/4,N/2,N/4)) \geq 15N/8$. The main weakness of theorem 4 is that it cannot get a bound above 2N. On the other hand, it was shown in [15] using information theoretic arguments that $C(P(N/4,N/4,N/4,N/4)) \geq 2N$.

4. The State Transition Adversary

The original Adversary proofs appeared in Knuth [5] under the guise of oracles. A familiarity with the basic ideas in [1], [4] and [7] will be helpful in understanding this paper. For the sake of continuity, we briefly review some concepts:

Throughout this paper, the input set is X with cardinality, $|X| = N$. X^2 is the cartesian product of X with itself. If $\phi \subseteq X^2$, ϕ is a (strict) partial order on X iff (i) $\forall x \in X$, $(x,x) \notin \phi$ and (ii) $(x,y) \in \phi$, $(y,z) \in \phi$ $\Rightarrow (x,z) \in \phi$. If ϕ is a partial order, we write $x \underset{\phi}{<} y$ (or $x < y$ if ϕ is understood) for $(x,y) \in \phi$. We also say $x \underset{\phi}{\leq} y$ if $x = y$ or $x \underset{\phi}{<} y$. If $x > y$, and there is no z such that $x > z > y$, then we say x is directly greater than y. The transitive closure of $\phi \subseteq X^2$ is $\overline{\phi} = \phi \cup \{(x,z): \exists x,y,z \in X, (x,y) \in \phi, (y,z) \in \phi\}$. In illustrations, a partial order ϕ will be represented by its corresponding Hasse diagram $H(\phi)$. Although $H(\phi)$ are digraphs, we shall only imply the direction of an arc by drawing the source of the arc on a higher level than its sink.

We are interested in a kind of 2-player game played on X. The two players are called the Algorithm and the Adversary. The game is played in rounds. Each round consists of a question move by the Algorithm, immediately followed by a reply move by the Adversary. A question move (also called a comparison) is of the form "x:y" where $x,y \in X$, $x \neq y$. A reply move is of the form "$x > y$" or "$x < y$." Let $\phi_0 = \emptyset$, $\phi_{i+1} = \phi_i \cup \{x_i R_i y_i\}$ where "$x_i R_i y_i$" is the reply of the Adversary in the ith round, $R_i \in \{>,<\}$. The only constrain on the Adversary's reply is that it must be consistent i.e. $\overline{\phi}_i$ is a partial order on X for each i. If "$x > y$" is a reply, we say that x defeated y or x is defeated by y. Note that it may be the case that $x > y$ but x did not defeat y since the "greater than" relation is transitive but "is defeated by" relation is not.

If ϕ is a partial order on X, we say that ϕ determines the median of X iff $\exists\, x \in X$, $X_1 \subseteq X - \{x\}$, $X_2 = X - (X_1 \cup \{x\})$ such that $|X_1| = \left\lfloor \frac{N-1}{2} \right\rfloor$, $|X_2| = \left\lceil \frac{N-1}{2} \right\rceil$, for all $y \in X_1$, $x \underset{\phi}{\lneq} y$, and for all $z \in X_2$, $z \underset{\phi}{\lneq} x$. The game ends when ϕ_t determines the median of X, and the cost of the game is said to be t. The essence of an Adversary Proof for lower bounds is to specify (describe) an adversary which forces every game it plays (against an arbitrary adversary) to have a big cost. Since our interest is lower bounds, from now on our discussion will be from the perspective of the Adversary.

Let ϕ be the partial order at the end of a game and x is the median. It is well-known [eg. 7] that if $y \underset{\phi}{\gneq} x$, then y has to defeat some z where $z \underset{\phi}{\leq} x$. Similarly if $y \underset{\phi}{\lneq} x$, then y has to be defeated by some z where $z \underset{\phi}{\geq} x$. Thus, with the N - 1 elements of X - {x}, we can a priori claim that N - 1 comparisons has to be made regardless of anything. We shall call these N - 1 comparisons essential. A comparison is called inessential if it is not essential. Now suppose that we know that y has defeated some d other elements. elements. Moreover, y is also greater than the median. Then we can immediately say that y has made (d-1) inessential comparisons since at most one of the d comparisons of y is essential. Thus to obtain a lower bound of (1+R)N, where R is some rational number, we just have to ensure that each element makes an average of R inessential comparisons. From now on, unless otherwise stated, we shall simply say "comparisons" to mean "inessential comparisons."

We (as the adversary) shall inductively maintain the elements to have one of 3 possible statuses: Active, Promoted and Demoted (the last 2 statuses correspond to "heaven" and "hell" of [7]). Initially, all the elements are active and they become *deactivated* (i.e. promoted or demoted) as the game progresses. We shall only count comparisons made among active elements, the others being free. We further assume that promoted elements are greater than active ones which are in turn greater then demoted ones.

Among the active elements, we define objects called *a-structures* ("active structures") which are just any set of elements which are *maximally connected* in the known partial order when restricted to active elements. Note that a-structures differs from the structures defined in section 2 in two respects: First, a-structures are restricted to active elements. Second, a-structures are maximally connected, while structures do not even have to be connected. From now on, we shall have no occasion to refer to structures, so we shall simply call a-structures "structures" without fear of ambiguity.

For example, let the known partial order be as in fig. 3(a). then the following are not structures: $\{x_7,x_8\}$ (since x_7 is not active), $\{x_2,x_3,x_4,x_5\}$ (not connected in the restricted partial order), $\{x_3,x_4\}$ (not maximally connected). The only structures are $\{x_2\}$, $\{x_3,x_4,x_5\}$ and $\{x_8\}$. Thus different structures are disjoint. The Adversary will only allow certain types of structures to occur. Thus we shall list certain structures as *allowable*. All other structures are *unallowable*. Since we concentrate only on active elements, we will not draw deactivated elements in the future. Thus fig. 3(a) would be just represented as in fig. 3(b).

When the Algorithm compares two elements "x:y", the Adversary reply either "x>y" or "y>x" according to some "rule". By a *rule* we mean the specification of how the Adversary should respond. Our rules try to specify a reply such that the resultant structure is an allowable one. If this is possible, we say the rule is a *C-rule* ("closure"). But it may be impossible to obtain an allowable structure, in which case the rule not only specify "x>y" or "y>x", but also the *deactivation* (i.e. promotion and/or demotion) of some elements so as to remove the unallowable structures. This latter kind of rule is a R-rule ("resolution").

For example, let the set of allowable structures be as indicated in fig. 4(a). Suppose that a comparison is made between x and y, as in fig. 4(b). It shoule be clear that the Adversary should reply "x>y" since the result would be an allowable structure. Thus a C-rule applies here. In general, C-rules are obvious from looking at the set of allowable structures and we omit specific mention of C-rules from now on. On the other hand, if the comparison is between x and y as in fig. 4(c), then clearly no C-rules are possible. In such a case, the Adversary must have an an R-rule which tells it may "resolve" the situation by deactivating some elements. For example, the R-rule may be as in fig. 4(d), which specifies that x should be promoted and z demoted (notations should be clear).

In fig. 4(d), note that x had made at least two inessential comparisons (including the latest one) and z made at least one inessential comparison, giving a total of 3 inessential comparisons. Furthermore, the application of this R-rule causes the promotion and demotion of one element respectively. In general, a R-rule may cause p elements to be promoted, d elements to be demoted and the number of (inessential) comparisons made by the deactivated elements is c. In that case we define c(p:d) to be the claim associated with that R-rule. The R-rule of fig. 4(d) has a claim of 3(1:1) . Thus "claims" are just 3-tuples of non-negative numbers with obvious meanings for each component. Claims may be added or subtracted in a component-wise manner. E.g. 1(0:1)+3(2:1)=4(2:2), 5(2:2)-3(1:2)=2(1:0).

Suppose at some moment, p elements had been promoted and d elements had been demoted so far; we say that the Adversary (at that moment) is in the state-of-unbalance s where s=p-d may be negative. For short, we just say state for "state-of-unbalance". The application of a R-rule will cause the values of p and/or d to change and in general, this will also result in a change in the state-of-unbalance (state-transition). As discussed in [1], a good Adversary must delay the deactivation of the median for as long as possible by having about equal number of promotions and demotions. This implies that we want |p-d| to be small. Call the number |p-d| the unbalance. For now, assume that our Adversary has the property of Bounded Unbalance, i.e. the unbalance is always bounded by some fixed constant U depending on the Adversary. Because of the desire to keep the unbalance small, the Adversary tries to bias the deactivations according to which state-of-unbalance it is is. E.G. if p>d, the Adversary is more willing to demote than to promote. This is reflected by specifying, for each state-of-unbalance, the corresponding set of defined structures and rules. The allowable structures and rules for state s and state -s are "duals." By symmetry, from now on we only consider non-negative states (i.e. $p \geq d$).

