

# A Combinatorial Approach to Ebert's Hat Game with Many Colors

Uthaipon Tantipongpipat

University of Richmond  
Richmond, Virginia, U.S.A.

uthaipon.tantipongpipat@richmond.edu

Submitted: May 15, 2014; Accepted: Nov 4, 2014; Published: Nov 13, 2014

Mathematics Subject Classifications: 05B40, 91A12, 91A46

## Abstract

This paper proves an optimal strategy for Ebert's hat game with three players and more than two hat colors. In general, for  $n$  players and  $k$  hat colours, we construct a strategy that is asymptotically optimal as  $k \rightarrow \infty$ . Computer calculation for particular values of  $n$  and  $k$  suggests that, as long as  $n$  is linear with  $k$ , the strategy is asymptotically optimal. We conclude by comparing our strategy with the strategy of Lenstra and Seroussi and with the bound of Alon, and suggest our strategy is better when  $2k \geq n \geq 7$ .

## 1 The Problem

There have been several different versions of hat games and various generalizations of the games' rules. For example, the paper [1] discusses the "hybrid" hat game that combines rules from a hat game where players stand on a single line and the Ebert's hat game, with the generalization on the number of hat colors. In this paper, we will focus on Ebert's hat game, and the generalization on the number of possible hat colors.

The simple version of Ebert's hat game is stated as follows [2]: three players walk into a room and each of them is given a hat. Each hat is either red or blue, and the probabilities of the colors of each of the three hats are equally and independently distributed. Each player can see the colors of the other players' hats but cannot see the color of his own hat. No communication of any type is allowed after the players walk into the room. After each player looks at the other players' hats, each of them has to guess the color of his own hat or pass. Each player does not know what the other players' responses are. They win collectively if at least one of the players guesses the color of his own hat correctly and no other player guesses incorrectly. Otherwise (if at least one player guesses incorrectly or everyone passes), they lose. Before the three players walk into the room and receive

hats, they may plan a strategy of responses. The question is: What is the best strategy to optimize the chance of winning?

In this paper we will use  $n$  as the number of players and  $k$  as the number of colors in Ebert's hat game. The simple version above ( $n = 3$  and  $k = 2$ ) has a proven optimal strategy with a winning probability of  $3/4$ .<sup>1</sup> In fact, for  $k = 2$  and  $n = 2^m - 1$  for some positive integer  $m > 1$ , there is a proof of the optimal strategy [5]. The solution when  $n = 2^m - 1$  is tied closely with the particular structure of the set of losing positions known as the 1-error-correcting binary Hamming Code. The question is: what about when  $k > 2$ ?

In this paper, we will show, with a combinatorial optimization proof, the optimal strategy for Ebert's hat game with  $n = 3$  and  $k > 2$ . (The case  $n = 1$  is trivial. For  $n = 2$ , fix one color  $c_0$ . The strategy is to instruct each player to guess  $c_0$  if he does not see  $c_0$ , and pass otherwise. It is easy to show that the strategy is optimal with the winning probability  $2(k - 1)/k^2$ .) There has been a construction of strategy for Ebert's hat game with three players and  $k$  colors [3]. With the case  $k = 3$ , that strategy is proved to be optimal in [3]. However, it was not known whether that strategy is optimal for any  $k > 3$ . We will show in this paper that the strategy is indeed optimal.

Furthermore, we will construct a strategy for general  $n$  and  $k$ , and compare the winning probability of that strategy with Lenstra and Seroussi's strategy [5] and Alon's lower bound [4, Theorem 7.1]. Computer search suggests that our strategy has a higher winning probability when  $2k \geq n \geq 7$  than Lenstra and Seroussi's strategy and Alon's bound. We discuss that Lenstra and Seroussi's strategy and Alon's bound are not preferable in the case  $k$  being linear with  $n$ . We prove an upper bound for the probability of winning of  $\lfloor \frac{nk^n - 1}{n + k - 1} \rfloor / k^n$ , and we show that our strategy's winning probability approaches this bound for fixed  $n$  while  $k$  approaching infinity. In addition, computer calculation leads to a conjecture that in the case  $k$  being linear with  $n$ , and we let  $n \rightarrow \infty$ , then the probability of winning still approaches this same upper bound.

## 2 Three Players and more than Two Colors

Let  $k > 2$  be a positive integer. Label the colors  $1, 2, \dots, k$ . In the 3-player Ebert's hat game, each player receives a hat from among the  $k$  equally probable colors. Let

$$S = \{(a, b, c) : a, b, c \in \{1, 2, 3, \dots, k\}\}$$

represent all equally probable  $k^3$  outcomes of hat colors distributed among three players. The first number in a triple represents the color of the first player's hat, and so on.

For a given strategy, let  $X \subseteq S$  be the set of all losing positions, and  $W \subseteq S$  be the set of all winning positions. Each possibility will be either a winning or losing position (A typical strategy that instructs a player to definitely do a certain action is called a

---

<sup>1</sup>**Disclaimer: Spoiler for a solution.** The strategy instructs a player when sees two other hats of a same color to guess the opposite of that color, and pass otherwise. That strategy will give a winning probability 6 out of 8 possibilities.

deterministic strategy. A strategy that instructs a player to do one of more than one possible responses according to the given probabilities (a non-deterministic strategy) will give a winning probability as a linear combination of other deterministic strategies. It therefore is sufficient to consider only all possible deterministic strategies [5]). Therefore,  $(X, W)$  is a partition of  $S$ . Also, any given strategy will determine the sets  $X$  and  $W$ .

**Definition 1.** A **line** is a set of  $k$  triples in  $S$  all of which have the same coordinates in two dimensions. For example,  $\{(1, 3, 4), (2, 3, 4), \dots, (k, 3, 4)\}$  and  $\{(1, 1, 4), (1, 2, 4), \dots, (1, k, 4)\}$  are both lines.

**Definition 2.** For each  $w \in W$ , a line consisting of  $k - 1$  losing positions and  $w$  is called a **supporting line** of  $w$ . If there can be more than one supporting line for  $w$ , pick only one to be a supporting line for  $w$ .

The following theorem is the same as the Claim in [4, Section 7], but we quote it in terms of a supporting line.

**Theorem 3.** *The given partition of  $S$  into  $X$  and  $W$  will represent a possible strategy if and only if each  $w \in W$  has a supporting line.*

Because of Theorem 3, from now on it is sufficient to maximize the size of  $W$  subject to the condition that for each  $w \in W$ , there exists a line consisting of  $k - 1$  losing positions and  $w$ .

We consider the strategy as appeared in [3, Subsection 29.4], which satisfies  $|W| = 3k^2 - 6k + 6$ , and now demonstrate that this strategy is optimal.

