SETS OF VISIBLE POINTS

Thesis by

Howard Rumsey, Jr.

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1961

ACKNOWLEDGEMENTS

I am indebted to Professor T. M. Apostol for his interest, encouragement and advice and to Dr. David F. Rearick who first aroused my interest in the problems treated in this thesis. I wish to thank the California Institute of Technology and the National Science Foundation for the scholarships and fellowships with which they provided me. And special thanks go to my wife, Jo Anne, for her constant encouragement and competence in typing the manuscript.

TABLE OF CONTENTS

ABSTRACT

We say that two lattice points are visible from one another if there is no lattice point on the open line segment joining them. If Q is a subset of the n-dimensional integer lattice L^n, we write VQ for the set of points which can see every point of Q, and we call a set S a set of visible points if S = VQ for some set Q.

In the first section we study the elementary properties of the operator V and of certain associated operators. A typical result is that Q is a set of visible points if and only if Q = V(VQ). In the second and third sections we study sets of visible points in greater detail. In particular we show that if Q is a finite subset of L^n, then VQ has a "density" which is given by the Euler product

$$\prod_p \left(1 - \frac{r_p(Q)}{p^n}\right)$$

where the numbers $r_p(Q)$ are certain integers determined by the set Q and the primes p. And if Q is an infinite subset of L^n, we give necessary and sufficient conditions on the set Q such that VQ has a density which is given by this or other related products.

In the final section we compute the average values of a certain class of functions defined on L^n, and we show that the resulting formula may be used to compute the density of a set of visible points VQ generated by a finite set Q.

§ 1. Definitions and Elementary Properties of Sets of Visible Points.

Let L^n be the n-dimensional integer lattice consisting of points of the form $x = (x_1, x_2, \ldots, x_n)$ with integer coordinates. If x and y are points of L^n and if m is a positive integer, we write

$$(1.1) \qquad x \equiv y \ (m)$$

to indicate that $x_i \equiv y_i \ (m)$ for $i = 1, 2, \ldots, n$. In other words the points x and y are congruent modulo m if and only if m divides each component of the vector $x - y$.

We say that two distinct points of L^n are mutually visible if there is no point of L^n on the open line segment joining them. If x and y are mutually visible, we say that "x can see y" or "y can see x", and we stipulate that a point can not see itself.

It was proved in [2] that two points are mutually visible if and only if the greatest common divisor of the components of the vector connecting them is one. For our purpose it will be more convenient to use a condition stated in terms of the congruence relation (1.1).

Theorem 1.1. Let x and y be two points of L^n. Then x and y are mutually visible if and only if the congruence $x \equiv y \ (p)$ is false for all primes p.

Proof: Since the theorem is evident if $x = y$, we assume that x and y are distinct points. We prove the theorem by showing that there is a point of L^n on the open line segment joining x and y if and only if $x \equiv y\ (p)$ for some prime p. Assume that z is any point on this line segment; then we can write $z = y + t(x - y)$ for some $0 < t < 1$. If z is also a point of L^n, then t must be a rational number, and we can write $t = a/b$ where a and b are relatively prime integers. But if p is any prime which divides b, then it is clear that p must divide each component of the vector $x - y$; that is $x \equiv y\ (p)$. Conversely, if we assume $x \equiv y\ (p)$ for some prime p, then $z = y + (x - y)/p$ is a point of L^n on the open line segment joining x and y. This completes the proof.

In view of Theorem 1.1 it is convenient to extend our concept of mutual visibility. Thus, if p is any prime, we say two points x and y are mutually visible modulo p if $x \not\equiv y\ (p)$. If x and y are mutually visible modulo p, we say that "x can see y modulo p" and "y can see x modulo p". Theorem 1.1 can be restated as follows:

Two points x and y are mutually visible if and only if x can see y modulo p for all primes p.

If Q is a subset of L^n ($Q \subseteq L^n$) and x a point of L^n ($x \in L^n$), we say that x can see Q if x can see every point of Q. We write VQ for the set of all points which can see Q, and we say that a set S is a "set of visible points" if there is a set Q such that $S = VQ$. Similarly, we write V_pQ for the set of points which can see Q modulo p. Using Theorem 1.1, we have

(1.2) $$VQ = \bigcap_p V_pQ$$

where the intersection is over all primes p.

Symbolically we can represent the set V_pQ as follows:

(1.3) $$V_pQ = \{x \in L^n \mid x \not\equiv y\ (p) \text{ for all } y \in Q\}.$$

This construction is rather awkward, therefore we introduce the sets X_pQ which are defined to be the complements of the sets V_pQ. We have

(1.4) $$X_pQ = (V_pQ)' = \{x \in L^n \mid x \equiv y\ (p) \text{ for some } y \in Q\}.$$

Example 1. Let Q be the subset of L^2 consisting of the points $(k,0)$ for $k = 0, \pm 1, \pm 2, \ldots$. Writing Q_p for the set of least positive residues* modulo p generated by the points of Q, we have

$$Q_p = \{(0,0), (1,0), \ldots, (p-1,0)\}.$$

Therefore $$X_pQ = \{x \in L^2 \mid (x_1, x_2) \equiv (r,0)\ (p) \text{ for some } 0 \leq r < p\}.$$

$$= \{x \in L^2 \mid x_2 \equiv 0\ (p)\}.$$

In other words, the points that can not see Q modulo p are just the lattice points on the lines $x_2 = jp$ where j is an integer. We compute V_pQ