Because a structure may be allowable in one state but not in another, we have a third kind of rule called a T-rule ("transition"). Suppose the structure of fig. 5(a) (for reference, call it the elbow structure) is allowable in state 2 but not in state 0. But as a result of a state transition from state 2 to state 0 we now find that we have an elbow structure in state

0. This is when we call on a T-rule to remove unallowable structures produced as a result of a state transition. For example, the T-rule as shown in fig. 5(b) will remove the elbow structure, leaving two singleton elements as in fig. 5(c). Note that this T-rule not only remove the "elbow" but also causes a transition from state 2 to state 1. There is a claim associated with each T-rule just as in the case of a R-rule. (E.g. the T-rule of 4(b) has a claim of 1(1:0). The only difference between a T-rule and a R-rule is that a T-rule is applied even before the Algorithm makes the next comparison, while a R-rule is applied in response to a comparison. We shall simply say "rule" if it is unimportant whether it is a C-rule, R-rule or a T-rule.

5. Balancing Accounts

The previous section has outlined a general scheme for constructing a state-transition adversary. This section indicates how a lower bound may be derived from such an adversary. Our strategy for a lower bound is as follows. Imagine the Adversary as a collector of claims. Each time a R- or a T-rule is applied, he adds to his collection the claims associated with that rule. Being a cautious man, he likes to deposit his claims in a bank. The bank, however, insists that each deposit of claims must be "balanced" (define a claim c(p:d) to be balanced iff p=d). Let us call the ratio c/(p+d) the rate, and c the value of the claim c(p:d). Assume the rate of a deposit is always at least R. Since the Adversary's account (i.e. sum of deposits) with the bank can only be balanced (since each deposit is balanced), there may be some "unbalanced" claims left over (whenever state s≠0). We assume inductively that in each state, s, the Adversary has a fixed amount of such unbalanced claims which are not deposited in the bank. We refer to such claims as the state-claim of state s. To make our proof go through inductively, the state-claim when s=0 is always the null claim (i.e. 0(0:0).

Suppose that the game is played according to the above strategy. Then, when the game ends, the number of (inessential) comparisons is at least the value of the Adversary's bank account (plus a little state-claim). Now the game ended only because the median is (uniquely) determined. There are two possibilities: (W.l.o.g. assume that more elements were promoted than demoted in both cases). First, the median may still be active. If that is so, we claim that only one structure was left. This is clear because if some other structure besides that which contains the median remained, this means that the median is unrelated to all the elements in the other structure. But by a well-known result [1,5] the median is not yet uniquely determined, a contradiction. Let us say that the size of the largest structure allowable for the Adversary is S. Thus at least $N-S$ elements were deactivated. In the second case, where the median is already deactivated, then $N/2$ elements are promoted. Since the unbalance is bounded by some constant U, we know that at least $N/2-U$ elements are also demoted. In either case, at least $N/2-\max\{U,S\}$ elements are demoted. Since the bank account is balanced, let it be $b(q:q)$. Let $Q = \max\{p+d: c(p:d)$ is a state-claim$\}$. Then, $q \geq N/2-\max\{U,S\}-Q$. But since the rate of each deposit is at least R, we have $(b/2q) \geq R$. This gives the value of the account, b to be at least $2qR \geq RN - K$ (where K is a fixed constant depending on U, S and Q). The lower bound of $(1 + R)N - K$ follows.

6. The Kirkpatrick-Schonhage Adversary

The $\frac{7N}{4}$ lower bound proofs of Kirkpatrick [4] and Schonhage [10] are inherently the same even though they were worded very differently. It is interesting to note that Kirkpatrick gave his Adversary in the scheme of the so-called Dynamic Adversary which obtained the best lower bounds for the ith Selection Problem, while Schonhage called his approach a Reduction Technique which worked for more general kinds of comparison problems. We shall give yet another another version of their proofs using the framework of the state-transition Adversary. This may serve to clarify and illustrate our technique.

In this Adversary, we allow 5 states-of-unbalance: $s = -2, -1, 0, 1, 2$. By symmetry, we only consider non-negative states. The allowable structures for each state and the state-claims for the respective state are shown in fig. 6. Finally the T- and R-rules are shown in fig. 7.

In fig. 7, Current Claims (column 5) refer to the claims associated with the rule currently being applied. The rules given are complete i.e., they cover all possible situations (we ignore the dual cases). We want to make a remark about a rule in line 4 of fig. 7 that may be confusing. The element labelled x is compared and the rule says "x whould be promoted and y demoted." We claim that at least 2 (inessential) comparisons were made by x and in fact the comparison between x and y must be inessential. This means that y has not yet made an essential comparison but will do so some time in the future!

This was called a "stretch" in [7]. Note that the rate of deposit in fig. 7 is at least 3/4. By the remarks in section 5, the lower bound of 7N/4 follows immediately. Note that for each rule, the following "accounting principle" holds: Assume that we are in state s_1 and the application of rule r takes us into state s_2. Then

$$\underline{\text{Claim}}(s_1) + \underline{\text{Claim}}(r) = \underline{\text{Claim}}(s_2) + \underline{\text{Deposit}}$$

where $\underline{\text{Claim}}(s_1)$ = the state-claim of state s_1

$\underline{\text{Claim}}(r)$ = the current claims (of rule r)

$\underline{\text{Claim}}(s_2)$ = the state-claim of state s_2

$\underline{\text{Deposit}}$ = the claims deposited at the bank.

The transitions between the states of the above Adversary may be summarised in the <u>state-transition diagram</u> of fig. 8. Each node represents a state and an arc from state s_1 to state s_2 means that there are rules that could cause a transition from state s_1 to s_2. The labels of the arc tell how much the "current claim" is.

To improve the 7N/4 bound the natural thing to try would be to

(i) increase the number of States-of-Unbalance, and

(ii) allow more complicated structures.

However, attempts in just those directions has been frustrated by combinatorial explosions. New ideas have to be introduced to facilitate (i) and (ii). In the following sections, (i)′ The number of States-of-Unbalance is allowed to increase significantly by introducing the concept of color classes and

(ii)′ More complicated structures which are "unfavorable" to the Adversary become allowable by introducing safe-boxes.

7. Color Classes

As a further aid to our analysis, we shall "paint" the structures into different colors. A color class is just a set of structures of the same color. We remark that "color" is a property of the structure, not the elements. By this we mean that if an element has one color while it is part of a structure x, then later it may assume another color if it became part of a different structure y. Suppose we have m such color classes $<C_1,...,C_m>$. For each class, imagine we have a different Adversary and the state-of-imbalance of each class only depend on how elements have been deactivated from that class. Thus we now use a m-tuple $<s_1, s_2,...,s_m>$ to indicate the overall state-of-unbalance. Now all our previous analysis may be viewed as an analysis for one particular color class. It is also true that if each Adversary of a color class continues to make balanced deposits with rate at least R, (think of the adversaries of each color class sharing a joint-account) then the final account will still have a value at least NR-K for some constant K. This device of painting structures into different colors greatly simplifies our analysis by allowing us to consider the Adversary in manageable portions. Moreover a combinatorial explosion is avoided because there is essentially no interaction between the different color classes when the technique is used correctly.

8. Safe-boxes and Unbounded Unbalance

In developing an Adversary, it becomes apparent that certain structures are unfavourable. However, if we can ensure that a "bad" structure is only created in situations where we have excess claims, we can use this "bad" structure as a temporary safe-box for depositing the excess claims. (Remark: We do not formally define the intuitive notion of "bad." Suffice to say that a structure is "bad" if it is "almost" a total ordering). Call the excess claims associated with a safe-box its fixed-deposit. If the safe-box is destroyed (by some deactivation), the Adversary will recover the fixed-deposit. This device helps us "remember" extra claims that we had before. For example, the structure in fig. 9(a) which we call a 3-link is such a "bad" case. But it turns out that we can develop an Adversary which always associates a fixed-deposit of 2(1:1) with this 3-link safe-box. Using just all the ideas discussed so far, and assuming that the safe-box deposits are balanced (as in the case of the bank deposits, a safe-box deposit of c(p:d) is balanced iff p=d), we were able to get a 23N/13 Adversary, a very small improvement over the 7N/4 result.

