Random Packings and Coverings of the Unit n-Sphere

By A. D. WYNER

(Manuscript received July 13, 1967)

It is well known that the quantity $M_p(n, \theta)$, the maximum number of nonoverlapping spherical caps of half angle θ (a "packing") which can be placed on the surface of a unit sphere in Euclidean n-space is not less than $\exp[-n \log \sin 2\theta + o(n)]$ ($\theta < \pi/4$). In this paper we give a new proof of this fact by a "random coding" argument, the central part of which is a theorem which asserts that if a set of roughly $\exp(-n \log \sin 2\theta)$ caps is chosen at random, that on the average only a very small fraction of the caps will overlap (when n is large).

A related problem is the determination of $M_c(n, \theta)$, the minimum number of caps of half angle θ required to cover the unit Euclidean n-sphere. We show that $M_c(n, \theta) = \exp[-n \log \sin \theta + o(n)]$. The central part of the proof is also a random coding argument which asserts that if a set roughly $\exp(-n \log \sin \theta)$ caps is chosen at random, that on the average only a very small fraction of the surface of the n-sphere will remain uncovered (when n is large).

I. INTRODUCTION

A problem in coding theory for the Gaussian channel is the determination of $M_p(n, \theta)$, the maximum number of points which may be placed on the surface of a unit n-sphere such that the spherical caps with centers at these points and half angle θ are disjoint (the "packing" problem). This quantity, though unknown, has been estimated by upper and lower bounds.[5] In this paper, we give a proof of the known lower bound by a "random coding" argument. It is felt that this new method is of interest in itself.

A related problem is the "covering" problem, the determination of $M_c(n, \theta)$, the minimum number of caps of half angle θ required to cover the surface of a unit n-sphere. This problem is of interest when one wants to quantize an n-dimensional Gaussian vector with independent components (which with very high probability lies near the surface of an n-sphere). In this paper, $M_c(n, \theta)$ is estimated with upper and lower bounds which are "exponentially" tight. The upper bound is also proved by a "random coding" argument.

The random coding arguments owe much to Shannon.[3,4] The random covering theorem in particular is similar to his approximation theorem in the latter reference. R. Graham has called my attention to the work of Rogers,[1,2] who has considered the problem of covering a large n-dimensional cube with spheres of a unit radius. Rogers' methods and result parallel those given here.

Let x, y with and without subscripts denote points on $\mathcal{S}_n$, the surface of a unit sphere in n-dimensional Euclidean space. Let $\alpha(x, y)$ be the angle* between x and y, and note that $\alpha(x, y)$ satisfies the axioms of a metric. For $0 \leqq \theta \leqq \pi$, let $\mathcal{C}(x, \theta) = \{y : \alpha(x, y) < \theta\}$, the open spherical cap of half angle θ centered at x. A set $S \subseteq \mathcal{S}_n$ is said to be a *θ-covering* $(0 \leqq \theta \leqq \pi)$ if $\bigcup_{x \in S} \mathcal{C}(x, \theta)$ covers $\mathcal{S}_n$, and $S \subseteq \mathcal{S}_n$ is said to be a *θ-packing* if $\mathcal{C}(x, \theta) \cap \mathcal{C}(y, \theta)$ is empty for $x, y \in S$, $x \neq y$. Let $M_c(n, \theta)$ be the minimum number of points which can constitute a θ-covering of $\mathcal{S}_n$ and let $M_p(n, \theta)$ be the maximum number of points which can constitute a θ-packing. These quantities are related by

Lemma 1: $M_c(n, 2\theta) \leqq M_p(n, \theta)$.