---

* If x is a point of L^n and m a positive integer, we say that y is the least positive residue of x modulo m if $y \equiv x$ (m) and $0 \leq y_i < m$ for $i = 1, 2, \ldots, n$.

as follows:

$$V_pQ = (X_pQ)' = \left\{x \in L^2 \;\middle|\; x_2 \not\equiv 0 \ (p)\right\}.$$

Using (1.2) we find

$$VQ = \bigcap_p V_pQ = \left\{x \in L^2 \;\middle|\; x_2 \not\equiv 0 \ (p) \text{ for all primes } p\right\}$$

$$= \left\{x \;\middle|\; x_2 = \pm 1\right\}.$$

Therefore the points that can see Q are just the lattice points directly above and directly below the x_1-axis. We might also ask for the set of points that can see VQ. From the definition of VQ it is evident that any point of Q can see VQ; and in this example we can show, quite easily, that the <u>only</u> points which can see VQ are those of Q. Therefore, writing V^2Q for $V(VQ)$, we have $V^2Q = Q$, and Q itself is a set of visible points. We shall see later that the equation $V^2Q = Q$ is a necessary and sufficient condition that a set Q be a set of visible points.

<u>Example 2.</u> Let Q be as in Example 1 and let R be any subset of Q of the form $R = \left\{(k,0)\right\}$ where $k \geq m$ for some fixed integer m. Writing R_p for the set of least positive residues modulo p generated by R, we see that

$$R_p = \left\{(r,0)\right\} \text{ where } r = 0, 1, \ldots, p-1.$$

Therefore $R_p = Q_p$ and it follows that the sets R and Q have the same set of visible points.

Example 3. Let S be the set of points $\{(q,q^2)\}$ where q ranges over the set of primes. To compute S_p (defined as above) we note that if p is a fixed prime, the set of all primes, $\{q\}$, generates a complete residue system modulo p by Dirichlet's theorem. Thus

$$S_p = \{(r,r^2)\} \quad \text{where } r = 0,1, \ldots ,p-1,$$

and $$X_pS = \{x \mid x_1 \equiv r\ (p), x_2 \equiv r^2(p) \text{ for some } r = 0,1, \ldots ,p-1\}.$$

$$= \{x \mid x_2 \equiv x_1^2\ (p)\}.$$

The points that can not see Q modulo p are, therefore, just the lattice points on the parabolas $x_2 = x_1^2 + jp$ where j is an integer. By a computation similar to the one used in Example 1, we have

$$VS = \{x \mid x_2 = x_1^2 \pm 1\},$$

$$V^2S = \{x \mid x_2 = x_1^2\} \supset S$$

and $$V^3S = V(V^2S) = VS.$$

These examples illustrate that sets of the form X_pQ are fundamental to the study of sets of visible points. To further our understanding of such sets we make the following definitions:

Definition 1.1. Let Q be a subset of L^n and let m be a positive integer. We define the sets Q_m and X_mQ as follows:

$$Q_m = \{x \in L^n \mid 0 \leq x_i < m \text{ for } i = 1,2, \ldots, n; \text{ and } x \equiv y \ (m) \text{ for some } y \in Q\}$$

(1.5) $$X_m Q = \{x \in L^n \mid x \equiv y \ (m) \text{ for some } y \in Q_m\}.$$

In addition, we define $r_m(Q)$ to be the number of points in Q_m.

In other words, Q_m is the set of least positive residues modulo m generated by the points of Q; and $r_m(Q)$ is the number of distinct, least positive residues modulo m generated by Q. The sets Q_m are generalizations of the sets Q_p, R_p and S_p which we used in Examples 1, 2 and 3. It is clear, from these same examples, that when m is a prime, the definition of the set $X_m Q$ is consistent with the definition of the sets $X_p Q$ given by (1.4).

It is convenient to have a name for sets which are constructed in the manner indicated by (1.5). Thus, we say that a set S is "periodic with period m" if we can write $S = X_m Q$ for some $Q \subseteq L^n$. We can eliminate the set Q which occurs in this statement by writing $S = X_m S$ which will hold if and only if S is a periodic set with period m. The reason for the name "periodic" is that if S is a periodic set with period m, then the characteristic function of S is a periodic function with period m in each of the components of its argument.

It is clear from (1.5) that the complement of a periodic set is periodic. Thus, for example, the sets $V_p Q = (X_p Q)'$ are periodic; and we compute*

$$(1.6) \qquad r_p(V_pQ) = p^n - r_p(X_pQ) = p^n - r_p(Q).$$

Example 4. Let Q be the set $\{(2,4),(6,0)\}$. We have

$$Q_2 = \{(0,0)\}$$
$$X_2Q = \{x \mid x \equiv (0,0)\ (2)\}$$
$$V_2Q = \{x \mid x \not\equiv (0,0)\ (2)\}$$
$$= \{x \mid x \equiv (1,0),(0,1) \text{ or } (1,1) \text{ modulo } 2\}.$$

Therefore $\quad r_2(X_2Q) = r_2(Q_2) = r_2(Q) = 1$ and $r_2(V_2Q) = 3$.

In the following theorem we state an important property which will enable us to approximate sets of visible points with periodic sets by using the identity $VQ = \bigcap_p V_pQ$.

