On Lotteries with Unique Winners*

Eyal Kushilevitz† Yishay Mansour‡ Michael O. Rabin§

February 4, 1998

1 Introduction

A *lottery* is a collection of discrete, independent random variables $\Pi_1, \ldots, \Pi_N$ defined over a set $\{1, \ldots, B\}$. We associate with the random variable Π_i a player P_i. A lottery has the *unique maximum property* if for *every* subset of $\Pi_1, \ldots, \Pi_N$, with constant probability (say 2/3), the maximum value of the random variables is chosen by *exactly* one random variable. (Formally, for every non-empty subset $S \subseteq \{1, \ldots, N\}$, define the random variable $M_S = \max_{\{i \in S\}} \Pi_i$. Let p_S be the probability that $|\{i \in S : \Pi_i = M_S\}| = 1$. The unique maximum property states that $p_S \geq 2/3$ for every S.)

A lottery has the *unique winner property* if for *every* subset of random variables, with constant probability, there *exists* a value that is chosen by *exactly* one random variable. (Formally, let q_S be the probability that there exists a $j \in \{1, \ldots, B\}$ such that $|\{i \in S : \Pi_i = j\}| = 1$. The unique winner property states that $q_S \geq 2/3$ for every S.)

Lotteries with these properties have many applications in computer science, specially in cases where symmetry breaking is required. Examples include randomized mutual exclusion algorithms [7, 5], broadcast in radio networks [1], elections in anonymous networks [6], and various CRCW-PRAM algorithms [2]. [1]

*Research of Eyal Kushilevitz and Michael Rabin supported by research contracts ONR-N0001491-J-1981 and NSF-CCR-90-07677 at Harvard University.

†Research was done while the author was at Aiken Computation Lab., Harvard University. Current address: Dept. of Computer Science, Technion. e-mail: eyalk@cs.technion.ac.il .

‡Computer science Dept., Tel-Aviv University and IBM – T. J. Watson Research Center. e-mail: mansour@math.tau.ac.il

§Aiken Computation Lab., Harvard University and Institute of Mathematics, Hebrew University of Jerusalem. e-mail: rabin@das.harvard.edu .

[1] Some of these applications require the unique maximum property (e.g., the mutual exclusion) while for others the unique winner property is sufficient (e.g., the radio broadcast).

A trivial way to achieve these properties is by letting the participants to draw numbers uniformly in the set $\{1, \ldots, B\}$, where B is "large enough" (compare to N). For $B = N$ with constant probability, the maximum is unique (and with much higher probability there exists a uniquely chosen value). Unfortunately, in the applications it is important that B is small as possible, as this value corresponds to important complexity measures such as *time* (in the case of radio broadcast) and *space* (in the case of mutual exclusion).

Rabin [7] described and analyzed the following *geometric* lottery: Let $B = \log_2 N + 4$. All players use the same probability distribution; For every i, $1 \leq i \leq B - 1$, the value i is chosen with probability $\frac{1}{2^i}$. The value B is chosen with probability $\frac{1}{2^{B-1}}$. Rabin proved that this lottery has the unique maximum property.

This research was initiated with the motivation to discover whether this construction can be improved, or is it optimal (in the sense of the number of values, i.e. B). The results of this note show that it is optimal (up to constants).

A critical point is that the number of *actual* participants, t, is not known in advance. If t was known beforehand, we were able to use the following lottery: choose the value 1 with probability $1 - \frac{1}{t}$ and the value 2 with probability $1/t$. One can verify that if t numbers are chosen according to this lottery then with probability of about $1/e$ the maximum is unique. (This probability can be easily improved to $2/3$.) This way we get a lottery whose number of values B is independent of N. However, we prove that this cannot be the case when t is not known in advance.[2] Namely, we show that every lottery with either the unique maximum property or the unique winner property requires $B = \Omega(\log N)$.[3]

A different line of research is to give lower bounds for the problems in which those lotteries are used. Following this research, a significant progress was made in this direction; In [4], a lower bound for randomized mutual exclusion is proven. From this lower bound, one can get a lower bound for lotteries with the unique maximum property, in which all players use the *same* random variable Π. In [3], a lower bound for broadcast in radio networks is proven. From this lower bound, the results of this note can be derived. However, the direct proofs in this note, are much simpler and give a better understanding of the problem, as well as much better constants than those that can be obtained indirectly by using the results of [3].

[2] Again, this is usually the case in the applications.

[3] Clearly, the $\Omega(\log N)$ bound for lotteries with the unique winner property implies the same bound for lotteries with the unique maximum property. Nevertheless, we present two different proofs as the proof for the case of unique maximum is much simpler, and yields a better constant.