Assume that there exists a possible strategy corresponding to a pair  $(X, W)$  such that  $|W| \geq 3k^2 - 6k + 7$ . If  $|W| \geq 3k^2 - 6k + 8$ , we can choose one of the winning positions and turn that into a losing position. The new pair  $(X, W)$  will still hold the condition that for each  $w \in W$ , there exists a line consisting of  $k - 1$  losing positions and  $w$ . Therefore, it is sufficient to consider only when  $|W| = 3k^2 - 6k + 7$  and prove that  $|W| = 3k^2 - 6k + 7$  is impossible. Assume  $|W| = 3k^2 - 6k + 7$ . Since  $|W| + |X| = k^3$ , we have  $|X| = k^3 - 3k^2 + 6k - 7$ . Let  $L$  be the set of all  $3k^2 - 6k + 7$  supporting lines in this strategy. Let

$$C = \{(x, l) \in X \times L : x \in l\}$$

Since each  $w \in W$  has exactly one supporting line, which corresponds to exactly  $k - 1$  elements in  $C$ ,  $|C| = (k - 1)|W|$ . Let

$$M = \{(x, l) : x \in X, l \text{ is a line, and } x \in l\} - C$$

Then,  $M$  and  $C$  are disjoint, and we get

$$|M| + |C| = |\{(x, l) : x \in X, l \text{ is a line, and } x \in l\}| = 3|X| \tag{1}$$

since any position in  $S$  is contained in exactly three different lines. We split the  $S$  into  $k$  planes  $P_1, P_2, P_3, \dots, P_k$ , where  $P_i = \{(i, b, c) \in S : 1 \leq b, c \leq k\}$ . Let  $M_i = T_i - C$ , where

$$T_i = \{(x, l) : x \in P_i \cap X, l \text{ is a line in } P_i, \text{ and } x \in l\}$$

Let  $a_i$  denote the number of losing positions in  $P_i$ . For any  $a_i \in \{0, 1, 2, \dots, k^2\}$ , let  $h(a_i)$  denote the minimum possible size of  $M_i$  given that there are  $a_i$  losing positions in that plane  $i$ . We will find a lower bound for  $\sum_{i=1}^k h(a_i)$  subject to the condition  $\sum_{i=1}^k a_i =$  total number of losing positions  $= k^3 - 3k^2 + 6k - 7$ . We state several Lemmas in order to find the bound. Lemmas 4, 5, 6, 8, and 9 below are stated with the detailed proofs and calculations deferred to Appendix A.

**Lemma 4.** *The sum  $\sum_{i=1}^k h(a_i)$  can be minimized by only considering  $a_i \leq (k-1)^2$  for all  $i = 1, 2, \dots, k$ .*

Intuitively, this is because having “too many” losing positions will not give enough spaces for winning positions to use supporting lines formed within that plane.

For each  $m \in \{0, 1, 2, \dots, 2(k-1)\}$ , let  $f(m)$  denote the minimum number of losing positions in the plane that is needed to generate  $m$  supporting lines in that plane.

**Lemma 5.** *For all  $m \in \{0, 1, 2, \dots, 2(k-1)\}$ ,*

$$f(m) = \begin{cases} (k-1)m - \left(\frac{m}{2}\right)^2 & \text{if } m \text{ is even} \\ (k-1)m - \left(\frac{m}{2}\right)^2 + \frac{1}{4} & \text{if } m \text{ is odd} \end{cases}$$

The idea is to try to let as many losing positions as possible to be in two supporting lines.

For each  $a_i \in \{0, 1, 2, \dots, (k-1)^2\}$ , let  $g(a_i)$  denote the maximum possible number of supporting lines in the plane that can be created given that there are  $a_i$  losing positions in that plane.

**Lemma 6.** *For all  $a_i \in \{0, 1, 2, \dots, (k-1)^2\}$ ,*

$$g(a_i) \leq 2k - 2 + \left\lfloor -2\sqrt{(k-1)^2 - a_i} \right\rfloor$$

The lemma can be proved using  $f(a_i)$  in Lemma 5. We now show how defining  $g(a_i)$  may help us to find  $h(a_i)$ .

**Lemma 7.** *For all  $a_i \in \{0, 1, 2, \dots, (k-1)^2\}$ ,*

$$h(a_i) = 2a_i - (k-1)g(a_i)$$

*Proof.* Each losing position increases the size of  $T_i$  by 2, and each supporting line in the plane  $P_i$  corresponds to  $k-1$  ordered pairs in  $C$  which decreases the size of  $M_i$  by  $k-1$ . Thus,  $h(a_i) = 2a_i - (k-1)g(a_i)$ .  $\square$

Now, we use these Lemmas to finally find a lower bound for  $\sum_{i=1}^k h(a_i)$  subject to two conditions:  $\sum_{i=1}^k a_i = k^3 - 3k^2 + 6k - 7$  and (from Lemma 4)  $a_i \leq (k-1)^2$  for all  $i = 1, 2, 3, \dots, k$ .

**Lemma 8.**  $\sum_{i=1}^k h(a_i) \geq 4k - 10$

This can be done by translating  $h(a_i)$  into  $g(a_i)$  term and give an upper bound to the sum

$$\sum_{i=1}^k \left( 2k - 2 + \left\lfloor -2\sqrt{(k-1)^2 - a_i} \right\rfloor \right).$$

Note that we split the entire cube  $S$  into  $k$  planes  $P_1, P_2, P_3, \dots, P_k$  in order to obtain the lower bound on  $\sum_{i=1}^k h(a_i)$ . However, we could have done the splitting in two other similar ways but in different orientations of the cubes. Applying similar idea of Lemma 8 to all three ways of splitting and using double counting argument, we get the bound for  $|M|$ :

**Lemma 9.**  $|M| \geq 6k - 15$

We are now ready to state the main result in this section, namely that the strategy for winning Ebert's hat game in [3, Subsection 29.4] is optimal.

**Theorem 10.** (3-Player Multicolor Game Theorem) *The maximum number of winning positions for the 3-player  $k$ -color hat game, where  $k > 2$ , is  $3k^2 - 6k + 6$ .*

*Proof.* Suppose  $|W| = 3k^2 - 6k + 7$ . From (1),  $|M| + |C| = 3|X|$ . Thus,

$$\begin{aligned} |C| &= 3|X| - |M| = 3(k^3 - 3k^2 + 6k - 7) - |M| \\ &\leq 3(k^3 - 3k^2 + 6k - 7) - (6k - 15) \\ &= 3k^3 - 9k^2 + 12k - 6 \end{aligned}$$

Since  $|C| = (k-1)|W|$ , we have

$$\begin{aligned} |W| &= \frac{|C|}{k-1} \\ &\leq \frac{3k^3 - 9k^2 + 12k - 6}{k-1} \\ &= 3k^2 - 6k + 6 \end{aligned}$$

By contradiction to  $|W| = 3k^2 - 6k + 7$ , we get the result. □

### 3 The General Case

We now consider Ebert's hat game with more than three players. First, we will look at the case where  $2k \geq n$ : in other words, we have a large number of colors relative to the number of players.