Our final and major improvement came from the following observation. All previous Adversaries satisfy the condition $C_1(K)$ for some constant K depending on the Adversary:

$C_1(K)$: "the unbalance throughout the game is at most K"

We note that this constraint is stronger than we need because the analysis in section 5 shows that we only need condition $C_2(K)$:

$C_2(K)$: "the unbalance is at most K at the end of the game"

Clearly $C_1(K)$ implies $C_2(K)$. We want to find sufficient conditions on the Adversary so that we can abandon Bounded Unbalance during the game and still have condition $C_2(K)$. Our idea is to use the safe-boxes. Suppose that the Adversary now allows arbitrary amounts of unbalance. But our stuffy old bank still insists on balanced deposits. But now we can use safe-boxes to store the unbalanced claims. Each safe-box has a fixed capacity, so that the amount of unbalance associated with each safe-box is bounded. However, because we can have arbitrarily many safe-boxes (depending on N), the total amount of unbalance is now arbitrarily large. The following lemma gives us sufficient conditions that ensures that $C_2(K)$ is still satisfied for some fixed K:

Lemma 1: Let P be a safe-box which has a fixed-deposit of c(p:d). Assume the size of P ($=|P|$) is at least equal to the unbalance in the fixed-deposit ($=|p-d|$). If this is true for every safe-box P in the Adversary, then for some fixed K the condition $C_2(K)$ holds.

Sketch Proof: We show it for the case where there is only one type of safe-box, P with size t and fixed-deposit of c(p:d). The proof for more than one type of safe-box is similar. Suppose the median is determined. If the median is still active, the discussion in section 4 shows that only one structure can remain, and clearly the unbalance is bounded by the size of the remaining structure. So assume that the median was promoted (w.l.o.g.). Suppose that number of safe-boxes, P remaining active was k, then the number of active elements that are in P structures is kt. Let a be the number of active elements that are not in P structures. Now the total claims deposited with k safe-boxes is kc(kp:kd). Let the claims deposited in the bank be b(q:q) and let e(u:v) be the sum of state-claims in each of the color classes. Since the median was promoted, the total number of promoted elements, kp+q+u is at least N/2. But the total number of elements is N = kp+kd+kt+a+2q+u+v. Combining them, we get that

$$(u-v)\geq k(t+d-p)+a \qquad (5)$$

Both $a\geq 0$ and $|u-v|$ are bounded, depending on the Adversary. By the assumption of the lemma, $(t+d-p)\geq 0$. Thus, (5) shows that k must be bounded. But the total unbalance is given by $|(kp+q+u)-(kd+q+v)|$ (i.e. the number of promoted elements minus the number of demoted elements) $= |k(p-d)+u-v| \leq k|p-d|+|u-v|$, which is bounded.

Q.E.D.

Lemma 1 forms the basis for obtaining our best results. In the Appendix, we show a 16N/9 Adversary, and then indicate how we can finally tune it into a 11N/6 Adversary. We remark that Lemma 1 is not vacuous because it is easy to demonstrate an Adversary not fulfilling the conditions of the Lemma and $C_2(K)$ is false for any K.

9. Proofs

Proof of Theorem 1:

We have already given the basic ideas of the proof in the preceding sections, especially section 5. It remains to specify a particular adversary which achieves a rate of deposit at least 5/6. This is done in the appendix.

Q.E.D.

Proof of Corollary 1: In our proof of the Theorem 1, the number of "inessential" comparisons claimed is independent of the number of excess elements. This observation is originally due to Kirkpatrick [4].

Q.E.D.

Proof of Corollary 2:

From Corollary (1), $C_\infty(S_k^k) \geq 1.833N$ but equation (1) shows that $\hat{C}(S_k^k) \cong 1.75N$.

Q.E.D.

Proof of Theorem 2: The Adversary initially demotes (1-2w)N elements before any comparison is made. Then the w-Fractile problem is reduced to the median problem for 2wN elements. But we know the number of non-essential comparisons for 2wN elements is at least 2wRN. Then the total number of comparison is N+2wRN.

Q.E.D.

Proof of Corollary 3: Substitute $R \geq 5/6$ (from Theorem 1) in Theorem 3.

Q.E.D.

Proof of Corollary 4: We would like to apply the Adversary in the Appendix to the Bipartition Problem. But first we have to show that a result corresponding to Lemma 1 is true for the Bipartition Problem. We see that the proof of Lemma 1 refers to the "median element", but it turns out that using the "median element" is only for convenience and is not crucial to the proof. For the Bipartition Problem, the only thing to note is the fact that at the end of the game, all the structures that are still active must belong to the upper partition, or else they all belong to the lower partition. So now, even though more than one structure may remain active, the total number of active elements is still bounded. Thus we may use the Adversary of Appendix 1 to obtain a lower bound of 11N/6 for the Bipartition Problem.

Q.E.D.

Proof of Theorem 3:

We will prove this by induction on k. For this proof, "comparisons" refer to essential as well as non-essential ones.

If k=2, this is true from Corollary 4.

For k>2, our Adversary only allows the "2-link" structure (fig. 9(b)) and the singleton element. The only R-rule is this: Whenever a top of a "2-link" is compared, we promote it. Whenever the bottom of a "2-link" is compared, we demote it. By symmetry, assume that an element is promoted and we claim two comparisons. This gives us:

$$C(P(i_1,\dots,i_k)) \geq 2+C(P(i_1-1,\dots,i_k))$$

and the following three cases can be verified:

(a) $i_1 = 1$. This follows by induction on k.

(b) $i_1 > 1$, and $i_1+i_2 \neq \max\{(i_j+i_{j+1}) : j=1,\ldots,k-1\}$.

(c) $i_1 > 1$, and $i_1+i_2 = \max\{(i_j+i_{j+1}) : j=1,\ldots,k-1\}$. Note that this is the case where the assumption that $R \leq 1$ is required.

Q.E.D.

Appendix: A New Adversary

We first show a 16N/9-Adversary (i.e. one which obtains a lower bound of 16N/9) in order to illustrate all the concepts introduced. Then we indicate how we might extend it to a 11N/6-Adversary. The 16N/9-Adversary has 4 color classes, say C_1, C_2, C_3, C_4 and thus the state-tuple is of the form $<s_1,s_2,s_3,s_4>$. The table of fig. 10 summarises the range of values that each s_i (i=1,2,3,4) may assume. For each value of s_i, the associated state-claim (column 3) and allowable structures (column 4) are also shown. By symmetry, we omit the negative states ($s_i<0$). The last column refers to the 11N/6-Adversary and should be overlooked for now.

In the notation of fig. 10, <-,-,2,-> for example refers to any state-tuple where $s_3=2$, and s_1, s_2, s_4 are arbitrary ("don't cares"). In particular, this implies that any structure that is allowable for <2,-,-,-> or <-,3,-,-> or <-,-,1,-> or <-,-,-,0> is also allowable in state <2,3,1,0>. Thus the set of structures allowable in state <2,3,1,0> is shown in fig. 11 and should be deducible from fig. 10.

The safe-box structures and their associated fixed-deposits are shown in fig. 12. With each safe-box, we indicate that there is more than one possible deposit e.g. with the 3-link structure, we have either 5(3:3) or 2(1:1) as fixed deposits. It turns out that 5(3:3) is a worse case (i.e. gives a smaller lower bound) so that we ignore the 2(1:1) case from now on. Similarly, 10(6:6) and 12(8:6) are worse cases and we concentrate on them rather than 4(2:2) and 6(4:2). Intuitively, 5(3:3) is less favourable than 2(1:1) because 5(3:3) represents a rate of 5/6 while 2(1:1) represents a rate of 1 (=2/2). We will return to the 2(1:1) case later on when we show how to avoid 5(3:3) deposits, and thus achieve the best bounds yet.

Notice in fig. 10 that the only structure in color class C_4 is a pair of "elbow" structures (see fig. 5(a)). It turns out that these elbow structures are always created in pairs and we conveniently lump them together as one structure and call the aggregate a "double-elbow" structure. The device of "lumping" them together just simplifies our description but is not essential. The double-elbow structure is a safe-box and it has an unbalanced fixed deposit (see fig. 12). But it clearly satisfies the conditions of Lemma 1. The state-transition diagrams of the adversary is given for each color classes in fig. 13.

Finally, the T- and R-rules for the adversary is given in fig. 14 in a tabular form. The notations should be almost self-explanatory (compare with the Kirkpatrick-Schonhage Adversary in section 6). A row of the table may contain a number of rules for compactness. The R-rules are distinguished in that there are dotted lines indicating the element being compared (e.g. row 20), while a T-rule has no dotted lines (e.g. row 44). Moreover some R-rules may have more than one dotted line (e.g. row 22). In such cases, it means that any one of the comparisons indicated by a dotted line will cause the same deactivations. This is just a short hand for combining a number of R-rules that are alike. Also note that, invariably the result of applying a rule will leave behind some simpler structures as "debris". Usually these "debris" will be allowable in almost every state-tuple (e.g. the singleton, 2-link and 3-link structures), or else there are T-rules to remove them. It is this feature of our rules that mitigates combinatorial explosion which will result if the different color classes interact arbitrarily. Essentially then we are justified in treating each color classes as independent of the others.

