Covering Codes for Hats-on-a-line

Sarang Aravamuthan

Advanced Technology Center, Hyderabad, India.

a.sarangarajan@tcs.com

Sachin Lodha

Tata Research Development and Design Center, Pune, India.*

sachin.lodha@tcs.com

Submitted: Sep 22, 2005; Accepted: Feb 28, 2006; Published: Mar 7, 2006

Mathematics Subject Classification: 91A46, 94B75

Abstract

We consider a popular game puzzle, called *Hats-on-a-line*, wherein a warden has n prisoners, each one wearing a randomly assigned black or white hat, stand in a line. Thus each prisoner can see the colors of all hats before him, but not his or of those behind him. Everyone can hear the answer called out by each prisoner. Based on this information and without any further communication, each prisoner has to call out his hat color starting from the back of the line. If he gets it right, he is released from the prison, otherwise he remains incarcerated forever. The goal of the team is to devise a strategy that maximizes the number of correct answers. A variation of this problem asks for the solution for an arbitrary number of colors.

In this paper, we study the standard *Hats-on-a-line* problem and its natural extensions. We demonstrate an optimal strategy when the seeing radius and/or the hearing radius are limited. We show for certain orderings that arise from a (simulated) game between the warden and prisoners, how this problem relates to the theory of covering codes.

Our investigations lead to two optimization problems related to covering codes in which one leads to an exact solution (for binary codes). For instance, we show that for $0 < k < n$, $(n-k-d) \leq \alpha_m n$ where $d = t(n-k, m^k, m)$ is the minimum covering radius of an m-ary code of length $(n-k)$ and size m^k and

$$\alpha_m = \frac{\log m}{\log(m^2 - m + 1)}.$$

*Both ATC and TRDDC are research units of Tata Consultancy Services Limited.

1 Introduction

In the *Hats-on-a-line* game puzzle, a warden has n prisoners stand in a line and places a hat of color black or white on each of their heads. Starting from the back of the line, each prisoner has to call out his hat color. If he gets it right, he is released from prison, otherwise he remains incarcerated forever.

Each prisoner can see the colors of all hats before him, but not his or of those behind him. Everyone can hear the answer called out by each prisoner. No other communication is allowed between the prisoners during the game. They are permitted, however, to come up with a strategy before the game starts. The distribution of hat color combinations is assumed to be random and uniform, i.e., all 2^n combinations are equally likely. The goal of the team is to devise a strategy that maximizes the number of correct answers in the worst case.

This is a well known puzzle and also goes by the name "Single-File Hat Execution" (see [1, 6]). A variation of this problem asks for the solution for an arbitrary, say $m > 1$, number of colors. An optimal strategy for the general m color hat problem is well-known and we discuss it in Section 2.1. The strategy combines the back-to-front ordering, see-all-in-front and hear-all features using the *modulus* operator to save all but one prisoner.

It is now natural to consider variants of the original problem where some of these features are not fully permitted. In Section 3, we consider a scenario where the seeing radius and/or the hearing radius are limited. We prove an upper bound on the number of correct guesses in this new model and show that it is tight by demonstrating a strategy that matches the same.

Some interesting situations arise when the prisoners don't follow a back-to-front order in calling out their hat colors. In Section 4, we consider two versions of an ordering game between $\mathcal{X}$, the set of prisoners, and $\mathcal{W}$, the warden. In the first version $\mathcal{X}$ chooses a value k between 0 and n while $\mathcal{W}$ chooses a front-to-back ordering for the first k and last $n-k$ members of $\mathcal{X}$. We derive bounds on the number of correct calls under this ordering. In the second version, $\mathcal{W}$ chooses k while $\mathcal{X}$ chooses the ordering for one of the two parts while $\mathcal{W}$ chooses the ordering for the other part. We estimate k and the number of correct guesses under this scenario. We use these results to show that finding the optimal strategy is equivalent to determining codes of minimal covering radius.