## Case $2k \geq n$ :

Label the colors  $1, 2, 3, \dots, k$ . Consider a symmetric strategy as follows:

For  $i = 1$  to  $k$ , if a player does not see a hat of color  $i$ , guess  $i$ . If a player sees one hat of color  $i$ , pass. If a player sees two or more hats of color  $i$ , increment  $i$  and repeat the process.

Now, we will find the winning probability from this strategy. Let

$$S = \{(c_1, c_2, c_3, \dots, c_n) : c_i \in \{1, 2, 3, \dots, k\}\}$$

be the set of all  $k^n$  possibilities of colors of  $n$  hats, where  $c_i$  represents the color of the hat of player  $i$ .

**Definition 11.** Let  $c = (c_1, c_2, c_3, \dots, c_n) \in S$ . Let  $d_j$  be the number of appearances of color  $j$  in  $c_1, c_2, \dots, c_n$ . Then,  $c$  has property  $\mathcal{P}_0$  if 1 appears before 0 in the sequence  $d_1, d_2, \dots, d_k$ .

**Theorem 12.** An element  $(c_1, c_2, c_3, \dots, c_n) \in S$  is a winning position according to the strategy described above if and only if  $(c_1, c_2, c_3, \dots, c_n)$  satisfies the property  $\mathcal{P}_0$ .

*Proof.* First, suppose an element  $c \in S$  has the property  $\mathcal{P}_0$  with the least positive integer  $i$  appears exactly once. It is clear to see that the player with hat color  $i$  will guess correctly and the rest will pass. Hence, the team will win. Second, suppose we have an element  $c \in S$  that does not satisfy the property  $\mathcal{P}_0$ . Let  $i$  be the least positive integer that does not appear more than once. Since  $i$  does not appear, any player with a hat color  $d > i$  will incorrectly guess color  $i$ , so the team will lose. If there is no player with a hat color  $d > i$ , i.e.  $2k = n$  and each color appears two times, every player will pass, and the team will lose.  $\square$

**Theorem 13.** The number of winning positions in the strategy we constructed (where  $2k \geq n$ ) is

$$n! \sum_{i=0}^{n-1} (-1)^{n-1+i} \frac{k^i}{i!}$$

*Proof.* The number of winning positions of the strategy is equal to the number of elements in  $S$  that has the property  $\mathcal{P}_0$ . In order to count that, we will use generating functions. The degree of the term will represent the length of the string of numbers constructed. The factorial in the denominator of a term represents all permutations of the same numbers being considered the same. Therefore, the number of elements satisfying  $\mathcal{P}_0$  with  $i$  being the least positive integer that appears once is the coefficient of the term  $\frac{x^n}{n!}$  in  $\left(\frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \dots\right)^{i-1} x \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots\right)^{k-i}$ . Thus, the total number of elements

satisfying  $\mathcal{P}_0$  is the coefficient of the term  $\frac{x^n}{n!}$  in

$$\begin{aligned} & \sum_{i=1}^k \left( \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \dots \right)^{i-1} x \left( 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \right)^{k-i} \\ &= x \frac{\left( 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \right)^k - \left( \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \right)^k}{\left( 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \right) - \left( \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \right)} \\ &= x \frac{(e^x)^k - (e^x - x - 1)^k}{x + 1} \\ &= x (1 - x + x^2 - x^3 + \dots) \left( (e^x)^k - (e^x - x - 1)^k \right) \end{aligned}$$

Since  $e^x - x - 1$  has only terms with degree at least 2,  $(e^x - x - 1)^k$  has only terms with degree at least  $2k$ . Therefore, the term  $(e^x - x - 1)^k$  in the expression (3.1) will only contribute terms with degree at least  $2k + 1$ , which, from  $2k \geq n$ , is at least  $n + 1$ . However, we consider only the term of degree  $n$ , so we can neglect  $(e^x - x - 1)^k$ . The expression then becomes

$$x (1 - x + x^2 - x^3 + \dots) (e^x)^k = x (1 - x + x^2 - x^3 + \dots) \left( 1 + \frac{kx}{1!} + \frac{(kx)^2}{2!} + \dots \right)$$

And the coefficient of  $\frac{x^n}{n!}$  is

$$n! \sum_{i=0}^{n-1} (-1)^{n-1+i} \frac{k^i}{i!}$$

as desired. □

### Case $2k < n$ :

A more general strategy is as follows:

For  $i = 0$  to  $\lfloor \frac{n-1}{2k} \rfloor$ :

For  $j = 1$  to  $k$ : if a player sees exactly  $2i$  hats of color  $j$ , guess  $j$ . If a player sees exactly  $2i + 1$  hats of color  $j$ , pass. Else, go to the next case.

The following definition is the natural generalization of  $\mathcal{P}_0$ .

**Definition 14.** Let  $c = (c_1, c_2, c_3, \dots, c_n) \in S$ . Let  $d_j$  be the number of appearances of color  $j$  in  $c_1, c_2, \dots, c_n$ . Then, for each non-negative integer  $i$ ,  $c$  has property  $\mathcal{P}_i$  if  $d_j \geq 2i$  for all  $j$ , and  $2i + 1$  appears before  $2i$  in the sequence  $d_1, d_2, \dots, d_k$ .

Analogously to Theorem 12, we can prove that the sequence of  $n$  integer will represent a winning position if and only if that sequence satisfies  $\mathcal{P}_i$  for some  $i$ . The number of sequences in which every integer appears at least  $2i$  times, and the least integer  $j \in \{1, 2, 3, \dots, k\}$  which appears no more than  $2i + 2$  times appears exactly  $2i + 1$  times is

the coefficient of  $\frac{x^n}{n!}$  in  $(E_{2i+2}(x))^{j-1} \left(\frac{x^{2i+1}}{(2i+1)!}\right) (E_{2i}(x))^{k-j}$ , where  $E_a(x) = \sum_{i=a}^{\infty} \frac{x^i}{i!}$ . The total number of winning positions then is the coefficient of  $\frac{x^n}{n!}$  in

$$\sum_{i=0}^{\infty} \sum_{j=1}^k (E_{2i+2}(x))^{j-1} \left(\frac{x^{2i+1}}{(2i+1)!}\right) (E_{2i}(x))^{k-j}$$

With some computation, we deduce that the number of winning positions is the coefficient of  $\frac{x^{n-1}}{n!}$  in

$$\sum_{i=0}^{n-1} (-1)^{n-1+i} \frac{k^i}{i!} x^{n-1} + \sum_{i=1}^{\lfloor \frac{n-1}{2k} \rfloor} \left( \sum_{j=0}^{n-1-2ik} (-1)^j ((2i+1)^{-j-1} - (2i-1)^{-j-1}) x^j \right) (E_{2i}(x))^k \tag{2}$$

This expression may be more helpful when is used by computer to calculate the exact coefficient of  $\frac{x^{n-1}}{n!}$ .