In fig. 14, the column under "current claims" refer to the inessential comparisons made by elements that are currently deactivated. A simple rule for computing the number of such comparisons is this: If an element is promoted and it had defeated k elements, then (k-1) of the comparisons made by x are inessential. Similarly, if an element is demoted and had been defeated by k other elements, then (k-1) of the comparisons are inessential (refer [4] for discussion). Finally, it is important to note that the following "accounting principle" holds for every rule:

Claim(i) + Current + Claim(P) = Claim(j) + Claim(Q) + Deposit

where

Claim(i), Claim(j) = the state-claims of states i and j, respectively.

Current = those made by the application of the current rule.

Claim(P) = the fixed deposit of safe-box P which is destroyed by the rule just applied.

Claim(Q) = the fixed deposit of safe-box Q which is created by the rule just applied.

Deposit = the bank deposit

Now we indicate how the 16N/9-Adversary may be modified into a 11N/6-Adversary. We had already seen that each of the safe-boxes in the 16N/9-Adversary has two possible values for its fixed-deposit. We shall modify the Adversary so that the more favorable situation is ensured i.e. the respective safe-boxes always have a fixed deposit of 2(1:1) instead of 5(3:3), 4(2:2) instead of 10(6:6), and 6(4:2) instead of 12(8:6) (compare fig. 12). The state-claims are also changed, and are given by the last column of fig. 10. It turns out that we only have to change the rule in row 8 (fig. 14) because this is the only rule that creates a 3-link structure with a 5(3:3) fixed deposit - all the other "unfavorable" claims are propagated from this rule alone. For exposition, in fig. 15(a) we show the comparison and in fig. 15(b) we show the old R-rule that handled that comparison. Our proposed new R-rule is shown in fig. 15(c). Whereas the old rule causes a state transition from <3,-,-,-> to <0,-,-,->, the new rule causes a transition from <3,-,-,-> to <1,-,-,->. Note that the new rule also created a new structure (fig. 15(d)) not allowable before -- for reference, call it an X-structure. Here is where the usefulness of the "color classes" idea is reiterated: we just have to paint the X-structure with a new color, C_5 (and in fact, the only allowable structure in color class C_5 is the X-structure). By our "accounting principle" we can make the X-structure a safe-box with fixed deposit of 3(2:1). This is also an unbalanced deposit but the conditions of Lemma 1 is clearly satisfied.

The rules to handle comparisons involving the X-structure are given informally in figure 16.

(M1) The rules indicated in fig. 16(a) and 16(b) are easily handled, and in each case we get a bank deposit of 5/6.

(M2) The rule of fig. 16(c) results in a structure which is a safe-box structure from color class C_3 with a fixed deposit of 4(2:2). We are able to associate a claim of 4(2:2) with the resultant safe-box according to our "accounting principle".

(M3) The rule of fig. 16(d) also results in a safe-box structure which has a fixed deposit of 2(1:1). The current claims amount to 2(1:1) and may be contributed to the safe-box. The fixed deposit of the original X-structure of 3(2:1) may be "floated". When this happens, other X-structures become "unstable" because we will then apply the T-rule of fig. 16(e) to remove X-structures. That T-rule uses up the "floating claims" of 3(2:1) and in the process causes a bank deposit of 5(3:3).

(M4) The comparison indicated by fig. 16(f) is handled by either of the rules of fig. 16(g) or 16(h). Applying fig. 16(g) gives us a claim of 5(2:4) and applying fig. 16(h) gives us 5(5:1). Thus if we apply fig. 16(g) twice for every time we apply fig. 16(h), we will achieve a rate of 5/6. This idea of applying two or more alternative rules to the same comparison in some fixed frequency ratio is important and is used extensively below.

(M5) The comparison indicated by fig. 16(i) is handled by either of the rules of fig. 16(j) or 16(k), which gives us claims of 5(2:5) and 5(4:1) respectively. By applying the two rules alternatedly (every other occasion), we again achieve a rate of 5/6.

(M1)-(M5) takes care of all possible comparisons involving X-structures. It turns out that almost all the rules of fig. 14 for the 16N/9-Adversary is still applicable and we are able to achieve a rate of at least 5/6. The only exceptions are the rules of rows (31), (39) and (46) in fig. 14. We shall modify them as follows:

(M6) The comparison of fig. 17(a) is handled as follows: Assume we in state <i,4,-,->. If i<2, we apply the rule of fig. 17(b) and we go into the next state of <i+1,4,-,->. Otherwise, we apply the rule of fig. 17(c) and go into state <i-1,4,-,->.

(M7) The comparison of fig. 17(d) may be handled by the rules of fig. 17(e) or 17(f) claiming 3(1:4) or 6(4:2) respectively. If the rule of fig. 17(f) is applied three times for every two times that fig. 17(e) is applied, we achieve a rate of 6/7, which better than 5/6. Likewise, the comparison of fig. 17(g) is handled by that of fig. 17(h) and 17(i), and the comparison of fig. 17(j) is handled by fig. 17(k) and 17(1).

(M8) The comparison of fig. 17(m) is handled by the rules of fig. 17(n) and 17(o), applied in the frequency ratio of three times to one. Fig. 17(n) claims 5(3:1) and fig. 17(o) claims 5(2:8). Thus the average rate is 10/11, which is better than 5/6.

(M9) In case of the double-elbow structure, we specify the rules for the two elbows independently. Thus fig. 17(p) and (q) are applied as appropriate. The first rule claims 2(1:2) and the second claims 1(0:1). Thus for the elbow-pair, we may claim any combination of the sum of the two claims: 2(0:2) or 3(1:4) or 4(2:4). But the fixed deposit of the elbow pair is 6(4:2), so that in the worse case we obtain a claim of 10(6:6) which is a rate of 5/6.

The new Adversary is now completely specified and achieves the announced rate of 5/6 in all cases.

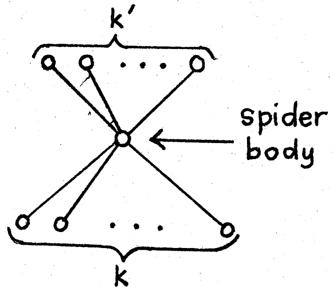


Fig. 1. A $S_k^{k'}$-spider structure

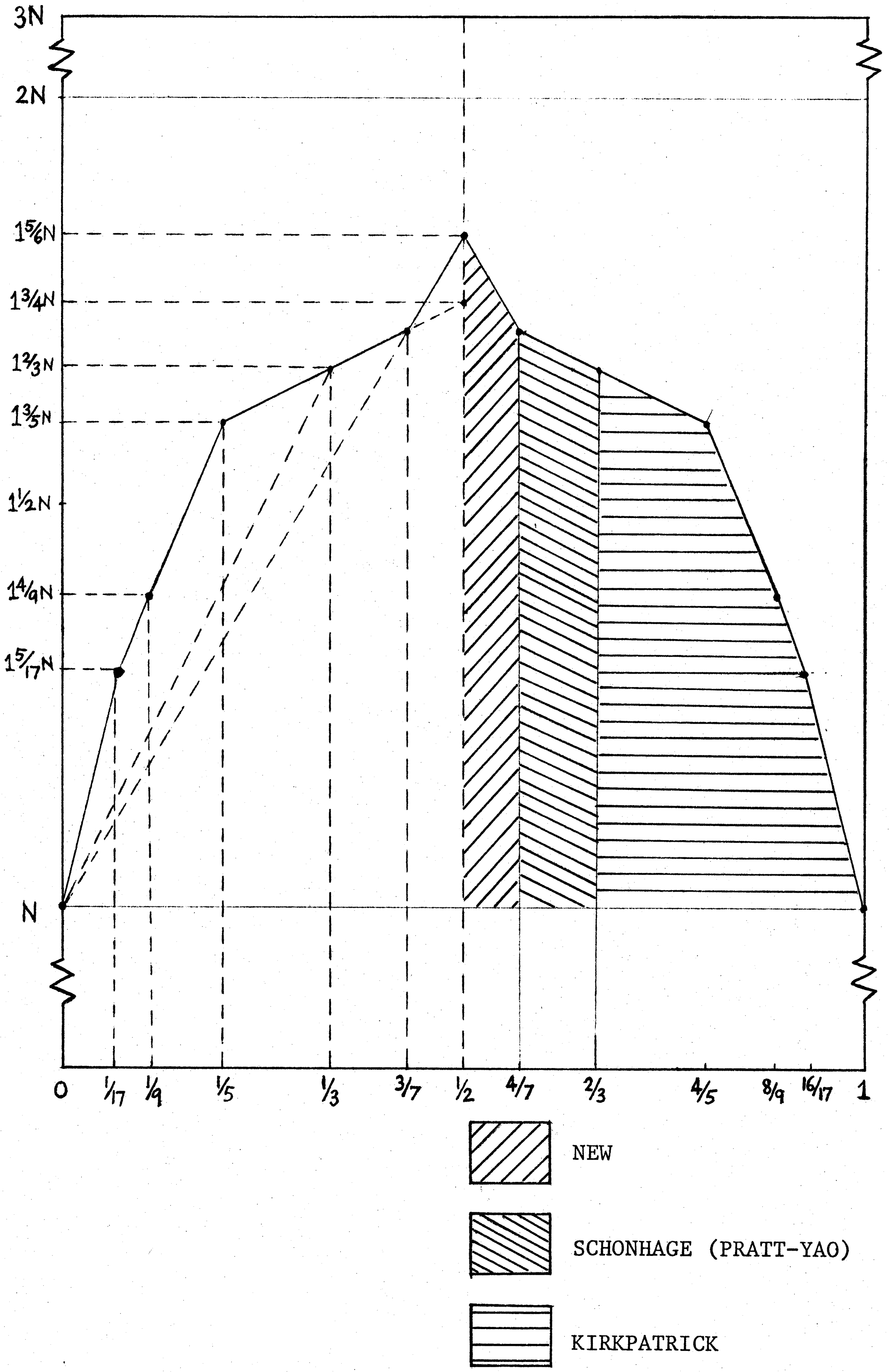
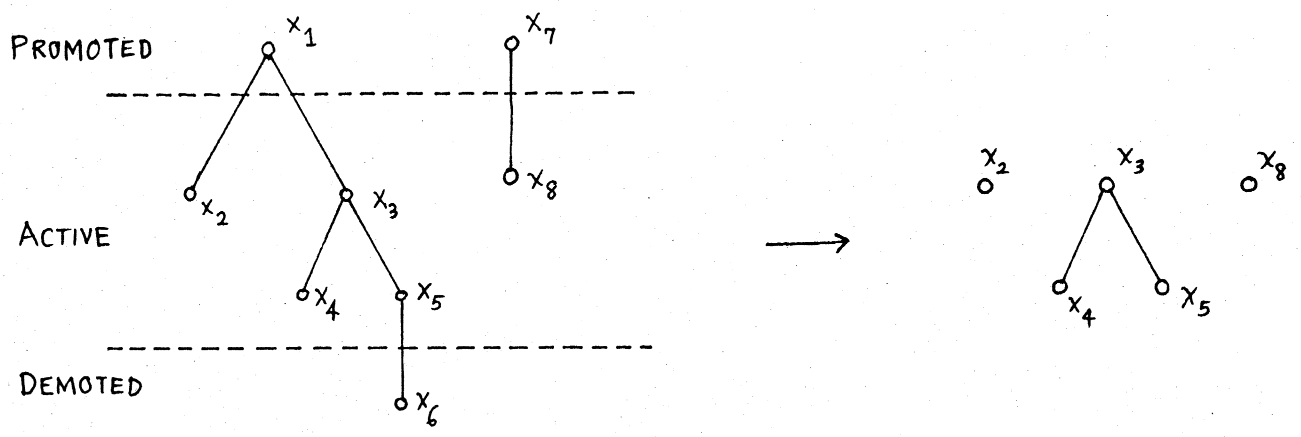