1.1 Related Work

To the best of our knowledge, the variants of *Hats-on-a-line* studied in this paper are new and have never been studied before. Our discovery of the strong correlation between the best strategies for some of these variants and covering codes is not surprising though. In [7], Lenstra and Seroussi study another popular hat puzzle [2, 8] where they too show that the best strategies are related in a natural way to covering codes. Their game is as follows:

A team of n players enter a game room, and each player is fitted with a hat, which is either black or white. A player can see the other players hat colors, but not his own. Each player is then asked to make a declaration, which must be one of the statements "my hat is black", "my hat is white", or "I pass". All the players must declare simultaneously, and no communication is allowed between them during the game. They are permitted, however, to hold a strategy coordination meeting before the game starts. The team wins if at least one player declares his hat color correctly, and no player declares an incorrect color. The distribution of hat color combinations is assumed to be random and uniform, i.e., all 2^n combinations are equally likely. The goal of the team is to devise a strategy that maximizes the winning probability.

Lenstra and Seroussi show an equivalence between binary covering codes of radius one and playing strategies for the case of two hat colors in [7]. Observing that this linkage is not sufficient for the case of $m > 2$ hat colors, they introduce the more appropriate notion of a strong covering, and also show efficient constructions of these coverings, which achieve winning probabilities approaching unity.

2 Preliminaries

Let m be the number of hat colors. We assume that the colors are represented by the set $\mathcal{M} = \{0, 1, \ldots, m-1\}$. Let $\mathcal{X} = \{x_1, \ldots, x_n\}$ be the set of n prisoners where x_i is the i^{th} prisoner from the back. Let y_i represent x_i's hat color and define $Y_i = \left(\sum_{j=i}^{n} y_j\right) \mod m$. Let $\mathcal{W}$ represent the warden.

The *seeing radius* of $x \in \mathcal{X}$ is the maximum number of people that x can see ahead of him. We assume that this is the same for all members of $\mathcal{X}$. Hence we refer to this value as the seeing radius of $\mathcal{X}$. Similarly, we define the *hearing radius* of $x \in \mathcal{X}$ as the maximum number of people ahead of x that can hear him. Again this value is assumed to be the same for all members of $\mathcal{X}$ and we refer to this as the hearing radius of $\mathcal{X}$.

We develop a uniform notation to cover situations where the seeing radius and/or the hearing radius is restricted. Let HATS (n, m, s, h) refer to the hat problem with s as the seeing radius, and h as the hearing radius. Thus the original problem under this notation would be HATS $(n, m, n-1, n-1)$.

An *ordering* on $\mathcal{X}$ is a permutation $x_{i_1}, \ldots, x_{i_n}$ of $\mathcal{X}$ such that the members of $\mathcal{X}$ call out their hat colors in the order $x_{i_1}, \ldots, x_{i_n}$. Define $\texttt{hat}(S)$ to be the minimum number of correct calls under an ordering S using any optimal strategy.

Let $X[i, j]$ denote the (partial) ordering $x_i, x_{i+1}, \ldots, x_j$ if $i \leq j$ (this is called a *back-to-front* ordering) and $x_i, x_{i-1}, \ldots, x_j$ (called a *front-to-back* ordering) if $i > j$.

Given $X \subseteq \mathcal{X}$, a back-to-front ordering is the most advantageous ordering for X since each announcer has the maximum possible information on which to base his color. A front-to-back ordering is the least advantageous for X as each announcer has no information that he can use to determine his color and cannot convey any information about the colors he sees as they have already been announced. Thus, whenever possible, X will choose a back-to-front ordering for itself while $\mathcal{W}$ will choose a front-to-back ordering for X.

We follow the notation from [4] for covering codes. A *code* $\mathcal{C}$ is any non-empty subset of $\mathcal{M}^n$. It's elements are called codewords. The *size* of $\mathcal{C}$ is the number of codewords in $\mathcal{C}$. The *distance* between two codewords is the number of co-ordinates they differ in. n is the *length* of the code. We say that $\mathcal{C}$ t-covers $\mathcal{M}^n$ if every element of $\mathcal{M}^n$ is at a distance at most t from $\mathcal{C}$. The *covering radius* of $\mathcal{C}$ is the smallest t such that $\mathcal{C}$ t-covers $\mathcal{M}^n$ and is denoted $t(\mathcal{C})$.