## 4 The Behavior of the Constructed Strategy

In this paper, the symbol  $\sim$  means that the ratio of quantities in the left and right is approaching one. Before we start, consider the simple upper bound for  $|W|$ . The bound  $|W| \leq \frac{nk^n}{n+k-1}$  is stated in [5] and [3], and proved in [3]. Proposition 5 in [5, Subsection 3.1] implies that there is no strategy which gives  $|W|$  to be exactly  $\frac{nk^n}{n+k-1}$  for any  $k > 2$ . The paper, however, does not include the proof of that proposition. The following theorem can be used to prove both the bound and the proposition.

**Theorem 15.** *For all  $n, k \geq 3$ ,*

$$|W| \leq \left\lfloor \frac{nk^n - 1}{n + k - 1} \right\rfloor$$

*Proof.* We can generalize the definition and Theorem 3 to general  $n$  as well. That is, define

$$S = \{1, 2, 3, \dots, k\}^n$$

The line is a set of  $k$  triples in  $S$  all of which have the same coordinates in  $k-1$  dimensions. Use the same definition of a supporting line. Then, Theorem 3 is still true for all general  $n$  and  $k$  (the proof is analogous). Similarly, define  $L$  as the set of all supporting lines, and define

$$\begin{aligned} C &= \{(x, l) \in X \times L : x \in l\} \\ M &= \{(x, l) : x \in X, l \text{ is a line, and } x \in l\} - C \end{aligned}$$

Since there can be  $n$  lines passing through a position, every losing position will be counted exactly  $n$  times in  $\{(x, l) : x \in X, l \text{ is a line, and } x \in l\}$ . Also, because

$$C \subseteq \{(x, l) : x \in X, l \text{ is a line, and } x \in l\}$$



Table 1: Ratio  $|W|/\lfloor \frac{nk^n-1}{n+k-1} \rfloor$  in different values of  $n$  and  $k$ . The value close to 1 shows when the strategy gives a winning probability close to the upper bound

$n \backslash k$	3	5	7	10	20	50	100	250
10	0.7158	0.9505	0.9642	0.9743	0.9889	0.9973	0.9992	0.99987
50	0.5722	0.6433	0.7116	0.8111	0.9897	0.9950	0.9978	0.99945
250	0.5271	0.5509	0.5724	0.6029	0.6973	0.9678	0.9980	0.99900

We get  $|M| = n|X| - |C|$ . Since each winning position will be counted exactly  $k - 1$  times in  $C$ , we have

$$\begin{aligned} |M| &= n|X| - (k - 1)|W| \\ |M| &= n(k^n - |W|) - (k - 1)|W| \\ |W| &= \frac{nk^n - |M|}{n + k - 1} \end{aligned}$$

Now, suppose  $|M| = 0$ . Then,  $|X| = k^n - |W| = \frac{(k-1)k^n}{n+k-1}$ . We split  $S$  into  $k^{n-2}$  non-intersecting planes  $P_1, P_2, \dots, P_{k^{n-2}}$ , and let  $a_i$  be the number of losing positions in the  $i^{\text{th}}$  plane. Because  $|M| = 0$ , we must have  $h(a_i) = 0$  for all  $i = 1, 2, 3, \dots, k^{n-2}$  (here we use the same definition for  $M_i, T_i$ , and  $h$  as in the proof of the 3-player game). However,  $h(a_i) = 0$  if and only if  $a_i = 0$  or  $(k - 1)^2$ . Therefore,  $|X| = \sum_{i=1}^{k^{n-2}} a_i$  must be a multiple of  $(k - 1)^2$ . We have  $(k - 1)^2 \mid |X|$ , which is the same as  $(k - 1)^2 \mid \frac{(k-1)k^n}{n+k-1}$ . This gives  $k - 1 \mid k^n$ , and so  $k - 1 \mid 1$ . But for all  $k > 2$ , this is impossible. Therefore,  $|M| \geq 1$ . This gives

$$|W| = \frac{nk^n - |M|}{n + k - 1} \leq \frac{nk^n - 1}{n + k - 1}$$

Because  $|W|$  is an integer,

$$|W| \leq \left\lfloor \frac{nk^n - 1}{n + k - 1} \right\rfloor. \quad \square$$

From the last section, we have a construction of the strategy with

$$|W| = \begin{cases} \text{Coefficient of } x^{n-1}/n! \text{ in the expression (3.2)} & \text{if } 2k < n \\ n! \sum_{i=0}^{n-1} (-1)^{n-1+i} \frac{k^i}{i!} & \text{if } 2k \geq n \end{cases}$$

We will investigate the ratio of  $|W|$  from this construction to the upper bound  $\lfloor \frac{nk^n-1}{n+k-1} \rfloor$ . Some values are shown in Table 1. More samples are shown in Appendix B.

One observation is that the ratio gets close to 1 as  $k$  grows. The computation suggests that for  $n \geq 50$ , one need  $k \geq n/2$  for the probability to be at least 99% of the simple upper bound, and as  $n$  grows, the ratio  $k/n$  we need to attain the same 99% ratio seems to get smaller. Below is the mathematical proof that the strategy indeed is asymptotically optimal as  $k \rightarrow \infty$ .