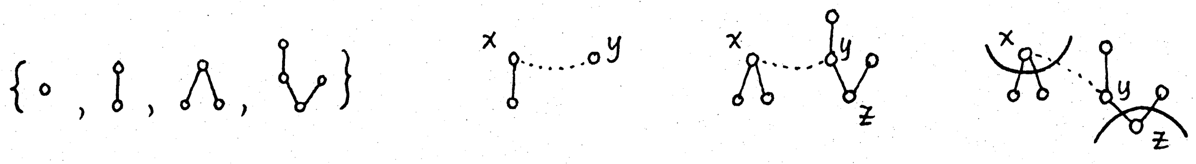
Figure 2: Lower Bounds for Fractiles



(a) Actual Partial Order

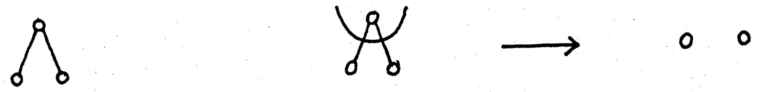
(b) Representation as a-structures

Fig. 3



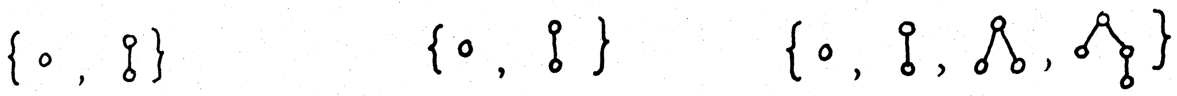
(a) (b) (c) (d)

Fig. 4 Examples of C- and R-rules



(a) (b) (c)

Fig. 5 Example of a T-rule



state = 0
state-claim = 0(0:0)

state = 1
state-claim = 1(1:0)

state = 2
state-claim = 2(2:0)

Fig. 6 Allowable structures and state-claims for the Kirkpatrick-Schonhage Adversary

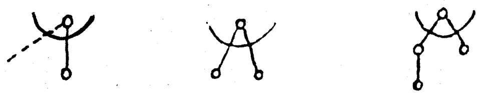
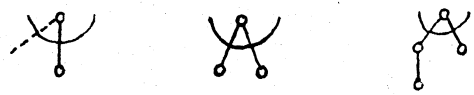
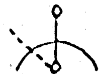
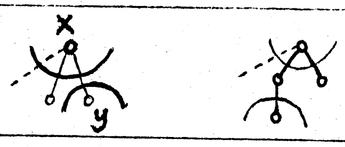
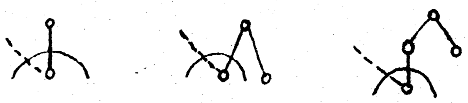
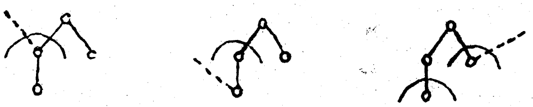
CURRENT STATE	STATE CLAIMS	RULES	NEXT STATE	CURRENT CLAIMS	DEPOSIT
0	0(0:0)		1	1(1:0)	0(0:0)
1	1(1:0)		2	1(1:0)	0(0:0)
1	1(1:0)		0	1(0:1)	2(1:1)
2	2(2:0)		2	2(1:1)	2(1:1)
2	2(2:0)		1	1(0:1)	2(1:1)
2	2(2:0)		0	1(0:2)	3(2:2)

Fig. 7. Transition Rules for the Kirkpatrick-Schonhage Adversary.

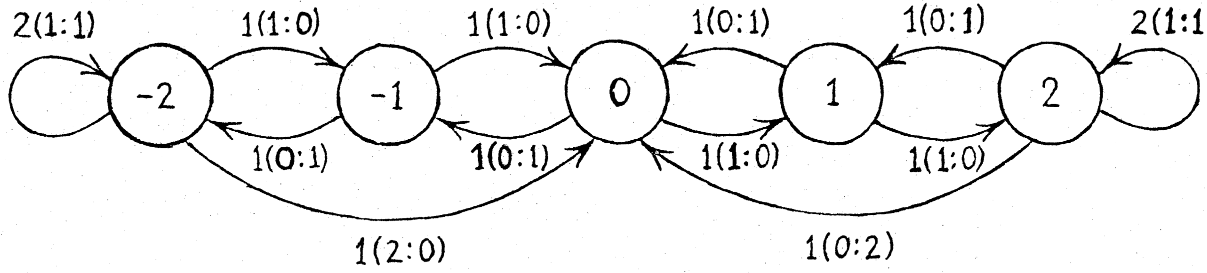


Fig. 8. State-Transition Diagrams for the Kirkpatrick-Schonhage Adversary.

(a)
(a) a 3-link structure

(b)
(b) a 2-link structure

Fig. 9.

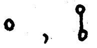
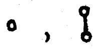
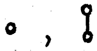
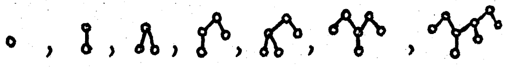
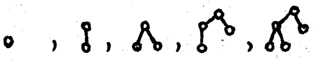
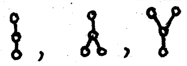
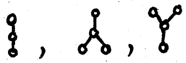
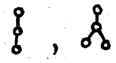
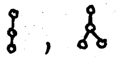
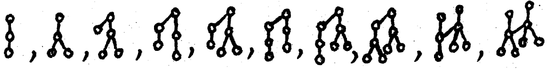
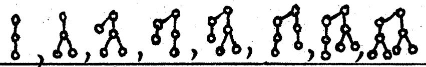
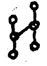
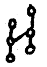
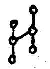
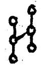
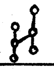
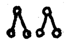
COLOR	STATE	STATE-CLAIMS FOR 16/9N	ALLOWABLE STRUCTURES	STATE-CLAIMS FOR 11/6N
C_1	⟨0,-,-,-⟩	0(0:0)		0(0:0)
	⟨1,-,-,-⟩	1(1:0)		1(1:0)
	⟨2,-,-,-⟩	2(2:0)		2(2:0)
	⟨3,-,-,-⟩	3(3:0)		3(3:0)
	⟨5,-,-,-⟩	6(5:0)		6(5:0)
C_2	⟨-,0,-,-⟩	0(0:0)		0(0:0)
	⟨-,1,-,-⟩	6(4:3)		3(2:1)
	⟨-,2,-,-⟩	7(5:3)		4(3:1)
	⟨-,3,-,-⟩	13(9:6)		7(5:2)
	⟨-,4,-,-⟩	14(10:6)		8(6:2)
	⟨-,6,-,-⟩	22(15:9)		13(9:3)
C_3	⟨-,-,0,-⟩	0(0:0)		0(0:0)
	⟨-,-,1,-⟩	18(12:11)		9(6:5)
	⟨-,-,2,-⟩	36(20:18)		16(11:9)
	⟨-,-,3,-⟩	12(9:6)		6(5:2)
	⟨-,-,4,-⟩	30(21:17)		13(10:6)
C_4	⟨-,-,-,0⟩	0(0:0)		0(0:0)

Fig. 10. Table of Defined Structures and State-claims for the 11/6N-Adversary.