An (n, K, m) code is an m-ary code of length n and size K. Let $t(n, K, m)$ be the smallest covering radius among all (n, K, m) codes.

An $[n, k]$ code is a binary linear code of length n and dimension k while an $[n, k]d$ code is a binary linear code of length n, dimension k and covering radius d.

We denote by $V(n, d)$, the size of the ball of radius d among binary words of length n. Specifically, $V(n, d) = \sum_{i=0}^{d} \binom{n}{i}$.

By $\log_r(s)$ we mean the logarithm of s to base r. When r is not indicated, it's assumed to be 2.

2.1 The Modulo Scheme

The solution to the original problem HATS $(n, m, n-1, n-1)$ is straightforward. x_1 calls out the value $Y_2 = \left(\sum_{i=2}^{n} y_i\right) \mod m$. For each $i > 1$, x_i

- can *see* the values $y_{i+1}, \ldots, y_n$
- has *heard* the values Y_2 and $y_2, \ldots, y_{i-1}$

and therefore uses the expression for Y_2 to solve for y_i. This results in $(n-1)$ members calling out their colors correctly.

We refer to the above procedure as the *modulo scheme*. Using the modulo scheme, one sees that any set of j members of $\mathcal{X}$ under a back-to-front ordering can call $(j-1)$ of their hat colors correctly.

3 Limited Sight and Limited Volume

Theorem 1 *For* HATS (n, m, r, h),

$$\mathtt{hat}(X[1, n]) = n - \left\lceil \frac{n}{\min(r, h) + 1} \right\rceil.$$

Proof: Let's fix any optimal strategy $\mathcal{H}$ for the HATS (n, m, r, h). Let $\mathcal{Y} = \{\mathrm{y}_1, \ldots, \mathrm{y}_n\}$ be the hat colors for which $\mathcal{H}$ achieves the minimum $\mathtt{hat}(X[1, n])$ number of survivors.

Note that we are concerned with the deterministic strategies wherein every prisoner uses the audio-visual inputs to uniquely determine the color that he calls out. But unlike the game in [7], this one is necessarily an asymmetric game, *i.e.*, every prisoner would have possibly a different function to compute his answer. This is natural since each of them has got a different view of the situation. Thus the prisoners will have to play different roles that depend on their individual functions although these roles have to be fixed in advance as a part of the strategy. Therefore we base our proof on the following axioms:

I. In $\mathcal{H}$, some of the prisoners are designated to act as *information providers*. An *information provider* is a sacrificial lamb who may or may not know his hat color, but, by calling out a color, he provides some information for those ahead of him. The rest are called *information users*.

II. If any *information user*, say x_i, calls out his hat color correctly, he is necessarily preceded by an *information provider* who can *see* x_i and whom x_i can *hear*.

We assume that the choice of $\mathcal{Y}$ is such that the calls of *information providers* turn out to be incorrect when everybody follows the strategy $\mathcal{H}$.

Let $z = \min(r, h)$. Now consider any set of $z+1$ contiguous people in the line, say, $X[i, i+z]$. For x_{i+z}, the answers given by $x_1, \ldots, x_{i-1}$ are irrelevant since either

- they cannot see his hat (if $r \leq h$), or
- he cannot hear them (if $h \leq r$), or
- both.

Suppose that none of the $x_i, x_{i+1}, \ldots, x_{i+z-1}$ is an *information provider*. Then x_{i+z} must either be

- an *information provider*, or
- an *information user* who incorrectly announces his hat color since he is not preceded by any *information provider* whom he can hear and trust, thus not fulfilling the axiom II.

Therefore, in any set of $z+1$ contiguous people, there is at least 1 prisoner who is an incorrect caller given $\mathcal{Y}$.