Table 2: Ratio  $|W|/\lfloor \frac{nk^n-1}{n+k-1} \rfloor$  when  $\alpha = 0.25$  as  $n$  increases

$n$	12	20	28	40	100	200	400	1000
$ W /\lfloor \frac{nk^n-1}{n+k-1} \rfloor$	0.6999	0.7767	0.8222	0.8721	0.9727	0.9955	0.9984	0.9994

Table 3: Ratio  $|W|/\lfloor \frac{nk^n-1}{n+k-1} \rfloor$  when  $\alpha = 0.15$  as  $n$  increases

$n$	20	40	60	100	200	300	500	1000
$ W /\lfloor \frac{nk^n-1}{n+k-1} \rfloor$	0.6342	0.7082	0.7438	0.7867	0.8358	0.8618	0.8984	0.9521

**Theorem 16.** For any fixed positive integer  $n$ , as  $k \rightarrow \infty$ ,

$$|W| \sim \left\lfloor \frac{nk^n - 1}{n + k - 1} \right\rfloor$$

*Proof.* Because  $n$  is fixed and  $k$  is growing, we can assume  $2k \geq n$  and use  $|W| = n! \sum_{i=0}^{n-1} (-1)^{n-1+i} \frac{k^i}{i!}$ . Then,

$$\frac{|W|}{\lfloor \frac{nk^n-1}{n+k-1} \rfloor} \sim \frac{|W|}{\frac{nk^n}{n+k-1}} = \frac{(n+k-1)(n! \sum_{i=0}^{n-1} (-1)^{n-1+i} \frac{k^i}{i!})}{nk^n}$$

As  $k \rightarrow \infty$ , since both numerator and denominator are a polynomial of variable  $k$  of degree  $n$ , we only need to take ratio of the coefficients of the leading terms  $k^n$ . Thus,

$$\lim_{k \rightarrow \infty} \frac{(n+k-1)(n! \sum_{i=0}^{n-1} (-1)^{n-1+i} \frac{k^i}{i!})}{nk^n} = \lim_{k \rightarrow \infty} \frac{(1)(n!)(\frac{1}{(n-1)!})}{n} = 1. \quad \square$$

The upper incomplete gamma function is defined as  $\Gamma(n, -k) = \int_{-k}^{\infty} t^{n-1} e^{-t} dt$ . When  $n$  is a positive integer, by induction on  $n$ ,  $\Gamma(n, -k)$  is equal to  $(n-1)! e^k \sum_{i=0}^{n-1} \frac{(-k)^i}{i!}$ . Therefore,  $|W| = n! \sum_{i=0}^{n-1} (-1)^{n-1+i} \frac{k^i}{i!}$  can be written as  $|W| = n(-1)^{n-1} e^{-k} \Gamma(n, -k)$ . Then, Theorem 16 can also be viewed as the asymptotic behavior of the incomplete gamma function  $\Gamma(n, -k)$  as  $n$  is fixed and  $k \rightarrow \infty$ .

We also investigate the asymptotic behavior in the case when  $k$  is linear with  $n$ . Table 2 and 3 provide some evidences that the ratio  $|W|/\lfloor \frac{nk^n-1}{n+k-1} \rfloor$  still approaches 1 as  $n \rightarrow \infty$ , which lead us to Conjecture 17.

**Conjecture 17.** As long as  $k \geq \alpha n$ , for some fixed positive real  $\alpha$ , then as  $n \rightarrow \infty$ ,

$$|W| \sim \left\lfloor \frac{nk^n - 1}{n + k - 1} \right\rfloor \sim \frac{nk^n}{n + k}$$

The convergence seems to be slower if  $\alpha$  is closer to 0. If we constrain this conjecture only with  $\alpha \geq 1/2$ , we can look at the conjecture in two other perspectives:

1. From the conjecture  $|W| = n! \sum_{i=0}^{n-1} (-1)^{n-1+i} \frac{k^i}{i!} \sim \frac{nk^n}{n+k}$ , multiply by  $-1$ , add  $k^n$ , and then divide by  $n!$  to both sides. The conjecture is then equivalent to the approximation of a finite alternating exponential series:

$$(-1)^n \sum_{i=0}^n (-1)^i \frac{k^i}{i!} \sim \frac{k^{n+1}}{(k+n)n!}$$

The approximation of a finite alternating exponential series seems to be more precise than to think about Taylor series expansion of  $e^{-k}$ , since the next term of the Taylor series  $\frac{k^{n+1}}{(n+1)!} \gtrsim \frac{\alpha(\alpha e)^n}{\sqrt{2n\pi}}$  (from Stirling's approximation) which bounds the error grows to infinity.

2. From  $|W| = n(-1)^{n-1}e^{-k}\Gamma(n, -k)$ , the statement  $|W| \sim \frac{nk^n}{n+k}$  is equivalent to

$$(-1)^{n-1}\Gamma(n, -k) \sim \frac{e^k k^n}{n+k}$$

which implies,

$$|\Gamma(n, -k)| \sim \frac{e^k k^n}{n+k}$$

This last statement may be further investigated whether it still holds for general  $n, k$  in some real and/or complex domain.

Now we will compare the combinatorial strategy constructed in this paper to Lenstra and Seroussi's and Alon's bound. Specifically, we want to know in what case our strategy will have higher winning probability and observe asymptotic behaviors in the case  $k = \alpha n$  for some  $\alpha > 0$  as well.

## Comparison with Lenstra and Seroussi's strategy

Lenstra and Seroussi's strategy [5] is constructed using the algebraic method and matrix multiplication so that the probability of winning  $1 - \left(1 - \frac{1}{k}\right)^{\log_2(n+1)}$  approaches 1 as  $n \rightarrow \infty$ . However, as  $k$  grows, even moderately around a hundred, the probability goes down rapidly. In other words, the strategy is good for big  $n$ , but not with big  $k$ , whereas the combinatorial strategy in this paper works well for big  $k$ . Examples of performance of this strategy is shown in Table 5 in Appendix B.

**Conjecture 18.** When  $2k \geq n \geq 7$ , the winning probability of the combinatorial strategy in this paper is greater than  $1 - \left(1 - \frac{1}{k}\right)^{\log_2(n+1)}$ .

Also, if  $2k$  is still "close enough" to  $n$ , such as when  $n = 50$  and  $k = 10$  or  $20$ , the winning probability from combinatorial construction seems to be greater as well. How exactly "close" it should be is still unknown.

If we have  $k = \alpha n$  for some  $\alpha > 0$ , then as  $n \rightarrow \infty$ , the ratio

$$\frac{1 - \left(1 - \frac{1}{k}\right)^{\log_2(n+1)}}{\left\lfloor \frac{nk^n - 1}{n+k-1} \right\rfloor / k^n} \approx (\alpha + 1) \left(1 - \left(1 - \frac{1}{\alpha n}\right)^{\log_2(n)}\right)$$

will converge to 0 because  $\left(1 - \frac{1}{\alpha n}\right)^{\log_2(n)}$  converges to 1.

## Comparison with Alon's bound

Alon's paper [4] uses a probabilistic argument to show an existence of a strategy with probability of winning at least  $1 - m\left(\frac{k-1}{k}\right)^n - \frac{1}{n}$ , where  $m = \left\lceil \frac{k^n \log n}{(k-1)^{n-1}n} \right\rceil$ . The bound obtained is good for the asymptotic behavior  $n \rightarrow \infty$ , which is even better than Lenstra and Seroussi's when  $n$  is big enough. For example, roughly  $n \geq 500$  for  $k = 3$ . Again, the strategy however does not work well when  $k$  grows. Examples of performance of this strategy is shown in Table 6 in Appendix B.