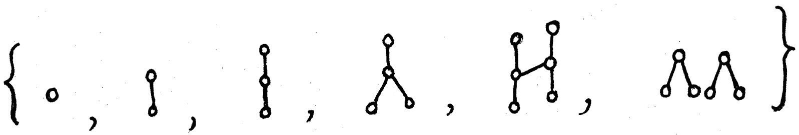


Fig. 11 Allowable structures in state ⟨2,3,1,0⟩

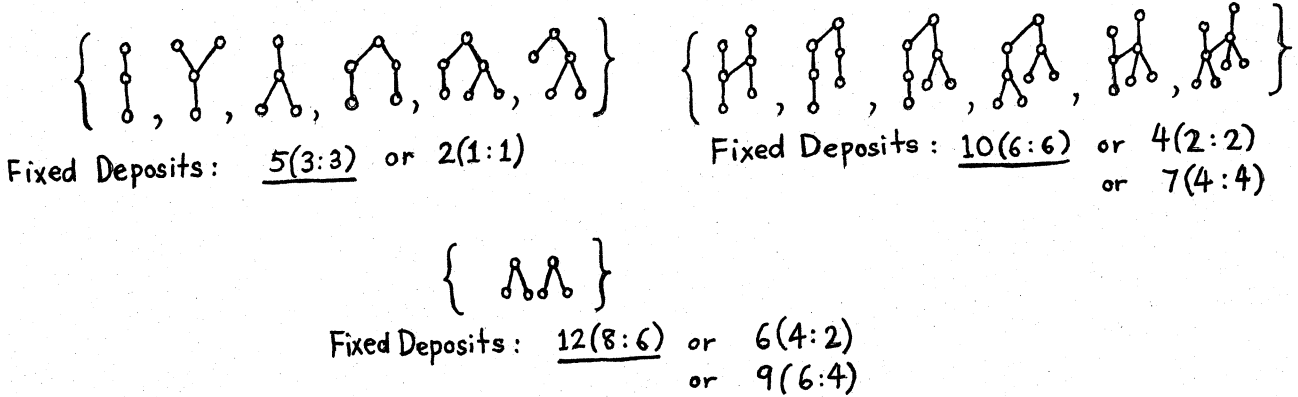

Fixed Deposits: 5(3:3) or 2(1:1)
Fixed Deposits: 10(6:6) or 4(2:2) or 7(4:4)
Fixed Deposits: 12(8:6) or 6(4:2) or 9(6:4)

Fig. 12. Safe-boxes for the Adversary
The worst case fixed-deposits are underlined

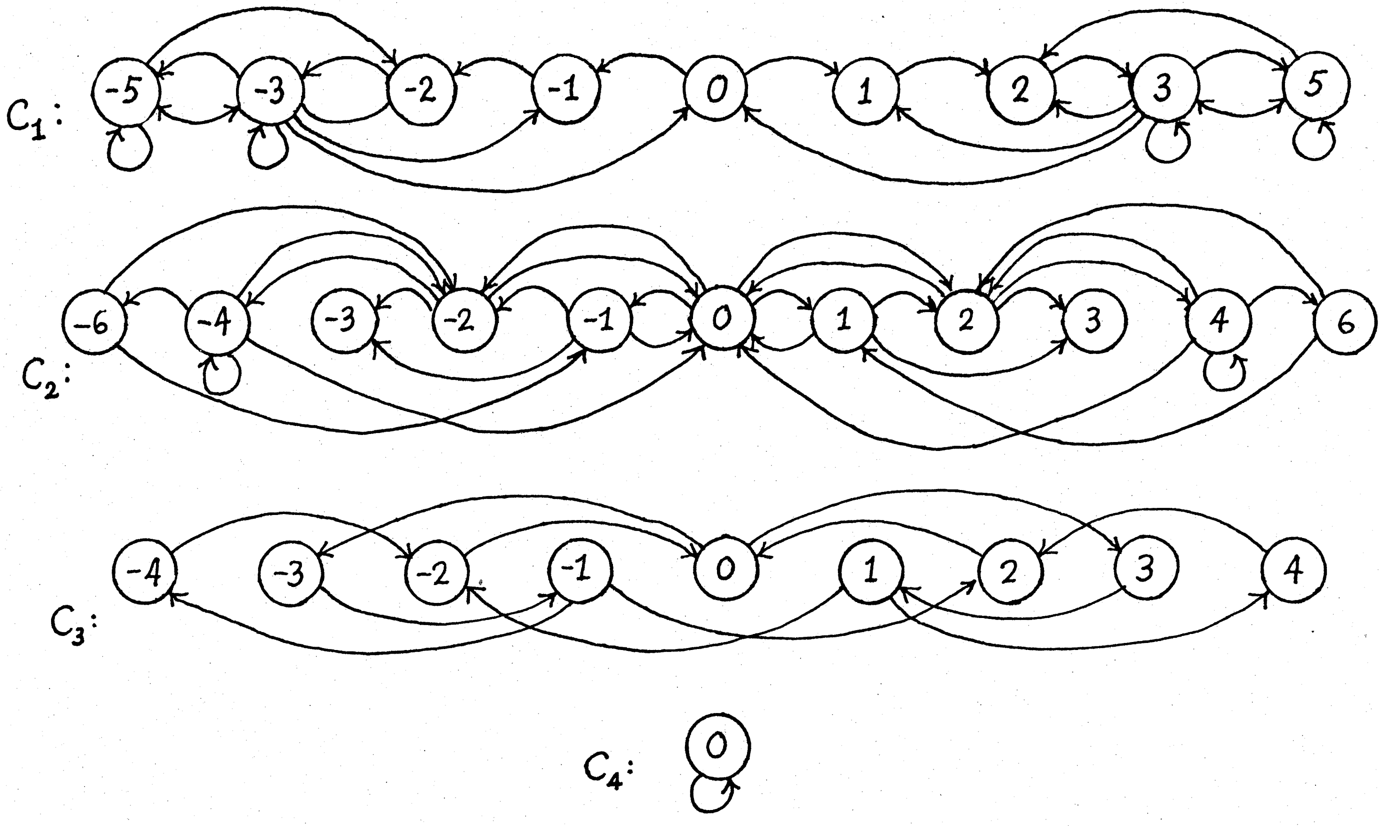
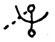
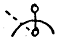
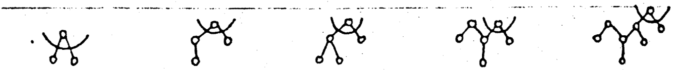
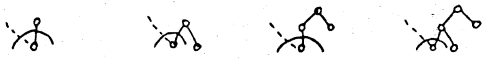
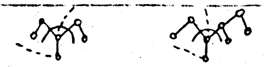
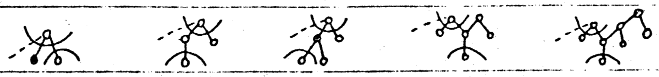
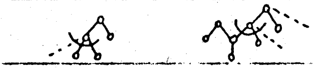
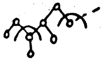
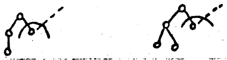
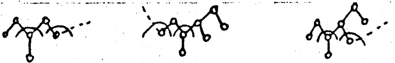
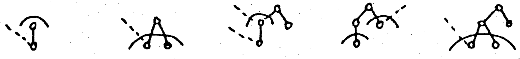
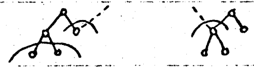
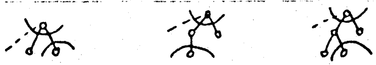
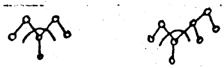
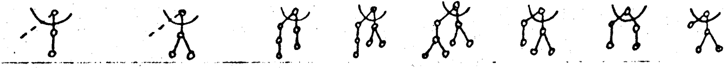
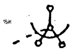
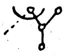
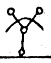
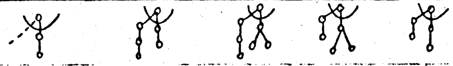
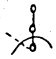
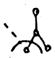
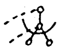
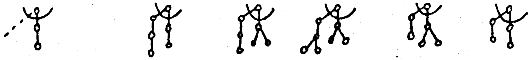
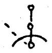
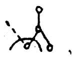
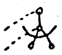
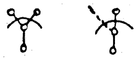