Theorem 1.2. Let $S_1, S_2, \ldots, S_k$ be periodic subsets of L^n with periods $m_1, m_2, \ldots, m_k$ respectively. Then, if the m_i's are coprime in pairs, the set $S = \bigcap_{i=1}^{k} S_i$ is periodic with period $m = m_1 m_2 \cdots m_k$ and

$$r_m(S) = \prod_{i=1}^{k} r_{m_i}(S_i).$$

Proof: We prove the theorem for the case of two periodic sets A and B with relatively prime periods a and b; the general result then follows by the obvious induction argument. Let $S = A \cap B$, then we have

---

* Using the fact that there are exactly p^n least positive residues modulo p.

by a simple computation

$$S = \left\{ x \in L^n \,\middle|\, \begin{array}{l} x \equiv u \ (a) \text{ for some } u \in A_a; \text{ and} \\ x \equiv v \ (b) \text{ for some } v \in B_b \end{array} \right\}.$$

For a fixed u and v the system of congruences

$$(1.7) \qquad \begin{array}{l} x \equiv u \ (a) \\ x \equiv v \ (b) \end{array}$$

has, by the Chinese Remainder Theorem [1], a solution which is unique modulo $m = ab$. In other words, if we denote the least positive solution of (1.7) by $x(u,v)$, then x is a root of (1.7) if and only if

$$x \equiv x(u,v) \ (m).$$

It is apparent from this that S is a periodic set with period m. To compute $r_m(S)$, we need to count the number of distinct values that $x(u,v)$ can assume. But by definition there are exactly $r_a(A)$ choices for the point $u \in A_a$ and $r_b(B)$ choices for $v \in B_b$. A simple argument shows that each choice of u and v leads to a distinct value for $x(u,v)$. Therefore $r_m(S) = r_a(A)r_b(B)$ which completes the proof of the theorem.

In the following theorem we list the properties of sets of visible points which we use in our subsequent analysis.

Theorem 1.3. If Q is a subset of L^n then

(1.8) $$V^2Q \supseteq \bigcap_p X_pQ \supseteq Q,$$

(1.9) $$V^3Q = VQ = \bigcap_p X_p(VQ),$$

(1.10) Q is a set of visible points if and only if $V^2Q = Q$.

Proof: First we show that $V_p(VQ) \supseteq X_pQ$. Assume $x \in X_pQ$, then $x \equiv u\ (p)$ for some point $u \in Q$. This point u can clearly see VQ and in particular u can see VQ modulo p. But since x and u are congruent modulo p, it follows that x can also see VQ modulo p. This proves $V_p(VQ) \supseteq X_pQ$. To prove the first part of (1.8), we write

$$V^2Q = V(VQ) = \bigcap_p V_p(VQ) \supseteq \bigcap_p X_pQ.$$

The second part of (1.8) is obvious since $u \in Q$ implies $u \in X_pQ$ for all primes p.

Applying (1.8) to the set VQ, we see that $V^3Q \supseteq VQ$. To prove the inequality goes the other way, assume $x \in V^3Q$. Then x can see V^2Q which implies by (1.8) that x can see Q. Therefore $x \in VQ$ which proves the first part of (1.9). The second part follows from another application of (1.8) to the set VQ.

To prove (1.10), we observe that if $V^2Q = Q$, then Q is clearly a set of visible points ($Q = V(VQ)$). Conversely, assume Q is a set of visible points. Then $Q = VS$ for some set S. But by (1.8) we have

$$V^2Q = V^3S = VS = Q,$$

which completes the proof of the theorem.

An important consequence of this theorem is that sets of visible points occur in conjugate pairs. That is, if Q is a set of visible points, then the set VQ is at once the set of points that can see Q and the set of points which Q can see ($Q = V(VQ)$).

§ 2. Sets of Visible Points Generated by Finite Sets.

In the preceeding section we discovered some of the combinatorial properties of sets of visible points and of periodic sets. In this section we probe more deeply into the nature of sets of visible points. Our principal tool will be the idea of the "density" of a set. However, even without a formal definition of density, we can make many plausible statements about sets of visible points.

Consider, for example, the question: What is the probability* that a point $x \in L^n$ can see a fixed point $b \in L^n$? To answer this question we ask first for the probability that x can see b modulo p for some fixed prime p. To compute this probability, we note that there are exactly p^n least positive residues modulo p. It seems reasonable to assign each of these residues the same probability. Therefore, since the event "x can see b modulo p" is equivalent to the event $x \not\equiv b$ (p), we could assign the probability $(1 - p^{-n})$ to the event "x can see b modulo p". It also seems reasonable that the events "x can see b modulo p" should be independent for distinct primes p. Thus we are tempted to write

---

* We make no attempt to justify the use of the language of probability theory. However, all the statements made in this introduction can be formulated in terms of the concept of the density of a set (Def. 2.1), and most of them will be proved in our subsequent analysis.

(2.1) $$\Pr(x \text{ can see } b) = \prod_p \Pr(x \text{ can see } b \text{ modulo } p)$$

$$= \prod_p (1 - p^{-n}) .$$

We might also ask for the probability that a point x can see a given subset Q of L^n. An argument much like the one used to obtain (2.1) indicates that the following expression is a plausible answer:

(2.2) $$\Pr(x \text{ can see } Q) = \prod_p \Pr(x \text{ can see } Q \text{ modulo } p)$$

$$= \prod_p (1 - \frac{r_p(Q)}{p^n}).$$

Various forms of (2.1) have been proved in the literature [1,3]. Rearick [2] has also derived (2.2) in the special cases where Q is a set consisting of two points of L^n or where Q consists of k mutually visible points of L^n. The methods used by these researchers are those of Analytic Number Theory, involving the application of limiting processes to finite sums which are used for counting visible points in certain regions. In this section we shall prove that (2.2) is valid for all sets $Q \subseteq L^n$ which contain at most a finite number of points. The methods we use are combinatorial in nature and are motivated by our preceding discussion of probabilities, though we shall make no attempt to point out the probabilistic interpretation of each of our results. In § 3 we apply these same methods to sets Q containing an infinite number of points; however in this case we shall see that the problem is much more difficult.