**Theorem 19.** *When  $2k \geq n \geq 7$ , the winning probability of the combinatorial strategy in this paper is greater than  $1 - \left\lceil \frac{k^n \log n}{(k-1)^{n-1}n} \right\rceil \left(\frac{k-1}{k}\right)^n - \frac{1}{n}$ .*

*Proof.*

$$\begin{aligned} 1 - \left\lceil \frac{k^n \log n}{(k-1)^{n-1}n} \right\rceil \left(\frac{k-1}{k}\right)^n - \frac{1}{n} &\leq 1 - \frac{k^n \log n}{(k-1)^{n-1}n} \left(\frac{k-1}{k}\right)^n - \frac{1}{n} \\ &= 1 - \frac{(k-1) \log n + 1}{n} \\ &\leq 1 - \frac{(n-2) \log n + 2}{2n} \end{aligned} \tag{3}$$

The last expression is a function of  $n$ , where after  $n \approx 9.61$ , will be less than 0. For  $n = 7, 8, 9$ , we can compute directly that the statement is true.  $\square$

As we can see from the proof in Theorem 19, Alon's bound itself does not give any information for  $k \geq 2n$ . In fact, for any  $\alpha > 0$ , if  $k \geq \alpha n$  ( $k$  linear with  $n$ ) and  $n \rightarrow \infty$ , the bound still eventually will not be useful. This is because  $\frac{(k-1) \log n + 1}{n}$  will asymptotically behave to be at least  $\alpha \log n$ , and so the term (3) will become negative as  $n$  grows.

## 5 Conclusion

It is interesting to see how different approaches solve the same hat problem. The combinatorial approach seems to work well with low values of  $n$  and big values of  $k$ , and with asymptotically when  $k \geq \alpha n$  for some  $\alpha > 0$ . In fact, the strategy seems to approach the proven upper bound. In contrast, when  $n$  gets bigger, for example when  $n$  is much bigger than  $2k$ , or when  $n \rightarrow \infty$  while  $k$  is fixed, Lenstra and Seroussi's and Alon's strategies may be better alternatives. Between Lenstra and Seroussi's and Alon's strategies, when  $n \rightarrow \infty$  with fixed  $k$ , Alon's bound converges closer to 1, with the exception of some moderate values of  $n$ .

## Acknowledgements

I want to thank Dr. James Davis of University of Richmond for introducing Ebert's hat puzzle to me and for reading this paper before its final draft.

## References

- [1] M. B. Paterson and D. R. Stinson. Yet another hat game. *The Electronic Journal of Combinatorics*, 17:#R86, 2010. <http://www.combinatorics.org/ojs/index.php/eljc/article/view/v17i1r86>
- [2] S. Robinson. *Why mathematicians now care about their hat color*. New York Times, April 10, 2001. <http://www.nytimes.com/2001/04/10/science/why-mathematicians-now-care-about-their-hat-color.html>
- [3] W. Guo, S. Kasala, M. B. Rao, and B. Tucker. The hat problem and some variations, in *Advances in Distribution Theory, Order Statistics, and Inference*, pages 459-479. Springer, 2006.
- [4] N. Alon. Problems and results in extremal combinatorics II, in *Discrete Mathematics*, 308(19):4460–4472, 2008. [doi:10.1016/j.disc.2007.08.090](https://doi.org/10.1016/j.disc.2007.08.090)
- [5] H. W. Lenstra and G. Seroussi. On Hats and other covers (extended summary), 2005. [arXiv:cs/0509045](https://arxiv.org/abs/cs/0509045)

## A Proofs of Lemmas

*Proof of Lemma 4.* First, consider  $h(a_i)$  when  $a_i > (k - 1)^2$ . The  $a_i$  losing positions in the plane will give exactly  $2a_i$  elements in  $T_i$  because there are exactly two lines in the plane  $i$  that can contain each losing position. Since there are a total of  $k^2$  positions  $P_i$ , there are  $k^2 - a_i$  winning positions in  $P_i$ . Each winning position  $w \in W$  corresponds to  $k - 1$  elements in  $C$ . If the winning position in the plane  $i$  has a supporting line that is in the same plane  $i$ , the  $k - 1$  elements in  $C$  that the winning position corresponds to will also be in  $T_i$ , thus reducing the size of  $M_i$  by  $k - 1$ . If the winning position in the plane has a supporting line that is not in the same plane, the size of  $M_i$  stays the same. Thus,

$$|M_i| \geq 2a_i - (k - 1)(k^2 - a_i)$$

which implies

$$h(a_i) \geq 2a_i - (k - 1)(k^2 - a_i)$$

with the inequality becoming equality if and only if all supporting lines of every winning position in the plane  $i$  lie in the same plane  $i$ . We can arrange  $(k - 1)^2$  losing positions in a  $(k - 1)$ -by- $(k - 1)$  square in a plane and place the  $k^2 - a_i$  (which is no more than  $2k - 2$ ) winning positions in the plane adjacent to that square so that they have supporting lines

in the same plane using those  $(k-1)$ -by- $(k-1)$  losing positions. Since equality can be achieved,  $h(a_i) = 2a_i - (k-1)(k^2 - a_i)$ . Let  $1 \leq m \leq k^2 - (k-1)^2$ . Then,

$$\begin{aligned} h((k-1)^2 + m) &= 2(k-1)^2 + 2m - (k-1)(k^2 - (k-1)^2 - m) \\ &= 2(k-1)^2 + 2m - (k-1)(2k-1) + (k-1)m \\ &= -(k-1) + (k+1)m = 2 + (k+1)(m-1) \end{aligned} \tag{4}$$

Second,  $h((k-1)^2) = 0$  because we can arrange  $(k-1)^2$  losing positions in a  $(k-1)$ -by- $(k-1)$  square in a plane and let  $2k-2$  winning positions in the plane adjacent to that square have supporting lines in the same plane using those  $(k-1)$ -by- $(k-1)$  losing positions. The last winning position  $(i, k, k)$  may have supporting line that does not lie in plane  $i$ . Third, when  $0 \leq a_i \leq (k-1)^2 - 1$ ,

$$h(a_i + 1) - h(a_i) \leq 2 \tag{5}$$

because a newly added losing position to  $P_i$  will increase the size of  $T_i$  by only 2, and we can put a newly added losing position replacing a winning position that has supporting line not in  $P_i$ . Thus, the size of  $M_i$  cannot increase by more than 2. If the set of  $a_i$  that minimizes  $\sum_{i=1}^k h(a_i)$  has some  $a_j > (k-1)^2$ , let  $a_t$  be an element in the set of  $a_i$  that is less than  $(k-1)^2$  (such  $a_t$  exists because  $\sum_{i=1}^k a_i = k^3 - 3k^2 + 6k - 7$  and  $k \geq 3$ ). We may create a new set of  $a_i$  by reducing  $a_j$  by 1 and increasing  $a_t$  by 1. By (4) and (5), the new set of  $a_i$  will have  $\sum_{i=1}^k h(a_i)$  less than or equal to the one with the old set of  $a_i$ . We may keep doing this until no  $a_j$  is greater than  $(k-1)^2$ .  $\square$

*Proof of Lemma 5.* Each supporting line passes through  $k-1$  losing positions. Our intuition would say that with  $m$  supporting lines, there should be  $(k-1)m$  losing positions. However, some losing positions may be used for more than one supporting lines. Because we are considering on a plane, a losing position can be used at most twice for two different supporting lines. Thus, to minimize the number of losing positions we need, we have to maximize the number of losing positions that are used for supporting lines twice.