Note that x_1 is necessarily an incorrect caller for $\mathcal{Y}$. Otherwise we could change y_1 and get $\mathcal{Y}'$ which has lesser number of survivors than $\mathcal{Y}$ – a contradiction. Moreover, by above analysis, there is at least one incorrect caller in $X[x_{(j-1)z+j+1}, x_{jz+j+1}]$ for $j = 1, 2, \ldots, \lfloor \frac{n-1}{z+1} \rfloor$. Thus, there are at least $1 + \lfloor \frac{n-1}{z+1} \rfloor = \lceil \frac{n}{z+1} \rceil$ incorrect callers.

Since the number of survivors is equal to the total minus the number of incorrect callers, we have

$$\mathtt{hat}(X[1,n]) \ \leq \ n - \left\lceil \frac{n}{z+1} \right\rceil. \tag{1}$$

In fact, by making x_{jz+j+1} for $j = 0, 1, 2, \ldots, \lfloor \frac{n-1}{z+1} \rfloor$ as *information providers*, and repeating the modulo scheme for each such $X[x_{jz+j+1}, x_{(j+1)z+j+1}]$, we can ensure that $n - \lceil \frac{n}{z+1} \rceil$ number of prisoners correctly announce their hat colors. Therefore, in light of inequality (1), we get

$$\mathtt{hat}(X[1,n]) = n - \left\lceil \frac{n}{\min(r,h)+1} \right\rceil. \qquad \square$$

4 An Ordering Game

$\mathcal{W}$ realizing that almost all members of $\mathcal{X}$ will get their hat colors right in a back-to-front ordering decides to choose his own ordering. The prisoners protest as $\mathcal{W}$ might choose a front-to-back ordering in which case no member of $\mathcal{X}$ may guess their color.

Suppose $\mathcal{W}$ relents and lets a member of $\mathcal{X}$ call out his color, before choosing his (front-to-back) ordering. Then $\mathcal{X}$ will simply have x_1 call out the majority color of all the hats in front of him. This will guarantee at least $\lceil (n-1)/m \rceil$ correct guesses. The prisoners realize that they can actually do better! So, they propose the following scheme to $\mathcal{W}$.

4.1 Partition Chosen by $\mathcal{X}$

In the first setting, $\mathcal{X}$ chooses a number k and $\mathcal{W}$ chooses the front-to-back ordering for the last k and the first $n-k$ members of $\mathcal{X}$. In other words, the members of $\mathcal{X}$ announce their hat colors in the order

$$S_k := X[k, 1], X[n, k+1].$$

Here $\mathcal{X}$ chooses k so as to *maximize* $\mathtt{hat}(S_k)$. Our goal is to derive bounds for $\mathtt{hat}(S_k)$.

For each k, consider the code $\mathcal{C}_k$ in $\mathcal{M}^{n-k}$ of size m^k and minimum covering radius $d(k) := t(n-k, m^k, m)$. The result below determines $\mathtt{hat}(S_k)$ in terms of n, k and $d(k)$.

Claim 2

$$\mathtt{hat}(S_k) = n - k - d(k)$$

Proof: The colors announced by $x_1, \ldots, x_k$ define a codeword in $\mathcal{C}_k$ within distance $d(k)$ of $(y_{k+1}, \ldots, y_n)$. This codeword is announced as the hat color by the members $x_{k+1}, \ldots, x_n$. Thus, utmost $d(k)$ of $\{x_{k+1}, \ldots, x_n\}$ would get their colors wrong. This implies $\mathtt{hat}(S_k) \geq n - k - d(k)$.

On the other hand, the m^k possible announcements by $\{x_1, \ldots, x_k\}$ map to a collection of m^k answers by $\{x_{k+1}, \ldots, x_n\}$ that we may interpret as forming a code $\mathcal{C} \subseteq \mathcal{M}^{n-k}$. With the goal of maximizing the number of correct guesses, the members $\{x_{k+1}, \ldots, x_n\}$ will always choose a codeword in $\mathcal{C}$ such that the number of incorrect guesses is $\leq k + t(\mathcal{C})$. Choosing a configuration of hat colors where the upper bound (for incorrect guesses) is achieved, the number of correct guesses is $n - k - t(\mathcal{C}) \leq n - k - d(k)$ since $t(\mathcal{C}) \geq t(n-k, m, m^k)$. This proves the result. $\square$

It follows from Claim 2 that $\mathcal{X}$ will choose k to maximize $n - k - d(k)$. The bounds derived in this section are in terms of the two quantities

$$\alpha_m := \frac{\log(m)}{\log(m^2 - m + 1)}$$

$$\beta_m := \frac{\log(m^2/(2m-1))}{\log(m^3/(2m-1))}$$

We first determine an upper bound on the number of correct guesses under S_k.