Fig. 13 State Transition Diagram for

the 16N/9-Adversary

FIG.14 RULES FOR A $^{16N}/_{9}$ - ADVERSARY

NO.	OLD STATE	RULES (r- and t-)	CURRENT CLAIMS	NEXT STATE	BANK DEPOSIT
1	⟨i,-,-,-⟩		1(1:0)	⟨i+1,-,-,-⟩	0(0:0)
2	(i=0,1,2)		1(0:1)	⟨i-1,-,-,-⟩	2(1:1)
3			1(1:0)	⟨i+1,-,-,-⟩	0(0:0)
4	⟨3-,-,-⟩		1(0:1)	⟨2,-,-,-⟩	2(1:1)
5			2(0:2)	⟨1,-,-,-⟩	4(2:2)
6			2(1:1)	⟨3,-,-,-⟩	2(1:1)
7			3(2:0)	⟨5,-,-,-⟩	0(0:0)
8			2(0:3)	⟨0,-,-,-⟩	0(0:0)
9			1(0:1)	⟨2,-,-,-⟩	0(0:0)
10			2(0:3)	⟨0,-,-,-⟩	5(3:3)
11	⟨5,-,-,-⟩		1(0:2)	⟨3,-,-,-⟩	4(2:2)
12			1(0:3)	⟨2,-,-,-⟩	5(3:3)
13			2(1:1)	⟨5,-,-,-⟩	2(1:1)
14			1(0:2)	⟨3,-,-,-⟩	4(2:2)
15	⟨-,0,-,-⟩		1(1:0)	⟨-,1,-,-⟩	0(0:0)
16			2(2:0)	⟨-,2,-,-⟩	0(0:0)
17	⟨i,0,-,-⟩ (i ≤ 1)		1(1:0)	⟨i+1,0,-,-⟩	0(0:0)
18	⟨i,0,-,-⟩ (i ≥ 2)		1(0:2)	⟨i-2,0,-,-⟩	8(5:5)
19	⟨-,1,-,-⟩		1(1:0)	⟨-,2,-,-⟩	5(3:3)
20			1(0:1)	⟨-,0,-,-⟩	12(7:7)
21			1(0:1)	⟨-,0,-,-⟩	7(4:4)
22			2(2:0)	⟨-,3,-,-⟩	0(0:0)
23	⟨-,2,-,-⟩		1(1:0)	⟨-,3,-,-⟩	0(0:0)
24			1(0:1)	⟨-,1,-,-⟩	7(4:4)
25			1(0:1)	⟨-,1,-,-⟩	2(1:1)
26			2(2:0)	⟨-,4,-,-⟩	0(0:0)
27			1(0:2)	⟨-,0,-,-⟩	13(8:8)

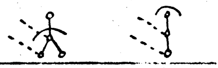
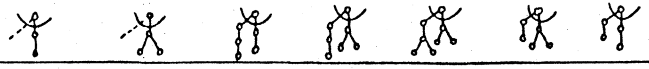
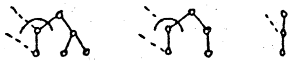
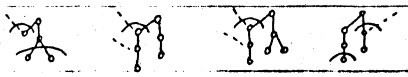
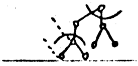
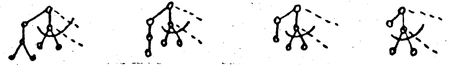
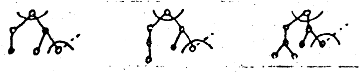
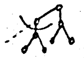
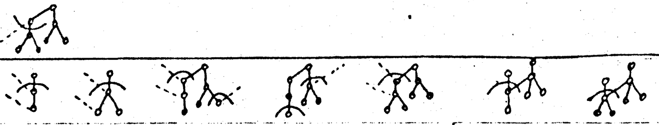
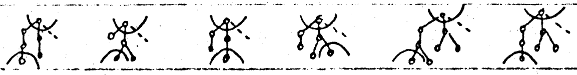
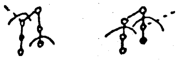
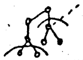
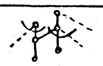
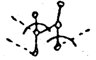
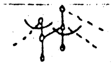
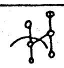
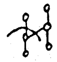
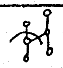
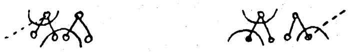
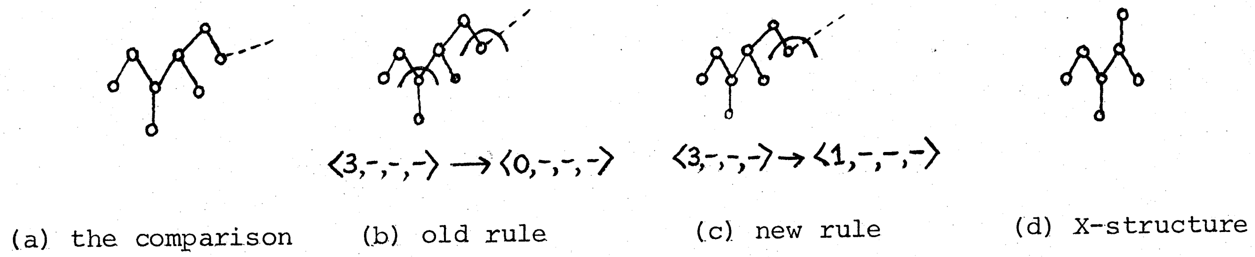
	OLD STATE	RULES (r- and t-)	CURRENT CLAIMS	NEXT STATE	BANK DEPOSIT
28	<-,3,-,->		1(0:3)	<-,0,-,->	19(12:12)
29			1(1:0)	<-,4,-,->	5(3:3)
30	<-,4,-,->		1(0:2)	<-,2,-,->	8(5:5)
31			1(0:3)	<-,1,-,->	14(9:9)
32			2(1:3)	<-,2,-,->	19(12:12)
33			3(2:0)	<-,6,-,->	0(0:0)
34			2(1:1)	<-,4,-,->	7(4:4)
35			2(2:0)	<-,0,-,->	0(0:0)
36	<-,6,-,->		1(0:4)	<-,2,-,->	21(13:13)
37			2(1:1)	<-,6,-,->	7(4:4)
38			1(0:4)	<-,2,-,->	26(16:16)
39			1(0:5)	<-,1,-,->	22(14:14)
40	<-,-,0,->		2(3:0)	<-,-,3,->	0(0:0)
41	<-,-,1,->		2(0:3)	<-,-,-2,->	0(0:0)
42			2(3:0)	<-,-,4,->	0(0:0)
43	<-,-,2,->		1(0:2)	<-,-,0,->	42(27:27)
44	<-,-,3,->		1(0:2)	<-,-,1,->	0(0:0)
45	<-,-,4,->		1(0:2)	<-,-,2,->	0(0:0)
46	<-,-,-,0>		2(1:2)	<-,-,-,0>	14(9:9)

Fig. 14 (cont.)



(a) the comparison (b) old rule (c) new rule (d) X-structure

Fig. 15.

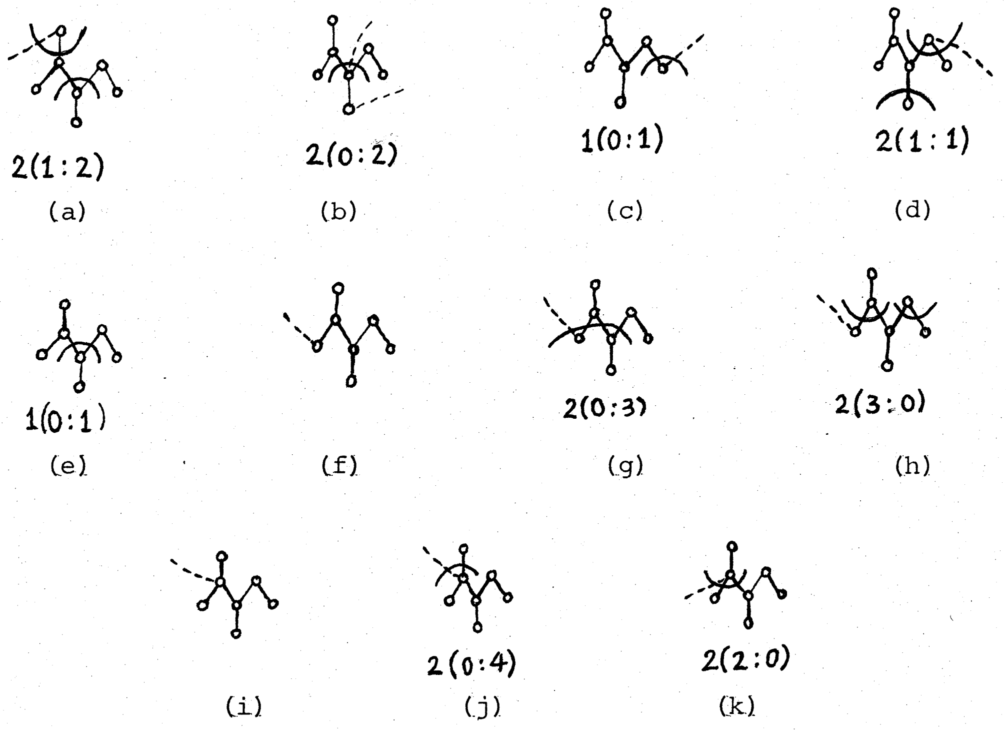


Fig. 16.