If among  $m$  supporting lines, there are  $u$  lines parallel to the x-axis and  $v$  lines parallel to the y-axis, the number of losing positions that are used in supporting lines twice is  $uv$ . Since  $u + v = m$  is constant,  $uv$  is maximized when  $u$  and  $v$  are as close to each other as much as possible. That is,  $u = v$  when  $m$  is even and  $|u - v| = 1$  when  $m$  is odd. If  $m$  is even, there are  $m/2$  lines in each orientation. Thus, there are  $(\frac{m}{2})^2$  losing positions that are used for supporting lines twice. Therefore, there are  $(k-1)m - (\frac{m}{2})^2$  losing positions. If  $m$  is odd, there are  $(m-1)/2$  lines in the first orientation and  $(m+1)/2$  lines in the second orientation. Thus, there are  $(\frac{m-1}{2})(\frac{m+1}{2})$  losing positions that are used for supporting lines twice. Therefore, there are  $(k-1)m - (\frac{m-1}{2})(\frac{m+1}{2}) = (k-1)m - (\frac{m}{2})^2 + \frac{1}{4}$  losing positions.  $\square$

*Proof of Lemma 6.* If there are  $d$  supporting lines in the plane, from the definition of  $f$ , there must be at least  $f(d)$  losing positions in that plane. Also, as  $a_i \leq (k-1)^2$ ,

$g(a_i) \leq 2(k-1)$  because each losing position can be used for a supporting line at most twice. Thus,

$$g(a_i) = \max \{d \in \{0, 1, 2, \dots, 2(k-1)\} : f(d) \leq a_i\}$$

From Lemma 5, whether  $d \in \{0, 1, 2, \dots, 2(k-1)\}$  is even or odd, when  $f(d) \leq a_i$ , we have

$$\begin{aligned} a_i &\geq f(d) \geq (k-1)d - \left(\frac{d}{2}\right)^2 \\ \left((k-1) - \frac{d}{2}\right)^2 &\geq (k-1)^2 - a_i \\ (k-1) - \frac{d}{2} &\geq \sqrt{(k-1)^2 - a_i} \quad (\because d \leq 2(k-1) \text{ and } a_i \leq (k-1)^2) \\ 2(k-1) - 2\sqrt{(k-1)^2 - a_i} &\geq d \end{aligned}$$

Because  $d$  is an integer,

$$d \leq \left\lfloor 2(k-1) - 2\sqrt{(k-1)^2 - a_i} \right\rfloor = 2k - 2 + \left\lfloor -2\sqrt{(k-1)^2 - a_i} \right\rfloor \quad \square$$

*Proof of Lemma 8.* From  $h(a_i) = 2a_i - (k-1)g(a_i)$ , we have

$$\begin{aligned} \sum_{i=1}^k h(a_i) &= 2 \sum_{i=1}^k a_i - (k-1) \sum_{i=1}^k g(a_i) \\ &= 2k^3 - 6k^2 + 12k - 14 - (k-1) \sum_{i=1}^k g(a_i) \end{aligned}$$

From  $g(a_i) \leq 2k - 2 + \left\lfloor -2\sqrt{(k-1)^2 - a_i} \right\rfloor$ , we get

$$\begin{aligned} \sum_{i=1}^k h(a_i) &\geq 2k^3 - 6k^2 + 12k - 14 - (k-1) \sum_{i=1}^k \left(2k - 2 + \left\lfloor -2\sqrt{(k-1)^2 - a_i} \right\rfloor\right) \\ &= 2k^3 - 6k^2 + 12k - 14 - (k-1)k(2k-2) - (k-1) \sum_{i=1}^k \left\lfloor -2\sqrt{(k-1)^2 - a_i} \right\rfloor \quad (6) \end{aligned}$$

For  $i = 1, 2, 3, \dots, k$ , let  $b_i = (k-1)^2 - a_i$ . Observe that  $0 \leq b_i \leq (k-1)^2$ , and that  $\sum_{i=1}^k b_i = k(k-1)^2 - \sum_{i=1}^k a_i = k^2 - 5k + 7$ . Also, the expression (2.4) becomes

$$\begin{aligned} &2k^3 - 6k^2 + 12k - 14 - (k-1)k(2k-2) - (k-1) \sum_{i=1}^k \left\lfloor -2\sqrt{b_i} \right\rfloor \\ &= -2k^2 + 10k - 14 - (k-1) \sum_{i=1}^k \left\lfloor -2\sqrt{b_i} \right\rfloor \quad (7) \end{aligned}$$

To minimize  $\sum_{i=1}^k h(a_i)$ , we need to maximize  $\sum_{i=1}^k \lfloor -2\sqrt{b_i} \rfloor$ . It is not hard to prove that  $\sum_{i=1}^k \lfloor -2\sqrt{b_i} \rfloor$  is maximized when every term but one of  $b_i$  is 0. Thus,

$$\begin{aligned} \sum_{i=1}^k \lfloor -2\sqrt{b_i} \rfloor &\leq \underbrace{\lfloor -2\sqrt{0} \rfloor + \lfloor -2\sqrt{0} \rfloor + \dots + \lfloor -2\sqrt{0} \rfloor}_{k-1 \text{ terms}} + \lfloor -2\sqrt{k^2 - 5k + 7} \rfloor \\ &= \lfloor -\sqrt{4k^2 - 20k + 28} \rfloor \end{aligned}$$

But, since  $k \geq 3$ ,

$$4k^2 - 20k + 25 < 4k^2 - 20k + 28 \leq 4k^2 - 16k + 16$$

which gives

$$\begin{aligned} 2k - 5 &< \sqrt{4k^2 - 20k + 28} \leq 2k - 4 \\ -2k + 5 &> -\sqrt{4k^2 - 20k + 28} \geq -2k + 4 \end{aligned}$$