Theorem 3 *Let θ_1 be the number of correct guesses under an optimal choice of k chosen by $\mathcal{X}$, i.e. $\theta_1 = \max_{0<k<n} \mathtt{hat}(S_k)$. Then*

$$\theta_1 \leq \alpha_m n$$

Proof: We assume the setting described above, i.e. the members $x_1, \ldots, x_k$ define a code $\mathcal{C}_k$ of covering radius $d(k)$. By the sphere covering bound,

$$m^k \sum_{i=0}^{d} \binom{n-k}{i} (m-1)^i \geq m^{n-k}.$$

Let $u = k/n$, $v = d/n$, $u, v \geq 0$. By Claim 2, $\mathtt{hat}(S_k) = n-k-d(k) = n(1-u-v)$. Since $\mathtt{hat}(S_{n/2}) = n/2$ and we are maximizing $\mathtt{hat}(S_k)$, we will assume $u+v \leq 1/2$. Then the above inequality yields

$$m^{n-2k} \leq \sum_{i=0}^{d(k)} \binom{n-k}{i} (m-1)^i \leq (m-1)^{d(k)} 2^{(n-k)H(d(k)/(n-k))}$$

where $H(x) = -(x\log(x) + (1-x)\log(1-x))$ is the Shannon's entropy function [9]. The last inequality follows because $d(k) \leq (n-k)/2$ (see [10] for a proof).

Taking logs and simplifying, our optimization problem becomes

$$\min h(u,v) := (u+v) \quad \text{s.t.}$$
$$g(u,v) := H(\frac{v}{1-u}) - \frac{(1-2u)L_1 - vL_2}{1-u} = 0$$

where $L_1 = \log(m)$ and $L_2 = \log(m-1)$. Note that we have replaced $g(u,v) \geq 0$ by $g(u,v) = 0$ as the minimum will occur at the boundary of g.

To find the minimum value, we use the method of Lagrange multipliers. Thus we get

$$\begin{aligned} \partial h/\partial u + \lambda \partial g/\partial u &= 1 + \lambda \left(\frac{v}{(1-u)^2} H'(\frac{v}{1-u}) + \frac{L_1 + L_2 v}{(1-u)^2} \right) = 0 \\ \partial h/\partial v + \lambda \partial g/\partial v &= 1 + \lambda \left(\frac{1}{(1-u)} H'(\frac{v}{1-u}) + \frac{L_2}{1-u} \right) = 0 \end{aligned}$$

where λ is the multiplier and $H'(x) = \log(\frac{1-x}{x})$. Solving these gives $\lambda = (1-u)(u+v-1)/L_1$, $u = 1-m^2\alpha_m/(m^2-m+1)$ and $v = (m-1)\alpha_m/(m^2-m+1)$ so that $1-u-v = \alpha_m$. This implies $u+v < 1/2$ and therefore a minimum since $(1/2, 0)$ is also a feasible solution to the optimization problem. This proves the result. $\square$

We observe that α_m approaches 0.5 as $m \to \infty$. So, as m gets large, the simple scheme of choosing $k = n/2$ and having x_i call out $y_{i+n/2}$ is close to optimal. For smaller values of m, considering specific codes will give better than 50% success.