Proof: We say that $S \subseteq \mathcal{S}_n$ is a *maximal θ-packing* if S is a θ-packing, and for all $y \notin S$, the union $\{y\} \cup S$ is not a θ-packing. We establish Lemma 1 by showing that every maximal θ-packing is a 2θ-covering. Let S be a maximal θ-packing. If S is not a 2θ-covering then there exists a y such that $\alpha(x, y) \geqq 2\theta$ for all $x \in S$. Thus, from the triangle inequality for α, $\mathcal{C}(x, \theta) \cap \mathcal{C}(y, \theta) = \Phi$ for all $x \in S$, and $\{y\} \cup S$ is a θ-packing contradicting the maximality of S. Hence, the lemma.†

The quantity $M_p(n, \theta)$ is well studied.[5] In particular, it is known that (for $\theta < \pi/4$)

$$\exp\,[nP_L(\theta)(1 + \beta_n(\theta))] \leqq M_p(n, \theta) \leqq \exp\,[nP_U(\theta)(1 + \gamma_n(\theta))], \quad (1a)$$

where $\beta_n, \gamma_n \to 0$ as $n \to \infty$ and

$$P_L(\theta) = -\log \sin 2\theta, \quad (1b)$$

* The angle is defined as follows. Say that the center of the unit sphere is the origin of coordinates in n-space. Then x and y may be thought of a unit vectors. The angle $\alpha(x, y)$ between them is defined by $\cos \alpha =$ inner product of x and y, where $0 \leqq \alpha \leqq \pi$.

† The fact that it does not seem possible to obtain a reverse inequality relating M_c and M_p may lead one to suspect that covering and packing are, in fact, not dual problems. This may account for the fact that random coding appears "better" for covering than for packing.

and

$$P_U(\theta) = -\log \sqrt{2} \sin \theta. \tag{1c}$$

Thus, roughly speaking $M_p(n, \theta)$ increases exponentially in n (as $n \to \infty$) with exponent between P_L and P_U.

In Section III we give another proof of the lower bound in (1). The central part of this proof is a theorem that asserts that if a packing with roughly exp $[nP_L(\theta)]$ points is chosen at random, that on the average only a very small fraction of the caps will overlap (Theorem 1). The lower bound of (1) is a corollary to this theorem. It is felt that Theorem 1 is of interest in itself.

Now consider $M_c(n, \theta)$. We will show that it too increases roughly exponentially in n (as $n \to \infty$). But here we can find the exponent exactly, viz., (for $\theta < \pi/2$)

$$M_c(n, \theta) = \exp [nR_c(\theta)(1 + \epsilon_n(\theta))], \tag{2a}$$

where $\epsilon_n \to 0$ as $n \to \infty$ and

$$R_c(\theta) = -\log \sin \theta. \tag{2b}$$

The central part of the proof of the existence of a covering satisfying (2) is a theorem which asserts that if a covering with roughly exp $[nR_c(\theta)]$ points is chosen at random, that on the average only a very small fraction of $\mathcal{S}_n$ will remain uncovered.

II. THEOREMS

In this section we give precise statements of our theorems, leaving the proofs for Section III. We begin with some definitions.

Assign the usual "area" measure to $\mathcal{S}_n$. If $A \subseteq \mathcal{S}_n$ is measurable, let $\mu(A)$ be its measure. In particular, let

$$C_n(\alpha) = \mu(\mathcal{C}(x, \alpha)) = \frac{(n-1)\pi^{(n-1)/2}}{\Gamma[(n+1)/2]} \int_0^\alpha \sin^{(n-2)} \varphi \, d\varphi \tag{3a}$$

be the area (measure) of a cap of half-angle α, and let

$$C_n(\pi) = \frac{n\pi^{n/2}}{\Gamma[(n+2)/2]} \tag{3b}$$

be the area of $\mathcal{S}_n$. It is easy to show that (for $\alpha < \pi/2$)

$$\frac{C_n(\pi)}{C_n(\alpha)} = \exp \left\{ n \log \left(\frac{1}{\sin \alpha} \right) + o(n) \right\}. \tag{4}$$

as $n \to \infty$.