We begin with a definition of the density of a set $Q \subseteq L^n$. The usual definition of density is made in terms of rectangular solids "expanding to cover L^n". Thus, to define the density of Q, we compute the density of Q in a rectangular solid of the form

$$R_{a,b} = \{ x \in L^n \mid a \leq x < b \} *$$

and let "$a \to -\infty$ and $b \to +\infty$". For the time being we shall restrict our considerations to such rectangular sets, but we shall examine the question of more general regions once we have obtained some results for rectangular solids. The following definition is made with these more general regions in mind.

Definition 2.1. Let S be a subset of L^n and let R be a set selected from a certain family of bounded subsets of L^n (for example the sets $R_{a,b}$). We define the density of S in R as the ratio of the number of points in $S \cap R$ to the number of points in R. If we indicate the density of S in R by $D_R(S)$ and use $N(A)$ to indicate the number of points in the set A, this definition becomes

$$D_R(S) = N(S \cap R) / N(R).$$

---

* We write $a \leq x < b$ to indicate the inequalities $a_i \leq x_i < b_i$ where $i = 1, 2, \ldots, n$. We write $a \to -\infty$ to indicate each component of a tends to $-\infty$, and similarly for $b \to +\infty$.

If it is possible to let R "expand to cover L^n" in some manner, we define D(S), the density of S, as the limit of $D_R(S)$ as R expands to cover L^n. This limit may not always exist, but we have recourse to the "upper density" and "lower density" of S by considering the limit superior and limit inferior of $D_R(S)$. Therefore we introduce the following notation:

$$\overline{D}(S) = \overline{\lim_{R \to L^n}} \; D_R(S)$$

$$\underline{D}(S) = \underline{\lim_{R \to L^n}} \; D_R(S)$$

$$D(S) = \lim_{R \to L^n} D_R(S) \qquad \text{(if it exists).}$$

It is easy to verify that the density function D satisfies the following properties of a general measure: If A and B are disjoint sets with densities in L^n, then

$$0 \leq D(A) \leq 1$$

$$D(A') = 1 - D(A) \text{ and}$$

$$D(A \cup B) = D(A) + D(B).$$

The proof of these properties follows immediately from the fact that they are satisfied by the function D_R.

We now prove the following theorem which refers to the <u>rectangular</u> density of periodic sets.

Theorem 2.1. If S is a periodic set with period m, the density of S exists and is given by

$$D(S) = r_m(S) / m^n.$$

Proof: It is clear from the definition of a periodic set that the number of points of S in any n-cube of side m is just $r_m(S)$. Let R be one of the rectangular solids $R_{a,b}$. If we cover R by n-cubes of side m, it is easily seen that the number of points in $S \cap R$ can be estimated by the inequalities

$$r_m(S) \prod_{i=1}^{n} \left[\frac{b_i - a_i}{m}\right] \leq N(S \cap R) \leq r_m(S) \prod_{i=1}^{n} \left(\left[\frac{b_i - a_i}{m}\right] + 1\right) .$$

Dividing by $N(R) = \prod (b_i - a_i)$, we obtain

$$(2.3) \quad r_m(S) \prod_{i=1}^{n} \frac{\left[\frac{b_i - a_i}{m}\right]}{b_i - a_i} \leq D_R(S) \leq r_m(S) \prod_{i=1}^{n} \frac{\left[\frac{b_i - a_i}{m}\right] + 1}{b_i - a_i} .$$

Letting $b \to +\infty$ and $a \to -\infty$, it is clear that

$$\left[\frac{b_i - a_i}{m}\right] / (b_i - a_i) \to \frac{1}{m} .$$

Therefore $D(S) = r_m(S) / m^n$ as stated.

Applying this result to the periodic sets $X_p Q$ and $V_p Q$, we find

(2.4) $$D(X_pQ) = r_p(Q) / p^n$$

(2.5) $$D(V_pQ) = 1 - r_p(Q) / p^n.$$

If $S_1, S_2, \ldots, S_k$ are periodic sets with relatively prime periods, then a simple application of Theorem 1.2 gives

(2.6) $$D(\bigcap_{i=1}^{k} S_i) = \prod_{i=1}^{k} D(S_i).$$

We return now to our discussion of sets of visible points.

<u>Theorem 2.2.</u> Let Q be any subset of L^n and let $\mathcal{P}$ be a collection of distinct primes. Let $V_{\mathcal{P}}$ be the set of points which can see Q modulo all the primes in $\mathcal{P}$, i.e. $V_{\mathcal{P}} = \bigcap_{p \in \mathcal{P}} V_pQ$. Then we have

(2.7) $$\overline{D}(V_{\mathcal{P}}) \leq \prod_{p \in \mathcal{P}} D(V_pQ) = \prod_{p \in \mathcal{P}} (1 - \frac{r_p(Q)}{p^n}) ,$$

and if $\mathcal{P}$ is a <u>finite</u> collection $V_{\mathcal{P}}$ has a density which is given by