Therefore,

$$\lfloor -\sqrt{4k^2 - 20k + 28} \rfloor = -2k + 4$$

So,

$$\sum_{i=1}^k \lfloor -2\sqrt{b_i} \rfloor \leq -2k + 4$$

From (2.5),

$$\begin{aligned} \sum_{i=1}^k h(a_i) &\geq -2k^2 + 10k - 14 - (k-1) \sum_{i=1}^k \lfloor -2\sqrt{b_i} \rfloor \\ &\geq -2k^2 + 10k - 14 - (k-1)(-2k + 4) \\ &= 4k - 10 \end{aligned}$$

as we claim. □

*Proof of Lemma 9.* Recall when we split the entire cube  $S$  into  $k$  planes  $P_1, P_2, P_3, \dots, P_k$ , where  $P_i = \{(i, b, c) \in S : 1 \leq b, c \leq k\}$ , and when we let  $M_i = T_i - C$ , where

$$T_i = \{(x, l) : x \in P_i \cap X, l \text{ is a line in } P_i, \text{ and } x \in l\}$$

From Lemma 8, we have  $\sum_{i=1}^k |M_i| \geq 4k - 10$ . However, we can also split the cube  $S$  into  $k$  planes in two other ways:

- $Q_1, Q_2, Q_3, \dots, Q_k$ , where  $Q_i = \{(a, i, c) \in S : 1 \leq a, c \leq k\}$ , and we let  $N_i = U_i - C$ , where

$$U_i = \{(x, l) : x \in Q_i \cap X, l \text{ is a line in } Q_i, \text{ and } x \in l\}$$



- $R_1, R_2, R_3, \dots, R_k$ , where  $R_i = \{(a, b, i) \in S : 1 \leq a, b \leq k\}$ , and we let  $O_i = V_i - C$ , where

$$V_i = \{(x, l) : x \in R_i \cap X, l \text{ is a line in } R_i, \text{ and } x \in l\}$$

Using Lemma 8 similarly, we get  $\sum_{i=1}^k |N_i| \geq 4k - 10$  and  $\sum_{i=1}^k |O_i| \geq 4k - 10$ . Each element in  $M = \{(x, l) : x \in X, l \text{ is a line, and } x \in l\} - C$  will be counted exactly twice among sets  $M_i, N_i, O_i$  because a line can be contained in exactly two different planes in  $P_i, Q_i, R_i$ . Also,  $M_i, N_i, O_i \subseteq M$  for all  $i = 1, 2, 3, \dots, k$ . Therefore,

$$\begin{aligned} |M| &= \frac{1}{2} \left( \sum_{i=1}^k |M_i| + \sum_{i=1}^k |N_i| + \sum_{i=1}^k |O_i| \right) \\ &\geq \frac{1}{2} (4k - 10 + 4k - 10 + 4k - 10) \\ &= 6k - 15 \end{aligned}$$

□

## B Comparing Different Strategies

Table 4 shows the ratio  $|W| / \lfloor \frac{nk^n - 1}{n+k-1} \rfloor$  of the combinatorial strategy constructed in this paper for several values of  $n, k$ .

Table 4:

$n \backslash k$	3	5	7	10	20	50	100	250
3	0.9375	0.9623	0.9737	0.9880	0.9963	0.9993	0.9998	0.99997
5	0.9538	0.9476	0.9641	0.9778	0.9926	0.9986	0.9996	0.99994
7	0.8276	0.9497	0.9629	0.9752	0.9906	0.9980	0.9995	0.99991
10	0.7158	0.9505	0.9642	0.9743	0.9889	0.9973	0.9992	0.99987
20	0.6342	0.7767	0.9267	0.9774	0.9873	0.9959	0.9986	0.99974
50	0.5722	0.6433	0.7116	0.8111	0.9897	0.9950	0.9978	0.99945
100	0.5466	0.5901	0.6305	0.6895	0.8811	0.9955	0.9975	0.99918
250	0.5271	0.5509	0.5724	0.6029	0.6973	0.9678	0.9980	0.99900

Table 5 shows the ratio of probability of winning of Lenstra and Seroussi's strategy  $1 - \left(1 - \frac{1}{k}\right)^{\log_2(n+1)}$  to the upper bound  $\lfloor \frac{nk^n - 1}{n+k-1} \rfloor / k^n$ . In their paper [5], their strategy only works when  $n = 2^m - 1$  for some positive integer  $m$ . Here we use  $1 - \left(1 - \frac{1}{k}\right)^{\log_2(n+1)}$  (from equation 5 in the paper) for general  $n$  only to see the big picture of comparison between winning probabilities of two strategies.

Table 5:

$n \backslash k$	3	5	7	10	20	50	100	250
3	0.9375	0.8491	0.7982	0.7631	0.7156	0.6865	0.6766	0.6707
5	0.9122	0.7890	0.7231	0.6676	0.5961	0.5495	0.5334	0.5236
7	0.9053	0.7669	0.6876	0.6194	0.5298	0.4705	0.4498	0.4371
10	0.9049	0.7530	0.6613	0.5804	0.4715	0.3983	0.3725	0.3566
20	0.9147	0.7497	0.6395	0.5372	0.3934	0.2930	0.2569	0.2347
50	0.9357	0.7754	0.6528	0.5309	0.3484	0.2144	0.1651	0.1344
100	0.9514	0.8046	0.6802	0.5495	0.3443	0.1875	0.1288	0.0919
250	0.9682	0.8445	0.7243	0.5887	0.3611	0.1779	0.1075	0.0628

Table 6 shows the ratio of the lower bound of probability of winning in Alon's paper [4],  $1 - \left\lfloor \frac{k^n \log n}{(k-1)^{n-1}n} \right\rfloor \left( \frac{k-1}{k} \right)^n - \frac{1}{n}$ , to the upper bound  $\lfloor \frac{nk^n-1}{n+k-1} \rfloor / k^n$ . Sometimes the lower bound  $1 - \left\lfloor \frac{k^n \log n}{(k-1)^{n-1}n} \right\rfloor \left( \frac{k-1}{k} \right)^n - \frac{1}{n}$  is less than 0, in which case we put 0 in the table instead.

Table 6:

$n \backslash k$	3	5	7	10	20	50	100	250
3	0	0	0	0	0	0	0	0
5	0.1988	0	0	0	0	0	0	0
7	0.3497	0	0	0	0	0	0	0
10	0.5181	0	0	0	0	0	0	0
20	0.7152	0.4206	0.0437	0	0	0	0	0
50	0.8565	0.7204	0.5716	0.3232	0	0	0	0
100	0.9159	0.8380	0.7565	0.6273	0.1354	0	0	0
250	0.9594	0.9222	0.8842	0.8259	0.6202	0	0	0