In connection with the packing problem, let $S = \{x_i\}_{i=1}^{M} \subseteq \mathcal{S}_n$, and consider $\{\mathcal{C}(x_i, \theta)\}_{i=1}^{M}$ the corresponding caps of half-angle θ. Define

$$F_p(S, \theta) = \frac{1}{M} \sum_{i=1}^{M} g_i(S, \theta), \tag{5a}$$

where g_i $(i = 1, 2, \cdots, M)$ is defined by

$$g_i(S, \theta) = \begin{cases} 1, & \mathcal{C}(x_i, \theta) \cap \mathcal{C}(x_j, \theta) = \Phi \quad \text{all} \quad j \neq i, \\ 0, & \text{otherwise}. \end{cases} \tag{5b}$$

Thus, $F_p(S, \theta)$ is the fraction of the caps which do not overlap. Notice that S is a θ-packing if and only if $F_p(S, \theta) = 1$. We now state

Theorem 1: (Random Packing) Consider a random experiment in which the M members of S are chosen independently with uniform distribution on $\mathcal{S}_n$. $F_p(S, \theta)$ is then a random variable. Let θ be fixed and let M increase as $n \to \infty$, then

$$\text{if} \qquad M \frac{C_n(2\theta)}{C(\pi)} \to \infty, \qquad EF_p(S, \theta) \to 0 \tag{6a}$$

and

$$\text{if} \qquad M \frac{C_n(2\theta)}{C(\pi)} \to 0, \qquad EF_p(S, \theta) \to 1, \tag{6b}$$

where E denotes expectation.

Thus, in particular, if $M = e^{\rho n}$ (ρ fixed), we have from (4) that $EF_p(S, \theta) \to 1$ or 0 according as $\rho < -\log \sin 2\theta = P_L(\theta)$ or $\rho > P_L(\theta)$. Further, since there must be a set S such that $F_p(S, \theta) \geqq EF_p$, we conclude that for any $\rho < P_L(\theta)$ and any $\epsilon > 0$ there exists an n sufficiently large and a set $S \subseteq \mathcal{S}_n$ with $M = e^{\rho n}$ members such that

$$F_p(S, \theta) \geqq 1 - \epsilon. \tag{7}$$

If we delete the (ϵM) members of S with overlapping caps we obtain a θ-packing with $M = e^{\rho n}(1 - \epsilon)$ points. This is equivalent to the lower bound of (1).

Let us now turn to the covering problem. We can easily establish a lower bound on $M_c(n, \theta)$ as follows. Let $S = \{x_i\}_{i=1}^{M} \subseteq \mathcal{S}_n$ be a θ-covering, so that $\bigcup_{i=1}^{M} \mathcal{C}_n(x_i, \theta)$ covers $\mathcal{S}_n$. Hence,

$$C_n(\pi) = \mu(\mathcal{S}_n) = \mu \bigcup_{i=1}^{M} \mathcal{C}(x_i, \theta) \leqq \sum_{i=1}^{M} \mu(\mathcal{C}(x_i, \theta)) = MC_n(\theta). \tag{8}$$

Thus, we have proved

Lemma 2: $M_c(n, \theta) \geqq C_n(\pi)/C_n(\theta)$.

In the light of (4), Lemma 2 implies that M_c is not less than the right member of (2a) for $\theta < \pi/2$.

Let $\beta > 0$ and $S \subseteq \mathcal{S}_n$ be given. Define the set

$$B(S, \beta) = \{y \in \mathcal{S}_n : y \notin \mathcal{C}(x, \beta) \text{ for all } x \in S\}. \tag{9a}$$

Then

$$F_c(S, \beta) = \mu(B(S, \beta))/C_n(\pi) \tag{9b}$$

represents that fraction of $\mathcal{S}_n$ not covered by the caps $\mathcal{C}(x, \beta)$, $x \in S$. We now state

Theorem 2: (Random Covering) Consider a random experiment in which the M members of a set S are chosen independently with uniform distribution on $\mathcal{S}_n$. Then $F_c(S, \beta)$ is a random variable. Let $\beta < \pi$ be fixed and let M increase as $n \to \infty$, then

$$\textit{if} \qquad M \frac{C_n(\beta)}{C_n(\pi)} \to \infty, \qquad E(F_c) \to 0, \tag{10a}$$

and

$$\textit{if} \qquad M \frac{C_n(\beta)}{C_n(\pi)} \to 0, \qquad E(F_c) \to 1. \tag{10b}$$