(2.8) $$D(V_{\mathcal{P}}) = \prod_{p \in \mathcal{P}} D(V_pQ).$$

Proof: Equation (2.8) is a special case of (2.6). The second part of (2.7) follows from (2.5) and the fact that the infinite product appearing there is either absolutely convergent or else it diverges to zero. We have only to prove the first part of (2.7) in the case where $\mathcal{P}$ is an infinite collection of primes. Let $\mathcal{P}'$ be any <u>finite</u> subset of $\mathcal{P}$. It is clear that $V_{\mathcal{P}} \subseteq V_{\mathcal{P}'}$ and therefore we have for any bounded set $R \subseteq L^n$

$$D_R(V_{\mathcal{P}}) \leq D_R(V_{\mathcal{P}'}).$$

Letting R "expand to L^n", we obtain

$$\overline{D}(V_{\mathcal{P}}) \leq D(V_{\mathcal{P}'}) = \prod_{p \in \mathcal{P}'} D(V_p Q).$$

The first part of (2.7) then follows by allowing "$\mathcal{P}'$ to tend to $\mathcal{P}$".

Probabilistically we can interpret (2.8) as saying that the events "x can see Q modulo p" are independent in finite collections. We do not yet know whether this is true for infinite collections of primes. However we can write by (2.7)

$$(2.9) \qquad \overline{D}(VQ) \leq \prod_{p} D(V_p Q).$$

In the remaining portions of this section we shall restrict ourselves to finite sets Q in order to improve (2.9) as much as possible. We begin with the following definition:

Definition 2.2. Let Q be a finite subset of L^n and let x be a point of L^n. The function $p_Q(x)$ which we abreviate $p(x)$ is defined by

$$p(x) = \begin{cases} 1 & \text{if } x \text{ can see } Q \\ p & \text{if } p \text{ is the smallest prime such that } x \text{ can not see } Q \text{ modulo } p. \end{cases}$$

If p is a prime, we define the set A_p by

$$A_p = A_p(Q) = \{x \mid p(x) = p\} .$$

We can write the set A_p in the form

$$A_p = \bigcap_{q<p} V_q Q \cap X_p Q$$

which is evident from the fact that $p(x) = p$ if and only if x can see Q modulo all primes $q < p$ and x can not see Q modulo p. An elementary computation shows that

$$(2.10) \qquad \Big(\bigcup_{p \leq P} A_p \Big)' = \bigcap_{p \leq P} V_p Q$$

for any prime P.

We may now state the fundamental theorem of this section as follows:

<u>Theorem 2.3.</u> (Density Theorem) If Q is a finite subset of L^n, then VQ has a density which is given by the Euler product

$$(2.11) \qquad D(VQ) = \prod_p D(V_p Q) = \prod_p \Big(1 - \frac{r_p(Q)}{p^n}\Big).$$

Proof: We prove this theorem for rectangular densities and then we display a larger class of regions for which the theorem is true. We begin by representing VQ in terms of the sets A_p

$$VQ = \{x \mid p(x) = 1\} = L^n - \{x \mid p(x) > 1\}$$
$$= L^n - \bigcup_p A_p .$$

Therefore if R is any bounded subset of L^n, we have

$$D_R(VQ) = 1 - D_R(\bigcup_p A_p)$$

$$= 1 - \sum_p D_R(A_p)$$

since the sets A_p are disjoint. Now we assume that $R = R_{a,b}$ is a rectangular set which is large enough to contain all the points of Q. We write $r = \min_{1\le i\le n} (b_i - a_i)$ and without loss of generality we assume $r = b_1 - a_1$. Letting P be a fixed prime smaller than r, we can write

$$D_R(VQ) = 1 - \sum_{p\le P} D_R(A_p) - \sum_{P<p\le r} D_R(A_p) - \sum_{p>r} D_R(A_p)$$

$$(2.12) \qquad = D_R(\bigcap_{p\le P} V_pQ) - \sum_{P<p\le r} D_R(A_p) - D_R(x \mid p(x) > r).^*$$

We estimate the size of the terms $D_R(A_p)$ as follows:

$$D_R(A_p) \le D_R(X_pQ) \le r_p(Q) \prod_{i=1}^{n} \frac{\frac{b_i - a_i}{p} + 1}{b_i - a_i} \qquad \text{(by (2.3))}$$

$$\le \frac{r_p(Q)}{p^n} \prod_{i=1}^{n} \left(1 + \frac{p}{b_i - a_i}\right)$$

$$\le 2^n \frac{r_p(Q)}{p^n} \qquad (\text{since } p \le \min (b_i - a_i)).$$

---

* That is $D_R(\{x \mid p(x) > r\})$.

To estimate $D_R(x \mid p(x) > r)$, we note that if $p(x) = p > r$, then $x \equiv y \ (p)$ for some $y \in Q$. Therefore p must divide $|x_1 - y_1|$. But since $Q \subseteq R$, we have $|x_1 - y_1| \leq b_1 - a_1 = r$, which implies $x_1 - y_1 = 0$. It is easily seen that the set of points that satisfy this condition has a density in R which is at most equal to $N(Q) / r$. Substituting these results in (2.12), we find

$$(2.13) \qquad D_R(VQ) \geq D_R\Big(\bigcap_{p \leq P} V_pQ\Big) - 2^n \sum_{P<p\leq r} \frac{r_p(Q)}{p^n} - \frac{N(Q)}{r} .$$

We may assume that the series $\sum_p \frac{r_p(Q)}{p^n}$ converges, since otherwise the product in (2.11) diverges to zero and the theorem is evident from (2.9). Therefore we may allow R to expand to L^n in (2.13) and obtain

$$\underline{D}(VQ) \geq D\Big(\bigcap_{p\leq P} V_pQ\Big) - 2^n \sum_{p>P} \frac{r_p(Q)}{p^n}$$

$$= \prod_{p\leq P} D(V_pQ) - 2^n \sum_{p>P} \frac{r_p(Q)}{p^n} .$$

Letting P tend to infinity, we find

$$\underline{D}(VQ) \geq \prod_p D(V_pQ)$$

which when coupled with (2.9) proves the theorem for rectangular densities.

