On hats and other covers

Hendrik W. Lenstra, Jr.
University of California, Berkeley
Berkeley, California, U.S.A.
e-mail: hwl@math.berkeley.edu

Gadiel Seroussi
Hewlett-Packard Laboratories
Palo Alto, California, U.S.A.
e-mail: seroussi@hpl.hp.com

I. Introduction

The following game puzzle has recently received attention from mathematicians, computer scientists, coding theorists, and even from the mass press [1]: A team of n players is fitted with hats, which are either red or green. A player can see the other players' hat colors, but not his own. Each player is then asked to declare his hat color, or pass. All the players must declare simultaneously, with no inter-player communication allowed 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 the correct color, and no player declares incorrectly. The goal of the team is to devise a strategy that maximizes the winning probability, under an assumption of uniform probability distribution on the hat color combinations.

A winning probability of 50% is guaranteed by a trivial strategy in which a designated player declares "red," and the rest "pass." The puzzle is popularly posed for $n = 3$. In that case, the following strategy yields a 75% winning probability, which turns out to be optimal: Upon observing the hats of the teammates, if a player sees two identical colors, he declares the opposite color, otherwise he passes. Clearly, the team wins whenever the color configuration consists of two hats of the same color and one of the opposite color, and it loses when the three hats are of the same color. Moreover, the following property holds: *In winning configurations, one player declares the correct color, and the rest pass; in losing configurations all the players declare a wrong color.* For any value of n, a strategy satisfying this property is said to be *perfect*. We will be interested in the behavior of the winning probability for the best strategies as a function of n, and in its asymptotic behavior as $n \to \infty$. We start with the binary (two-color) game just defined, and then generalize the problem to an arbitrary number $q \geq 2$ of colors.

II. Coverings for the Binary Game

Let 0 and 1 represent the colors in the binary hats game, let $N=\{1, 2, \ldots, n\}$, and let $V_n=\{0,1\}^n$ denote the n-dimensional binary space. A *deterministic n-player strategy* is a vector $\mathcal{F} = (f_1, f_2, \ldots, f_n)$, where the function $f_i : V_{n-1} \to \{0, 1, pass\}$, $i \in N$, encodes the instructions for player i, i.e., upon observing $\mathbf{u} \in V_{n-1}$, player i declares $f_i(\mathbf{u})$. Clearly, given a hats configuration $\mathbf{v} \in V_n$ and a strategy $\mathcal{F}$, it is uniquely determined whether $\mathcal{F}$ wins on $\mathbf{v}$ or not. For a given strategy $\mathcal{F}$, let $W_{\mathcal{F}} \subseteq V_n$ denote the set of winning configurations for $\mathcal{F}$. A 1-*covering* of V_n (in the Hamming metric) is a set $C \subseteq V_n$ such that for all $\mathbf{v} \in V_n$ there is a vector $\mathbf{c} \in C$ that differs from $\mathbf{v}$ in at most one coordinate [2].

Proposition 1 *There is a one-to-one correspondence between strategies for the binary hats game and 1-coverings of V_n. For each strategy $\mathcal{F}$, $C_{\mathcal{F}}=V_n \setminus W_{\mathcal{F}}$ is a 1-covering and, conversely, each 1-covering C is the losing set of a strategy $\mathcal{F}_C$. Moreover, $\mathcal{F}$ is perfect if and only if $C_{\mathcal{F}}$ is a perfect code.*

A strategy $\mathcal{F}_C$ corresponding to a 1-covering C has *losing probability* $P_L = |C|/|V_n| = 2^{-n}|C|$. For values $n = 2^m - 1$, the (perfect) binary Hamming code of length n defines a strategy with $P_L = (n+1)^{-1}$, and the winning probability $1 - P_L$ converges to 1 at the fastest possible rate. When n is not a Hamming length, a shorter Hamming code can be trivially lengthened to obtain $P_L < 2(n+1)^{-1}$. The factor of 2 relative to the optimal convergence is inevitable in the case of linear codes, but it follows from the results in [3] that one can construct sequences of *non-linear* 1-coverings with P_L approaching, asymptotically, the ideal $(n+1)^{-1}$.

III. Strong coverings for the q-ary game

We now consider a game where the hat colors are drawn from a q-ary alphabet Q, for an arbitrary integer $q \geq 2$. The playing rules remain the same as before. In this case, an approach based on q-ary 1-coverings quickly leads to disappointment, even in the case of perfect codes. Strategies derived from q-ary 1-coverings approach a winning probability of $(q-1)^{-1}$, which is fine when $q = 2$, but leaves room for improvement otherwise. As before, we characterize a deterministic strategy $\mathcal{F}$ in terms of its set $W \subseteq Q^n$ of winning configurations, and its complement $C = Q^n \setminus W$.

Proposition 2 *Let $\mathbf{w} = (w_1, w_2, \ldots, w_n)$. If $\mathbf{w} \in W$, then there exists a coordinate $i \in N$ such that for all $x \in Q \setminus \{w_i\}$, we have $(w_1, w_2, \ldots, w_{i-1}, x, w_{i+1}, \ldots, w_n) \in C$. Conversely, any set C satisfying this condition defines a strategy for the q-ary game.*

We call a set C as in Proposition 2 a *strong covering* of Q^n. A sphere-packing-type bound exists for strong coverings, as well as a notion of a *perfect strong covering*, which corresponds to a perfect strategy as defined in Section I (the definition carries to $q > 2$). However, the following proposition holds.

Proposition 3 *There are no perfect strong coverings for $q>2$ and $n>1$.*

Assume Q is endowed with an abelian group law. Then, we can efficiently construct C in the following proposition.

Proposition 4 *There is a strong covering C of Q^n, with $P_L = |C|q^{-n} = O(n^{-c})$, with $c \geq (1-q^{-1})(1+(2(q-1)^{-1})(e\log(q-1))^{-1}$.*

For $0 \ll q \ll n$, the dominant term in the exponent c is of the form $1/(e\log(q-1))$. Noga Alon [4], using a non-constructive random-coding argument, showed the existence of strong coverings with $P_L = O((q\log n)/n)$. The full paper will expand on these results and their proofs, as well as on deterministic, probabilistic, and symmetric variants of the basic game.

Acknowledgments. Thanks to Joe Buhler for introducing us to the problem and stimulating discussions, and to Noga Alon for [4].

References

[1] S. Robinson, "Why mathematicians now care about their hat color," The New York Times, Science Times section, p. D5, April 10, 2001.

[2] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North-Holland, Amsterdam, 1997.

[3] G.A. Kabatyanskii and V.I. Panchenko, "Unit sphere packings and coverings of the Hamming space," *Probl. Peredachi Informatsii*, vol. 24, No. 4, pp. 3–16, 1988. Translated in *Probl. Inform. Transm.*, vol. 24, No. 4, pp. 261–272.

[4] N. Alon, personal communication.