Further,

$$E(F_c) \leqq \exp\left\{-M \frac{C_n(\beta)}{C_n(\pi)}\right\}. \tag{11}$$

In particular, if $M = e^{\rho n}$ (ρ fixed) and $\beta < \pi/2$, we have from (10) and (4) that $E(F_c) \to 0$ or 1 according as $\rho > -\log \sin \beta = R_c(\beta)$ or $\rho < R_c(\beta)$. Further, since there must be at least one set S for which $F_c(S, \beta) \leqq EF_c$, we conclude from (11) and (4) that for any $\beta < \pi/2$ and any $\rho > R_c(\beta)$ there exists for each $n = 1, 2, \cdots$ a set $S \subseteq \mathcal{S}_n$ with $M = e^{\rho n}$ members such that

$$\frac{\mu(B(S, \beta))}{C_n(\pi)} \leqq \exp\{-\exp[(\rho - R_c(\beta))n(1 + \lambda(\beta))]\}, \tag{12}$$

where $\lambda(\beta) \to 0$ as $n \to \infty$. The following corollary (also proved in Section III) follows from (12).

Corollary: Let $\theta (0 < \theta < \pi/2)$ be arbitrary and let $\rho > R_c(\theta)$. Then for n sufficiently large there exists at θ-covering of $\mathcal{S}_n$ with $M = e^{\rho n}$ points.

It remains to show that M_c is not more than the right member of (2a). For $\theta < \pi/2$ let

$$\rho^*(\theta) = \limsup_{n\to\infty} \frac{1}{n} \log M_c(n, \theta).$$

Say $\rho^* > R_c(\theta)$. Let $\rho' = (R(\theta) + \rho^*(\theta))/2 < \rho'$. We conclude that there is an infinite sequence of n's such that any set of $e^{\rho' n}$ points in $\mathcal{S}_n$ cannot be a θ-covering. But since $\rho' > R_c(\theta)$, application of the above corollary yields a contradiction. Thus, $\rho^* \leqq R_c(\theta)$. This taken together with Lemma 2 gives

$$\lim_{n\to\infty} \frac{1}{n} \log M(n, \theta) = R_c(\theta),$$

from which (2) follows.

III. PROOFS

Proof of Theorem 1: Let the points $x_1, x_2, \cdots, x_M \in \mathcal{S}_n$ be chosen independently with a uniform distribution on $\mathcal{S}_n$. The random variables g_i $(i = 1, 2, \cdots, M)$ defined in (5b) may be rewritten

$$g_i(x_1, x_2, \cdots, x_M, \theta) = \begin{cases} 1, & \alpha(x_i, x_j) \geqq 2\theta, \quad j \neq i, \\ 0, & \text{otherwise}. \end{cases} \tag{13}$$

Thus, the random variable F_p of (5a) has expectation

$$EF_p = \frac{1}{M} \sum_{i=1}^{M} Eg_i = \frac{1}{M} \sum_{i=1}^{M} \Pr\{g_i = 1\}. \tag{14}$$

Let i be fixed. If $x_i = x$ then $g_i = 1$ if and only if the $(M - 1)$ independent choices of $x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_M$ do not belong to $\mathcal{C}(x, 2\theta)$. Since the x_i are uniformly distributed on $\mathcal{S}_n$ we have

$$\Pr\{g_i = 1 \mid x_i = x\} = \left(1 - \frac{C_n(2\theta)}{C_n(\pi)}\right)^{M-1},$$

independent of x. Thus, from (14)

$$E(F_p) = \left(1 - \frac{C_n(2\theta)}{C_n(\pi)}\right)^{M-1} = \left(1 - \frac{1}{\mu_n}\right)^{\mu_n[(M-1/\mu_n)]}, \tag{15}$$

where $\mu_n = C_n(\pi)/C_n(2\theta)$. Our result follows on noting that as $n \to \infty$,

$$(1 - 1/\mu_n)^{\mu_n} \to e^{-1} \quad \text{and} \quad (M - 1)/\mu_n \approx MC_n(2\theta)/C_n(\pi).$$