It would be futile to attempt to characterize, in a meaningful way, all those families of sets $\{R\}$ for which the Density Theorem is true. We shall content ourselves with the following sufficient condition which includes a large class of sets. Let $S = (S_1, S_2, \ldots)$ be a sequence of subsets of L^n which satisfy $\lim_{i \to \infty} S_i = L^n$. Then the Density Theorem will hold if: (1) S assigns the "proper density" (as given in Theorem 2.1) to periodic sets and (2) each set S_i can be covered by a rectangular set R_i in such a way that $\overline{\lim}_{i \to \infty} N(R_i)/N(S_i)$ is bounded. We omit the details of the proof that these conditions are sufficient for (2.11) to hold. The idea of the proof is to use the sets of S in computing the first term of (2.12) and to use the rectangular sets to estimate the other two terms.

The following examples illustrate the types of sets that satisfy conditions (1) and (2) and those that do not.

Example 1. Let S be any bounded region of E^n which has Jordan content. If x_0 is any point in the interior, we can "magnify" S about x_0 by using the mapping $f_t(x) = x_0 + t(x - x_0)$ defined for $x \in E^n$. It is easy to verify that the sets

$$S_i = \{x \in L^n \mid x = f_i(y) \text{ for some } y \in S\}$$

satisfy properties (1) and (2).

Example 2. Let S_i be the set defined by

$$S_i = \{x \in L^n \mid (x_1^2 + \ldots + x_n^2) \leq i^2, \text{ or } 0 \leq x_1 \leq i^2 \text{ and } x_2 = x_3 \ldots = 0\}.$$

Not only do the sets S_i not satisfy property (2), they do not satisfy property (1) for the periodic set

$$T = \{x \in L^n \mid x_1 \equiv 1 \ (2) \text{ and } x_i \equiv 0 \ (2) \text{ for } i = 2, \ldots, n\}.$$

In the following theorem we show that a finite number of the sets V_pQ can be perturbed in the intersection $\bigcap_p V_pQ$ without affecting the truth of (2.11).

<u>Theorem 2.4.</u> Let Q be a finite subset of L^n and let $S_2, S_3, S_5, \ldots, S_P$ be an arbitrary collection of periodic sets with prime periods $2, 3, 5, \ldots, P$ respectively. Then the set $S = \bigcap_{p \leq P} S_p \cap \bigcap_{p > P} V_pQ$ has a density given by

$$D(S) = \prod_{p \leq P} D(S_p) \cdot \prod_{p > P} D(V_pQ).$$

Proof: The proof of this theorem is essentially the same as that of Theorem 2.3. In fact we can make the same estimates of the error terms in the equation (2.12). The details of the proof are omitted.

Using Theorems 2.3 and 2.4, we can say a great deal about the structure of VQ for finite sets Q. Before proceeding to these remarks, we give the following theorem which characterizes sequences of the form $\{r_p(Q)\}$.

<u>Theorem 2.5.</u> Let $t_2, t_3, \ldots, t_p$ .. be a sequence of integers (indexed by the primes) which satisfies the inequalities $0 < t_p \leq p^n$ for all p. Then a necessary and sufficient condition that there exists a finite set $Q \subseteq L^n$ with the property that $r_p(Q) = t_p$ for all p is that $\lim_{p\to\infty} t_p$ exist and

(2.14) $$\lim_{p\to\infty} t_p = \max_p t_p .$$

Proof: The necessity of the conditions is apparent, for let Q be a finite subset of L^n. Then $r_p(Q) \leq N(Q)$ for all p, while $\lim_{p\to\infty} r_p(Q) = N(Q)$ since for sufficiently large p all the points of Q are distinct modulo p. The sufficiency can be proved by constructing a set which satisfies the requirements. Write $\lim_{p\to\infty} t_p = t$, then we must choose t points which satisfy $r_p(x_1, x_2, \ldots, x_t) = t_p$ for all p. We choose x_1 arbitrarily, then we define the sequence $(x_2, x_3, \ldots, x_t)$ recursively as follows: Having selected $x_1, x_2, \ldots, x_{j-1}$, we choose x_j to satisfy

(1) $x_j \equiv x_1$ (p) for all primes p such that $r_p(x_1, \ldots, x_{j-1}) = t_p$

(2) x_j can see $x_1, x_2, \ldots$, and x_{j-1} for all other primes.

The existence of such a point x_j is guaranteed by Theorem 2.4 in the case $n \geq 2$ since the set specified by conditions (1) and (2) has a positive density. For the case $n = 1$ a separate proof can be given by ordinary congruence methods. The set $Q = (x_1, x_2, \ldots, x_t)$ is seen to satisfy $r_p(Q) = t_p$ since for each p $x_1, x_2, \ldots, x_{t_p}$ are distinct modulo p and all the remaining points of Q (if any) are congruent to x_1 modulo p. This completes the proof.

This theorem will be extended to the case of infinite sets in the next section.