Lower Bound on θ_1:

For $m = 2$, it is possible for $\mathcal{X}$ to realize the upper bound of $\alpha_2 = 1/\log 3$. Specifically, we set u and v to the values achieving the upper bound in Theorem 3, i.e. $u = 1 - 4/(3\log 3)$ and $v = 1/(3\log 3)$. Set $k = \lfloor un \rfloor$ and $d = \lfloor vn \rfloor$ and consider a $[n-k, k]d$ code. By Theorem 12.3.2 of [3], such a code exists (for a sufficiently large n) because for u and v specified as above, we have

$$u = (1-u) - (1-u)H(\frac{v}{1-u})$$

so that

$$k \leq \lceil n - k - \log V(n-k, d) + \log(n-k) + \log(\ln 2) \rceil.$$

By the choice of u and v, the number of correct guessers is $n(1-u-v) = \alpha_2 n$.

A Generalization to Multiple Partitions:

The above setting can be extended as follows. Instead of k, $\mathcal{X}$ now chooses r numbers $0 < k_1 < \cdots < k_r \leq n$ while $\mathcal{W}$ chooses the front-to-back ordering $X[k_i, k_{i-1}+1]$ for each i. Let $\mathcal{K}_r = \{k_1, \ldots, k_r\}$. The final ordering is $S_{\mathcal{K}_r} := X[k_1, 1]X[k_2, k_1+1] \cdots X[n, k_r+1]$. $\mathcal{X}$ will choose $\mathcal{K}_r$ so as to maximize $\texttt{hat}(S_{\mathcal{K}_r})$. Let θ_r be this maximum value. We observe that

I. $0.5n \leq \theta_1 \leq \cdots \leq \theta_{n-1} = n-1$. The first inequality was shown in Section 4.1 while the last one follows from Section 2.1.

II. Let $a_r = \lfloor n/(r+1) \rfloor$. Then $\theta_r \geq r a_r$. To see this, choose $k_i = i a_r$ for $i = 1, \ldots, r$. Then, for $i = 1, \ldots, a_r$, the members $x_i, x_{i+a_r}, \ldots, x_{i+ra_r}$ use the modulo scheme ensuring that r of them call out correctly. This gives a total of $r a_r$ correct guesses.

III. For the 2-color case, we observe that θ_1 is achieved using a purely covering code scheme while θ_{n-1} is achieved using a purely modulo scheme. It would be interesting to see how the transition between these schemes occur.

Geometric Analogues of the Two Schemes:

The two strategies used by the prisoners, namely the modulus scheme and the covering code scheme, turn out to have natural geometric interpretations.

I. A modulus scheme under the ordering $X[1, n]$ defines a *hyperplane* $\sum_{i=2}^{n}(z_i - y_i) = 0$ in $\mathbb{R}^{n-1}$ with coordinates $z_2, \ldots, z_n$. The point $(y_2, \ldots, y_n)$ lies on this hyperplane. The coefficient $Y_2 = (\sum_{i=2}^{n} y_i) \mod m$ is announced by x_1 and enables $x_2, \ldots, x_n$ to determine their colors.

II. A covering code scheme under the ordering $X[k, 1]X[n, k+1]$ defines a *point* in $z \in \mathbb{R}^{n-k}$ that is *near* $(y_{k+1}, \ldots, y_n)$. The members $x_1, \ldots, x_k$ identify z and the members $x_{k+1}, \ldots, x_n$ identify the coordinates of z as their colors.

4.2 Partition Chosen by $\mathcal{W}$

An alternative to the previous setting is one where $\mathcal{W}$ first chooses a k and $\mathcal{X}$ chooses the ordering of *one* of the two parts, while $\mathcal{W}$ chooses the ordering of the other. Of course, if $\mathcal{X}$ is allowed to choose the ordering of both parts, then it will choose back-to-front for both parts ensuring that $n-1$ members guess correctly.

In this case, $\mathcal{W}$ chooses a k so as to *minimize* the number of correct guesses. The final ordering is either $R_k := X[1,k], X[n,k+1]$ or $T_k := X[k,1], X[k+1,n]$ which we may assume is chosen by $\mathcal{X}$ to maximize the number of correct guesses. The goal here is to determine the range for k and the number of correct guesses in this setting.

Since $\mathcal{W}$ will not choose $k=0$, we assume $k>0$. For the ordering T_k, x_k will call out the value Y_{k+1}. The members $x_{k+1},\ldots,x_n$ now follow the modulo scheme resulting in $\mathtt{hat}(T_k) = n-k$.