Rules for X-structures

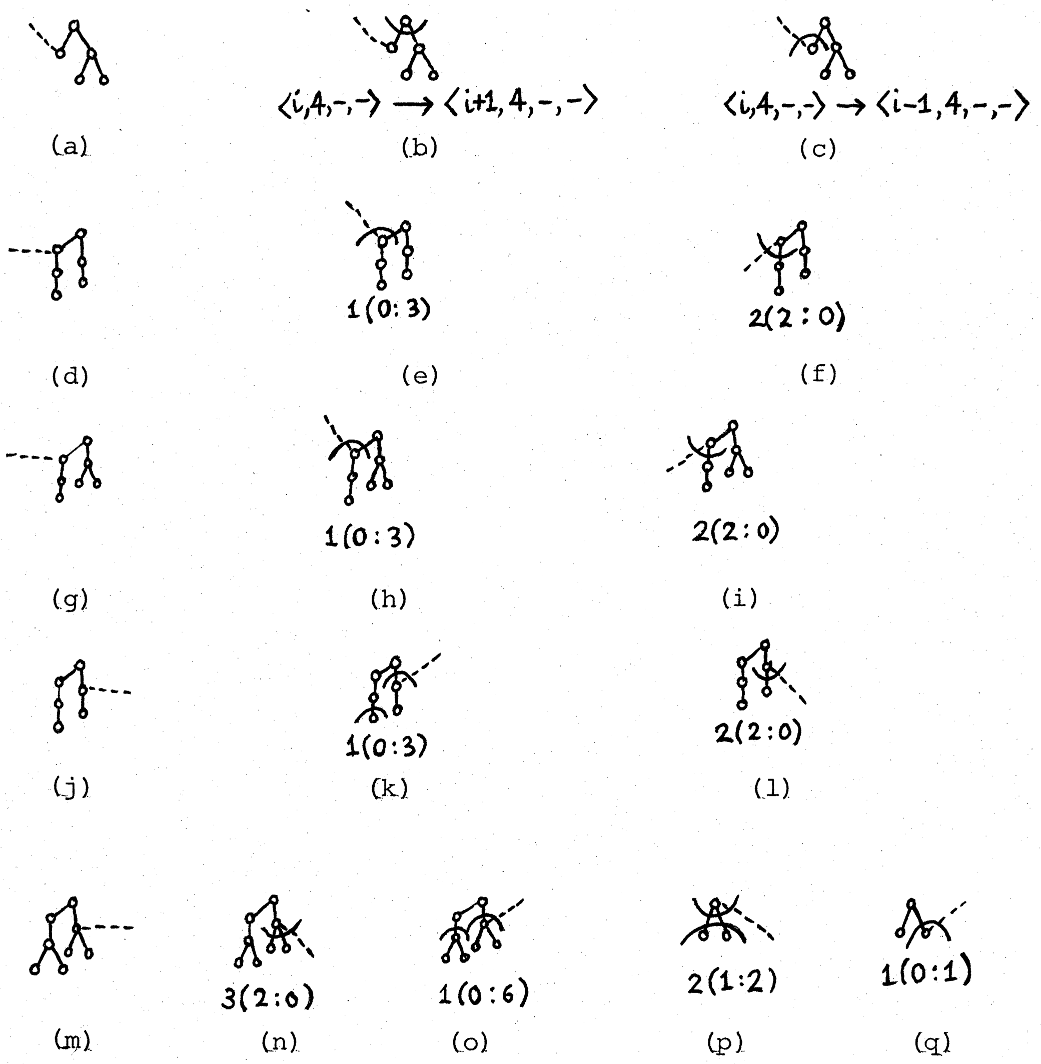


Fig. 17.

Rules for the 11N/6-Adversary which differ from the 16N/9-Adversary

Bibliography

[1] Blum, M., Floyd, R.W., Pratt, V., Rivest, R.L., and and Tarjan, R.E. "Linear Time Bounds for Median Computations" 4th Annual ACM Symposium on Theory of Computing (1972)

[2] Hadian, A. and Sobel, M. "Selectiing the t-th Largest Using Binary Errorless Comparisons", Colloquia Mathematica Societatis Janos Bolyai, Balatofured, Hungary (1969)

[3] Hyafil, L. "Bounds for Selection", SIAM J. of Computing, Vol. 5, No. 1, (Jan 1976)

[4] Kirkpatrick, D. "Topics in the Complexity of Combinatorial Algorithms", Technical Report No. 74, Univ. of Toronto (Dec 1974)

[5] Knuth, D.E. "The Art of Computer Programming: Vol.3, Sorting and Searching", Addison-Wesley (1973)

[6] Paterson, M., Pippenger, N. and Schonhage, A. "Finding the Median", Theory of Computation Report No. 6, Univ. of Warwick (April 1975)

[7] Pratt, V.R. and Yao, F.F. "On Lower Bounds for Computing the i-th Largest Element", Fourteenth Annual IEEE Symp. SWAT (1973)

[8] Reingold, E.M. "On some Optimal Algorithms" Technical Report No.428, Univ. of Ill. at Urbana-Champaign (Jan 1971)

Acknowledgements:

I would like to thank Professor Vaughn R. Pratt who first introduced the problem to me and whose personal interests in the Median Problem stimulated me. Professor David P. Dobkin read an early version of this paper which gave a 1.8n lower bound. The encouragement and support of Professor Ronald V. Book is greatly appreciated.

[9] Schnorr, C.P. "The Network-Complexity of Equivalence and other Applications of the Network Complexity," Automata Theory and Formal Lang., 2nd GI Conference.

[10] Schonhage, A. "A Reduction Technique for Lower Bounds" (unpublished paper.)

[11] Schonhage, A. "The Production of Partial Orders" (to appear in "Asterique").

[12] Shamos, I.M. and Hoey, D. "Closest-Points Problems", *16th Annual Symp. on Foundations of Computer Science* (Oct 1975)

[13] Yao, A. C. "An $O(|E|\log\log|V|)$ Algorithm for Finding Minimum Spanning Trees", *Information Processing Letters*, Vol.4, No.1 (Sep 1975)

[14] Yao, F.F. "On the Lower Bounds for Selection Problems", *Project MAC Technical Report TR-121*, M.I.T. (1974)

[15] Yap, C.K. "On Selection Problems", S.B. Thesis, M.I.T. (May 1975)

[16] Yap, C.K. "On Mass Production," in preparation.

New Lower Bounds for Median and Related Problems

by

Chee-Keng Yap

Yale University

Abstract

The previous best lower bound for the Median Problem is 7N/4 - logN due to Pratt and Yao. Since then, no substantial progress had been made, although both Kirkpatrick and Schonhage independently made the slightly improved bound of 7N/4 in simplified proofs. In this paper, we obtain a new lower bound of 11N/6. The proof employs a rather sophisticated Adversary. A number of new techniques are introduced. The most significant gain came from a kind of "Church-Rosser Property" of our Adversaries.

Combined with a result of Paterson, Pippenger and Schonhage, our result is the first general example showing that the average cost of "mass production" of a particular structure ("spiders") is cheaper than individual production. Such a phenomena (what Schnorr call "hidden dependencies") has appeared in many different contexts, and seems to be fundamental in understanding the meaning of intrinsic complexity.

Based on the new result for Median, the lower bound for the w-Fractile Problem due to Schonhage and Kirkpatrick are improved. Like all previous proofs, our proof for the Median carries over to the Bipartition Problem. This in turn can be used to obtain lower bounds for a very general class of problems called the General Partition Problem, $P(i_1, \ldots, i_k)$. This class includes many of the important comparison-based problems studied in the literature as special cases (e.g. Sorting, Selection, Ordering Problems).