2 Lotteries with the Unique Maximum Property

In this section we prove that any lottery with the unique maximum property requires $\Omega(\log N)$ values.

Theorem 1: Let B be an integer. Let $\Pi_1, \ldots, \Pi_N$ be a lottery for N players $P_1, \ldots, P_N$ over the set $\{1, 2, \ldots, B\}$. If the lottery has the unique maximum property then $B \geq \log_6 N$.

Proof: We use the following notation: Let A be a set of participants and let E be an event, then, $Pr(E|A)$ denotes the probability that the event E happens given that A is the set of the participants in the lottery (and each participant $i \in A$ uses the corresponding random variable Π_i). We use the following definitions: Let $A \subseteq \{P_1, \ldots, P_N\}$ be a non-empty set of participants. We define

$$m(A) \stackrel{\triangle}{=} \max_{1 \leq j \leq B} \left[Pr(\max \geq j|A) > \frac{1}{2} \right].$$

That is, $m(A)$ is the maximal value j, such that if A is the set of participants in the lottery, the probability that the maximum number drawn is at least j is greater then $1/2$. We also define for every $1 \leq t \leq N$,

$$m(t) \stackrel{\triangle}{=} \min_{A:|A|=t} m(A).$$

This definition satisfies the following trivial properties:

- For every A, $m(A)$ is well defined (as at least $j = 1$ satisfies the condition).
- For every A, $1 \leq m(A) \leq B$ and therefore for every $1 \leq t \leq N$, $1 \leq m(t) \leq B$.
- If $A' \subset A$ then $m(A') \leq m(A)$. This follows immediately from the definition of m and by the fact that for every j, $Pr(\max \geq j|A) \geq Pr(\max \geq j|A')$. This implies that if $t' < t$ then $m(t') \leq m(t)$ (take A to be a set that gives the minimum for $m(t)$ and A' a subset of A of size t' then $m(t') \leq m(A') \leq m(A) = m(t)$).

The following claim says that $m(t)$ is not only non-decreasing but it should be strictly increasing from time to time. More precisely:

Claim 1: Assume t is divided by 6. Then $m(t/6) < m(t)$.

Proof of Claim: Assume, by way of contradiction, that $m(t) = m(t/6) = j_0$. Let A be a set of size t such that $m(A) = j_0$ (i.e., A gives the minimum for $m(t)$). Partition the set A into 6 disjoint subsets, $A_1, \ldots, A_6$ each of size $t/6$. For each of these A_i's, since $A_i \subseteq A$, then $m(A_i) \leq m(A) = j_0$. On the other hand, since $|A_i| = t/6$, $m(A_i) \geq m(t/6) = j_0$. Thus, $m(A_i) = j_0$. This in particular implies that $Pr(\max \geq j_0|A_i) > 1/2$.

Let M be the random variable which is the number of A_i's for which the maximum is at least j_0, and M' the number of A_i's for which the maximum is exactly j_0 (i.e., M and M' take values in $\{0, 1, \ldots, 6\}$). Note that if $M' \geq 2$ then the lottery fails. Also note that

$$Pr[M' \geq 2|A] \geq Pr[M \geq 2|A] - Pr[\max \geq j_0 + 1|A].$$

Since $m(A) = j_0$, we have $Pr[\max \geq j_0 + 1|A] \leq 1/2$. By the independence of choices between the A_i's and since for each of the A_i's $Pr(\max \geq j_0|A_i) > 1/2$, we get $Pr[M \geq 2|A] > 57/64$. All together we get that $Pr[M' \geq 2|A] \geq 57/64 - 1/2 = 25/64 > 1/3$. This contradicts the assumption that the algorithm succeeds with probability $2/3$ for any number of participants. □

As $m(N) \leq B$ and $m(1) \geq 1$, then the above claim implies $B \geq \log_6 N$. □

3 Lotteries with the Unique Winner Property

In this section we prove that any lottery with the unique winner property requires $\Omega(\log N)$ values. We start by proving it for the case that all players use the same probability distribution. Then, we prove the general case by reducing it to this special case.

Theorem 2: Let B be an integer. Let $\Pi_1, \ldots, \Pi_N$ be a lottery for N players, over the set $\{1, 2, \ldots, B\}$, such that $\Pi_1 = \ldots = \Pi_N \triangleq \Pi$. If the lottery has the unique winner property then $B \geq (\frac{1}{2} \log_6 N) - 2$.

Proof: The idea of the proof is the following: Let p_j be the probability, according to Π, to pick the number j. We consider the probabilities $p_1, p_2, \ldots, p_B$, and prove that for every t ($1 \leq t \leq N$) there must be one of the p_j's which is "close" to $\frac{1}{t}$. Otherwise, if all the p_j's are either "much bigger" than $\frac{1}{t}$ or "much smaller" than $\frac{1}{t}$ and there are t participants that choose numbers according to these probabilities, then with a high probability each number is either picked at least twice or is not picked at all. In such a case there is no number which is chosen by a single participant (i.e, no unique winner). Therefore, for every t there must be (at least) one of the p_j's which is "close" to $\frac{1}{t}$ and this implies the result.