If Q is a finite subset of L^n, we have seen that the density of VQ is given by $\prod_p (1 - \frac{r_p(Q)}{p^n})$. This product will converge absolutely for $n \geq 2$ since $\sum_p \frac{1}{p^n}$ converges and the $r_p(Q)$ are bounded. Therefore, in the case $n \geq 2$, the only way VQ can have zero density is for one or more of the factors $1 - \frac{r_p(Q)}{p^n}$ to vanish. If $D(V_pQ) = 1 - \frac{r_p(Q)}{p^n}$ is zero for some prime p, then V_pQ must be empty in which case $VQ = \bigcap_p X_pQ$ is also empty. Therefore VQ either has a positive density or it is empty. If VQ is not empty, we may prove

(2.15) $$V^2Q = Q \text{ (Q is a set of visible points) and}$$

$$r_p(VQ) = p^n - r_p(Q).$$

From Theorem 1.3 we have $V^2Q \supseteq Q$ which implies $r_p(V^2Q) \geq r_p(Q)$. Therefore we have

$$D(V^3Q) = \prod_p (1 - \frac{r_p(V^2Q)}{p^n}) \leq \prod_p (1 - \frac{r_p(Q)}{p^n}) = D(VQ).$$

But since $V^3Q = VQ$, we must have equality and it follows that $r_p(V^2Q) = r_p(Q)$ for all primes p. This is possible only if $V^2Q = Q$; for if V^2Q were larger than Q,
$\lim_{p\to\infty} r_p(V^2Q) = N(V^2Q) > N(Q) = \lim_{p\to\infty} r_p(Q)$. To prove the second part of (2.15) we note that $r_p(VQ) + r_p(Q) \leq p^n$ since $VQ = \bigcap_p V_pQ$ and $Q = \bigcap_p X_pQ$. From Theorem 1.3 we have $VQ = \bigcap_p X_p(VQ)$.
Applying Theorem 2.2 we see that

$$\bar{D}(VQ) \leq \prod_p \frac{r_p(VQ)}{p^n} .$$

Therefore if $r_p(VQ) < p^n - r_p(Q)$ for some p, we have the contradiction

$$\prod_p (1 - \frac{r_p(Q)}{p^n}) = \bar{D}(VQ) \leq \prod_p \frac{r_p(VQ)}{p^n} < \prod_p (1 - \frac{r_p(Q)}{p^n}).$$

We summarize these results in the following:

<u>Theorem 2.6.</u> Let Q be a finite subset of L^n for $n \geq 2$. Then either VQ has positive density or VQ is empty, and the second possibility can arise only if V_pQ is empty for some prime p. If VQ is non-empty, then Q is a set of visible points ($Q = V(VQ)$) and we have

(2.16) $$X_p(VQ) = V_pQ.$$

Proof: The proof of (2.16) is immediate from (2.15) and the fact that $X_p(VQ) \subseteq V_pQ$.

Equation (2.16) may be interpreted as follows: Let x_o be any point of L^n. Then for a fixed prime p we can always solve the congruence $x \equiv x_o$ (p) subject to the condition that $x \varepsilon Q$ or $x \varepsilon VQ$.

§ 3. The Infinite Case.

In this section we extend some of the results of the last section to the case where Q is an infinite set. We begin with a theorem which strongly indicates the need for some modification of our previous results.

Theorem 3.1. Let $t_2, t_3, \ldots, t_p, \ldots$ be a sequence of integers (indexed by the primes) satisfying the conditions

$$0 < t_p \leq p^n \text{ for all } p .$$

Then a necessary and sufficient condition that there exist a set Q such that $r_p(Q) = t_p$ for all p is that $t = \lim_{p \to \infty} t_p$ exist (we allow $t = +\infty$) and that $t = \sup_p t_p$. In addition, if t is infinite, the set Q may be selected so that VQ is empty.

Proof: The portions of this theorem dealing with a finite set Q and a finite limit t were proved in Theorem 2.5. Therefore we need only consider the case where $t = \infty$ or where Q is an infinite set. If we recall that $r_p(Q)$ is at least as large as the number of points of Q contained in any n-cube of dimension p, it follows that whenever Q is an infinite set

$$\lim_{p \to \infty} r_p(Q) = \infty = \sup_p r_p(Q).$$

All that remains to prove is that if we have a sequence satisfying $\lim t_p = \infty$, then there exists a set Q such that $r_p(Q) = t_p$ for all p and VQ is empty.

We shall construct such a set recursively. Let $b_1, b_2, \ldots$ be the set of integers defined by

$$b_1 < b_2 < b_3 \ldots$$
$$\{b_1, b_2, \ldots\} = \{t_2, t_3, \ldots\} .$$

In other words the b's are just the integers which occur in the sequence $(t_2, t_3, \ldots)$ arranged in ascending order without repetition. Let $(e_1, e_2, \ldots) = L^n$ be a linear ordering of L^n. We define $Q = (x_1, x_2, \ldots)$ as follows: Choose $x_1 = e_1$. Choose x_k for $k \geq 2$ by solving the congruences

(3.1)
$$x_k \equiv x_1 \ (p) \quad \text{for those primes p such that } r_p(x_1, \ldots, x_{k-1}) = t_p$$
$$x_k \equiv e_k \ (p) \quad \text{for those primes p such that } r_p(x_1, \ldots, x_{k-1}) < t_p \leq b_k .$$

To prove that the congruences (3.1) actually serve to define a set, we need only show that there are a finite number of conditions imposed on the selection of each x_k. To prove this, notice that, since $\lim t_p = \infty$, there can be only a finite number of primes such that $t_p \leq b_k$ for any particular k, and that