To estimate the optimal k as chosen by $\mathcal{W}$, we first show that $\mathtt{hat}(R_k)$ is monotonic.

Claim 4 *For* $0<k<n$,

$$\mathtt{hat}(R_{k+1}) \geq \mathtt{hat}(R_k)$$

Proof: For R_k, each $x_i, i>k$ determines his hat color based only on the answers given by $x_1,\ldots,x_k$. Under the ordering R_{k+1}, the members $x_{k+1},\ldots,x_n$ are still preceded by $x_1,\ldots,x_k$. Thus they can potentially use the same scheme as in R_k to determine their hat colors. This proves the claim. □

Next we derive a bound for $\mathtt{hat}(R_k)$.

Claim 5

$$\mathtt{hat}(R_k) \leq \max_{0\leq k'\leq k}((n-k-d)+(k-k'))$$

where $d = t(n-k, m^{k'}, m)$.

Proof: Under R_k, the members $x_{k+1},\ldots,x_n$ determine their colors based on the information provided by $x_1,\ldots,x_k$. If, in any particular instance of the optimal strategy, x_i is an information provider then clearly his answer is not *fixed* by $x_1,\ldots,x_{i-1}$ and thus x_i cannot be counted as a correct guesser. If k' of the first k members are information providers, then the number of correct guesses among $x_{k+1},\ldots,x_n$ is utmost $n-k-d$ and the total number of correct guesses utmost $(k-k')+(n-k-d)$. As k' can be any value between 0 and k, this proves the result. □

As $\mathtt{hat}(R_k)$ (resp. $\mathtt{hat}(T_k)$) increases (resp. decreases) with k, the quantity $\max(\mathtt{hat}(R_k), \mathtt{hat}(T_k))$ is minimized when $\mathtt{hat}(R_k) = \mathtt{hat}(T_k)$. Let κ be the value of k at which this happens.

The following result bounds κ from below.

Theorem 6

$$\kappa \geq \beta_m n$$

Proof: By Claim 5,

$$\texttt{hat}(R_k) \leq \max_{0 \leq k' \leq k} ((n-k-d)+(k-k')) \tag{2}$$

where, as in the claim, the first $k' \leq k$ members $x_1, \ldots, x_{k'}$ opt to define a code of minimum covering radius $d = t(n-k, m^{k'}, m)$ in $\mathcal{M}^{n-k}$ while the members $x_{k'+1}, \ldots, x_k$ choose the modulo scheme.

Let $u = k'/(n-k), v = d/(n-k)$. To estimate $\texttt{hat}(R_k)$, we use the sphere covering bound,

$$m^{k'} \sum_{i=0}^{d} \binom{n-k}{i} (m-1)^i \geq m^{n-k}$$

which implies

$$m^{n-k-k'} \leq (m-1)^d \sum_{i=0}^{d} \binom{n-k}{i} \leq (m-1)^d 2^{(n-k)I(v)}$$

where

$$I(v) = \begin{cases} H(v) & v \leq 0.5, \\ 1 & v > 0.5 \end{cases}$$

Taking logs and simplifying, we get

$$(1-u)L_1 - vL_2 \leq I(v) \tag{3}$$

where $L_1 = \log m$ and $L_2 = \log(m-1)$. From (2),

$$\texttt{hat}(R_k) \leq \max_{0 \leq k' \leq k} n - d - k' = \max_{0 \leq u \leq k/(n-k)} n - (n-k)(u+v).$$

From (3),

$$u + v \geq 1 + (1 - L_2/L_1)v - I(v)/L_1.$$

When $0.5 \leq v \leq 1$, the right hand side attains a minimum at $v = 0.5$. So we can assume $v \leq 0.5$ and replace $I(v)$ by $H(v)$ above. Taking derivatives, the right hand side is minimized when $v = \bar{v} := (m-1)/(2m-1)$. Substituting κ for k, we have

$$(n-\kappa) = \texttt{hat}(T_\kappa) = \texttt{hat}(R_\kappa) \leq n - (n-\kappa)(L_1 + (L_1 - L_2)\bar{v} - H(\bar{v}))/L_1.$$