More formally, suppose that $B < (\frac{1}{2} \log_6 N) - 2$ (otherwise, we are done). Let $m = 2B + 3$ and $0 < \alpha < 1$ be some small enough constant (e.g., $\alpha = 1/6$). We associate with every probability p_j ($1 \leq j \leq B$) a subinterval $I_j = [\ell_j, u_j]$ of $[0, 1]$ that contains p_j, in the following way: Let i (≥ 1) be the smallest integer such that $p_j \leq \alpha^i$ and such that α^i is not the right point of any $I_{j'}$, for $j' < j$. If such an i exists then $u_j = \alpha^i$ otherwise $u_j = 1$. Let i ($\leq m$) be the largest integer such that $p_j \geq \alpha^i$ and such that α^i is not the left point of any $I_{j'}$, for $j' < j$. If such an i exists then $\ell_j = \alpha^i$ otherwise $\ell_j = 0$. As $m = 2B + 3$, then by the way of constructing the subintervals I_j ($1 \leq j \leq B$) there exists an index $1 < i < m$ such that α^i does not belong to any of these subintervals. Consider the case where $t = 1/\alpha^i$ numbers are chosen. In this case we prove that with a "high probability" each "big" j (i.e., j such that $p_j \geq \alpha^{i-1}$) is chosen at least once and each "small" j (i.e., j such that $p_j \leq \alpha^{i+1}$) is not chosen at all:

$$\begin{aligned} Pr\left(\text{no "small" } j \text{ is picked} \mid t\right) &= 1 - Pr\left(\text{some "small" } j \text{ is picked} \mid t\right) \\ &\geq 1 - \sum_{j:p_j \leq \alpha^{i+1}} Pr\left(j \text{ is picked} \mid t\right) \\ &\geq 1 - \sum_{j:p_j \leq \alpha^{i+1}} t \cdot p_j \\ &= 1 - t \cdot \sum_{j:p_j \leq \alpha^{i+1}} p_j. \end{aligned}$$

By the construction of the subintervals I_j we can bound the p_j's in the above sum by the corresponding u_j's which form a geometric progression. Thus the sum is bounded by $\alpha^{i+1} \cdot \frac{1}{1-\alpha}$. Therefore,

$$Pr\left(\text{no "small" } j \text{ is picked} \mid t\right) \geq 1 - \frac{t \cdot \alpha^{i+1}}{1-\alpha}.$$

By the choice of t, this is equal to $\frac{1-2\alpha}{1-\alpha}$. By the choice of $\alpha = 1/6$, this is at least $4/5$. Similarly, we have:

$$\begin{aligned} Pr\left(\text{every "big" } j \text{ is picked} \mid t\right) &= 1 - Pr\left(\text{some "big" } j \text{ is not picked} \mid t\right) \\ &\geq 1 - \sum_{j:p_j \geq \alpha^{i-1}} Pr\left(j \text{ is not picked} \mid t\right) \\ &= 1 - \sum_{j:p_j \geq \alpha^{i-1}} (1-p_j)^t \end{aligned}$$

By the construction of the subintervals I_j we can bound the p_j's in the above sum by the corresponding ℓ_j's. Thus we have,

$$\sum_{j:p_j \geq \alpha^{i-1}} (1-p_j)^t \leq \sum_{j:p_j \geq \alpha^{i-1}} (1-\ell_j)^t$$

In addition, all the ℓ_j's in the last sum are of the form α^k, $k < i$, and $t = 1/\alpha^i$. Therefore, the last sum is less than

$$\sum_{j=1}^{i-1} e^{-(\frac{1}{\alpha})^{j-i}}.$$

By the choice of $\alpha = 1/6$ this sum is at most $1/5$, and therefore, the above probability is at least $4/5$. Therefore, with probability at least $3/5$ each "big" j is chosen at least once and each "small" j is not chosen at all. Hence, when there are $2t$ participants then with probability $\geq \frac{9}{25} > \frac{1}{3}$ each "big" j is chosen at least twice and each "small" j is not chosen at all. Therefore, with probability $> 1/3$ no number is chosen by a single participant – contradicting the requirement about the lottery. The only thing remained to be verified is that $2t \leq N$ (otherwise there are not enough participants). This follows from our choice of parameters: as $t = 1/\alpha^i$, $\alpha = 1/6$, $i < m$, $m = 2B+3$, and by assumption $B < (\frac{1}{2}\log_6 N) - 2$ then $t = 1/\alpha^i = 6^i \leq 6^{m-1} = 6^{2B+2} = 6^{\log_6 N - 2} < N/2$. The theorem follows. $\square$

In the following we extend the result of the previous theorem to the case where each participant P_i may use a different distribution Π_i. The proof is by a reduction to the case where all participants use the same distribution.