Proof of Theorem 2: Let the points $x_1, x_2, \cdots, x_M \in \mathcal{S}_n$ be chosen independently with a uniform distribution on $\mathcal{S}_n$. The random variable F_c may be written

$$F_c = \frac{1}{C_n(\pi)} \int_{\mathcal{S}_n} h(y, x_1, x_2, \cdots, x_M)\, d\mu(y), \tag{16}$$

where

$$h(y, x_1, \cdots, x_M) = \begin{cases} 1, & \text{if} \quad \alpha(x_i, y) \geqq \theta, \qquad 1 \leqq i \leqq M \\ 0, & \quad \text{otherwise.} \end{cases}$$

Since $h \geqq 0$ we may interchange the expectation and integration operations and obtain

$$EF_c = \frac{1}{C_n(\pi)} \int_{\mathcal{S}_n} d\mu(y) Eh(y, x_1, \cdots, x_M),$$

where as indicated Eh is computed with y held fixed. Now

$$\begin{aligned} Eh(y, x_1, \cdots, x_M) &= \Pr\{h = 1\} = \Pr \bigcap_{i=1}^{M} \{\alpha(x_i, y) \geqq \theta\} \\ &= \left(1 - \frac{C_n(\theta)}{C_n(\pi)}\right)^M \leqq \exp\,[-MC_n(\theta)/C_n(\pi)], \end{aligned}$$

from which (10) and (11) follow.

Proof of Corollary to Theorem 2: Let $\rho > R_c(\theta)$ be given. Let γ be defined by $R_c(\gamma) = \rho$. Since $\rho > R_c(\theta)$ a decreasing function, we have $\gamma < \theta$. We will apply Theorem 2 with $\beta = (\theta + \gamma)/2$, so that $\rho > R(\beta)$. Let S_n $(n = 1, 2, \cdots)$ be the sets which satisfy (12). By (4) and (12), $C_n[(\theta - \gamma)/2]/C_n(\pi)$ decreases much more slowly (as $n \to \infty$) than $[\mu(B(S_n, \beta))]/C_n(\pi) \triangleq \delta_n$, so that we can find an N sufficiently large such that for $n \geqq N$,

$$\delta_n < \frac{C_n[(\theta - \gamma)/2]}{C_n(\pi)}.$$

We claim that for $n > N$, the sets S_n are θ-coverings of $\mathcal{S}_n$. To show this observe that if $y \notin \bigcup_{x_i \in S_n} \mathcal{C}(x_i, \theta)$, then $\alpha(x_i, y) \geqq \theta$, all $x_i \in S_n$. Thus,

$$\mathcal{C}\left(y, \frac{\theta - \gamma}{2}\right) \cap \mathcal{C}\left(x_i, \frac{\theta + \gamma}{2}\right) = \Phi \text{ for all } x_i \in S_n,$$

which in turn implies

$$\mathcal{C}\left(y, \frac{\theta - \gamma}{2}\right) \subseteq B\left(S_n , \frac{\theta + \gamma}{2}\right).$$

Thus,

$$\delta_n = \frac{\mu\left\{B\left(S_n , \frac{\theta + \gamma}{2}\right)\right\}}{C_n(\pi)} \geqq \frac{\mu\left\{\mathcal{C}\left(y, \frac{\theta - \gamma}{2}\right)\right\}}{C_n(\pi)} = \frac{C_n\left(\frac{\theta - \gamma}{2}\right)}{C_n(\pi)},$$

a contradiction. Thus, there is no such y and the corollary follows.

REFERENCES

1. Rogers, C. A., A Note on Coverings, Mathematica, *4,* 1957, pp. 1–6.
2. Rogers, C. A., *Packing and Covering,* Cambridge University Press, Cambridge, 1964.
3. Shannon, C. E., A Mathematical Theory of Communication, B.S.T.J., *27,* 1948, pp. 379–423 and pp. 623–656.
4. Shannon, C. E., Coding Theorems for a Discrete Source with a Fidelity Criteria, 1959 IRE Conv. Record, Part 4, pp. 142–163.
5. Wyner, A. D., Capabilities of Bounded Discrepancy Decoding, B.S.T.J., *44,* 1965, pp. 1061–1122. (The tightest known bounds are summarized on pp. 1071–1072, Eq. 24.)