Solving this gives $\kappa \geq \beta_m n$. □

For an upper bound on κ we consider specific codes. We consider only the 2-color case. A bound of $n/3$ for κ is seen from the following argument. For R_k, $\mathcal{X}$ can have $x_2, \ldots, x_{k+1}$ choose the modulo scheme while x_1 can call out the majority color among $y_{k+2}, \ldots, y_n$. This shows

$$n - \kappa = \texttt{hat}(R_\kappa) \geq (\kappa - 1) + (n - \kappa - 1)/2 = (n + \kappa - 3)/2$$

Thus $\kappa \leq (n/3+1)$.

A small improvement to this bound can be obtained through first order Reed-Muller codes. These are $\texttt{RM}(z) := [2^z, z+1]$ codes (for some integer z) with covering radius $\rho(z) < 2^{z-1} - 2^{(z-2)/2}$ when z is odd; see [4, section 7.1] for more details. In particular, when $z = 9$, we have a $\texttt{RM}(9) = [512, 10]$ code with covering radius ≤ 244. For a given k, we take a direct sum of $\texttt{RM}(9)$ codes to form a code of length $512\lfloor (n-k)/512 \rfloor$ and size $2^{10}\lfloor (n-k)/512 \rfloor$. The remaining $k - 10\lfloor (n-k)/512 \rfloor$ members use the modulo scheme. Thus we have

$$n - \kappa = \texttt{hat}(R_\kappa) \geq (512-244)\lfloor (n-\kappa)/512 \rfloor + (\kappa - 10\lfloor (n-\kappa)/512 \rfloor - 1)$$

Solving this, we get $\kappa \leq 127n/383 + c$ for some constant c.

Summarizing,

Remark 7 *For the 2-color case, $\mathcal{W}$ will choose a value k such that* $\log(4/3)n/\log(8/3) \leq k \leq 127n/383$*. The number of correct guesses, $n-k$ lies between $\frac{256n}{383}$ and $\frac{n}{\log(8/3)}$.* □

5 Conclusion

We studied the standard *Hats-on-a-line* problem and its extensions to cases where the seeing radius and/or the hearing radius were limited. We also considered different orderings under which the prisoners call out their colors and showed how these orderings relate to covering codes and defines a new optimization problem on the covering radius.

Acknowledgment:

The authors are indebted to the referee for pointing out that the upper bound in Theorem 3 can be realized and for various comments that improved the exposition of this paper.

References

[1] Berkeley Riddles. URL: *http://www.ocf.berkeley.edu/~wwu/riddles/hard.shtml.*

[2] J.P. Buhler. Hat tricks. *Mathematical Intelligencer*, 24(4):44–49, 2002.

[3] G.D. Cohen, I. Honkala, S.N. Litsyn and A.C. Lobstein, *Covering Codes*, Elsevier, 1997.

[4] G.D. Cohen, S.N. Litsyn, A.C. Lobstein and H.F. Mattson Jr. Covering radius 1985–1994. *Applicable Algebra in Engineering Communication and Computing*, 8:173–239, 1997.

[5] T. Ebert. *Applications of recursive operators to randomness and complexity*. Ph.D. Thesis, University of California at Santa Barbara, 1998.

[6] A. Frieze and D. Sleator. Alan and Danny's puzzle page. URL: *http://www.cs.cmu.edu/puzzle*.

[7] H.W. Lenstra and G. Seroussi. On hats and other covers. *IEEE International Symposium on Information Theory*, 2002. URL: *http://www.hpl.hp.com/infotheory/hats_extsum.pdf*.

[8] S. Robinson. Why mathematicians now care about their hat color. *New York Times*, April 10, 2001.

[9] C.E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423 and 623–656, 1948.

[10] T. Worsch. Lower and upper bounds for (sums of) binomial coefficients. Technical Report 31/94, Universität Karlsruhe, Fakultät für Informatik, 1994. URL: *http://liinwww.ira.uka.de/~worsch/research/papers/bounds_for_sums_of_binomial_coeffs/index.html*