Theorem 3: Let B be an integer. Let $\Pi_1, \ldots, \Pi_N$ be a lottery for N players, over the set $\{1, 2, \ldots, B\}$. If the lottery has the unique winner property then $B \geq d \cdot \log_6 N$, for some constant d.

Proof: Assume towards a contradiction, that there exist distributions $\Pi_1, \ldots, \Pi_N$ defined over the set $\{1, \ldots, B\}$, for $B = d \log_6 N$, such that the unique winner property holds (and d is some constant). We construct a distribution Π over the same set that guarantees the unique winner property (with almost the same success probability[4]) for any $1 \leq \ell \leq N^{1/4}$, participants. By theorem 2 the result follows. The distribution Π is defined as follows:

Choose, uniformly at random $i \in \{1, \ldots, N\}$.
Choose a number in $\{1, \ldots, B\}$ *according to* Π_i.

Let $1 \leq \ell \leq N^{1/4}$ participants choose numbers according to Π. We say that the choice is *good* if each participant P_j chooses a different distribution Π_i. The first claim says that this happens with a high probability.

Claim 2: For any $1 \leq \ell \leq N^{1/4}$, the choice is good with probability at least $1 - \frac{1}{\sqrt{N}}$.

Proof: The probability that a pair of participants P_{j_1} and P_{j_2} choose the same Π_i is exactly $1/N$. Therefore, the probability that among ℓ participants there exists a pair that choose the same Π_i is no more than $\binom{\ell}{2} \cdot \frac{1}{N}$. As $\ell \leq N^{1/4}$ it implies that the choice is good with probability at least $1 - \frac{1}{\sqrt{N}}$. $\square$

Claim 3: For any $1 \leq \ell \leq N^{1/4}$, the probability of having a unique winner is at least $\frac{2}{3} \cdot (1 - \frac{1}{\sqrt{N}})$.

Proof: Clearly,

$$Pr(\textit{unique winner}) \geq Pr(\textit{unique winner} | \textit{choice is good}) \cdot Pr(\textit{choice is good}).$$

[4]Amplification of the success probability to $2/3$ can be done by picking pairs of numbers according to Π, which only slightly affects the constants.

The probability that the choice is good is at least $1 - \frac{1}{\sqrt{N}}$, by the previous claim. In such a case we are exactly in the same situation as in the original lottery. By assumption, this lottery guarantees unique winner with probability at least $2/3$ for any set of ℓ participants, hence this is certainly true for a random set of ℓ participants. The claim follows. $\square$

We defined a lottery for $N^{1/4}$ *identical* participants which has the unique winner property. Therefore, by Theorem 2, $B \geq c \log_6 N^{1/4}$, for some constant c, which completes the proof of the theorem. $\square$

References

[1] Bar-Yehuda R., O. Goldreich, and A. Itai. "On the time-complexity of broadcast in multi-hop radio networks: An exponential gap between determinism and randomization", *Journal of Computer and System Sciences*, 45:104–126, 1992.

[2] Gil J., Y. Matias, and U. Vishkin, "Toward a Theory of Nearly Constant Time Parallel Algorithms", *32nd IEEE Symp. on Foundations of Computer Science*, 1991, pp. 698–710.

[3] Kushilevitz E., and Y. Mansour, "An $\Omega(D \log(N/D))$ Lower Bound for Broadcast in Radio Networks", *12th ACM Symp. on Principles of Distributed Computing*, August 1993, pp. 65-74.

[4] Kushilevitz E., Y. Mansour, M. O. Rabin, and D. Zuckerman, "Lower Bounds for Randomized Mutual-Exclusion", *25th ACM Symp. on Theory of Computation*, May 1993, pp. 154-163.

[5] Kushilevitz E., and M. O. Rabin, "Randomized Mutual Exclusion Algorithms Revisited", *11th ACM Symp. on Principles of Distributed Computing*, 1992, pp. 275–283.

[6] Matias Y., and Y. Afek, "Simple and Efficient Election Algorithms for Anonymous Networks", Proc. of WDAG, Lecture Notes in Computer Science Vol. 392, pp. 183-194.

[7] Rabin, M. O., "N-Process Mutual Exclusion with Bounded Waiting by $4 \log_2 N$-Valued Shared Variable", *Journal of Computer and System Sciences*, Vol. 25 (1), 1982, pp. 66-75.