$r_p(x_1, \ldots, x_{k-1}) \leq k - 1 < b_k$. Therefore a sequence of points may be selected which satisfies (3.1). Writing $Q = (x_1, x_2, \ldots)$, we must show that $r_p(Q) = t_p$ and VQ is empty. The fact that VQ is empty is immediate; for if e is any point of L^n, then $e = e_i$ for some i, and e can not see x_i modulo those primes p for which $t_p = b_i$. To prove that $r_p(Q) = t_p$, we note that if $r_p(x_1, \ldots, x_k) = t_p$ for some k, then $x_i \equiv x_1$ (p) for $i > k$, and no new residues modulo p are introduced by $x_{k+1}, x_{k+2} \ldots$. Therefore $r_p(Q) \leq t_p$. However it is impossible that $r_p(Q) < t_p$ because this would imply that the prime p occurs in all but a finite number of the congruences $x_k \equiv e_k$ (p). But since $(e_1, e_2 \ldots) = L^n$, the set $(x_1, x_2 \ldots)$ would contain all possible residues modulo p which contradicts $r_p(Q) < t_p \leq p^n$.

Theorem 3.1 indicates that there can be no immediate extension of the "Density Theorem" for finite sets to infinite sets. For if Q is any infinite subset of L^n with the properties listed in Theorem 3.1, then we clearly can not prove

$$D(VQ) = \prod_p \left(1 - \frac{r_p(Q)}{p^n}\right)$$

except in the trivial case where the product is zero. However, we can easily improve the estimate (2.9) by writing

$$(3.2) \qquad \bar{D}(VQ) = \bar{D}(V(V^2Q)) \leq \prod_p D(V_p(V^2Q)) = \prod_p \left(1 - \frac{r_p(V^2Q)}{p^n}\right).$$

This is a better result than the one stated in (2.9) since $V^2Q \geq Q$ which implies $D(V_p(V^2Q)) \leq D(V_pQ)$. It should be noted that Theorem 3.1 in no way excludes the possibility that <u>equality</u> holds in (3.2). For the sets Q discussed in the theorem we have $V^2Q = L^n$, and the equation

$$(3.3) \qquad D(VQ) = \prod_p D(V_p(V^2Q))$$

holds trivially since both sides are zero.

We can refine (3.2) further if we write $VQ = \bigcap_p X_p(VQ)$ and use a slight modification of the proof of Theorem 2.2 to show that

$$(3.4) \qquad \overline{D}(VQ) \leq \prod_p D(X_p(VQ)) = \prod_p \frac{r_p(VQ)}{p^n} .$$

This result is stronger than (3.2) since we have trivially $r_p(VQ) + r_p(V^2Q) \leq p^n$.

One might reasonably ask, "Why even mention (3.2) when the stronger version given by (3.4) exists?" The reason for doing so is that if we can prove that equality holds in (3.2) for some class of sets, then equality must also hold in (3.4) for this same class. And if the infinite products involved in (3.2) and (3.4) are positive, it follows that

$$(3.5) \qquad r_p(VQ) + r_p(V^2Q) = p^n$$

We shall return to these matters after we obtain some more information. However we mention in passing a nice interpretation of (3.5): Equation (3.5) holds for the prime p if and only if the congruence $x \equiv a \ (p)$ has a solution, for any $a \in L^n$, which also satisfies $x \in VQ$ or $x \in V^2Q$. When (3.4) does not hold, these last conditions can not be met for some residues a modulo p.

We now extend the definition of the function p(x) and the sets A_p to enable us to handle the representations indicated by (3.2) and (3.4).

Definition 3.1. Let Q be a subset of L^n and let p be a fixed prime. We define the sets A_p, B_p and C_p as follows:

$$A_p = A_p(Q) = \bigcap_{q<p} V_q Q \ \cap \ X_p Q$$

$$B_p = \bigcap_{q<p} V_q(V^2Q) \ \cap \ X_p(V^2Q)$$

$$C_p = \bigcap_{q<p} X_q(VQ) \ \cap \ V_p(VQ)$$

where the intersections are over all primes $q < p$ and are defined to be L^n if $p = 2$. We define the function $p_A(x)$ as follows:

$$p_A(x) = \begin{cases} p & \text{if } x \in A_p \\ 1 & \text{if } x \notin A_p \text{ for all } p. \end{cases}$$

The functions $p_B(x)$ and $p_C(x)$ are similarly defined in terms of

B_p and C_p.

It should be noted that the function $p_A(x)$ is well defined since the sets $A_2, A_3, \ldots, A_p \ldots$ are clearly disjoint, and similarly p_B and p_C are well defined.

In Theorem 3.2 we shall demonstrate how the sets A_p, B_p and C_p are used to represent VQ, but first we compare the sets with one another. It is evident from their definitions that the sets A_p and B_p are constructed in essentially the same manner; in fact $B_p = A_p(V^2Q)$. The construction of the sets C_p is essentially different since it makes reference to the set VQ rather than Q or V^2Q. However, if (3.5) holds, we have $C_p = B_p$ for all primes p; and in the case of a finite set Q with a non-empty set of visible points all three collections become identical. In fact, let Q be a finite subset of L^n and assume VQ is non-empty. Then we have $V^2Q = Q$ which implies $A_p = B_p$, and from Theorem 2.6 we have $X_p(VQ) = V_pQ$ which implies $C_p = A_p$. In the case where Q is finite and VQ is empty ($VQ = \emptyset$) we easily verify that

(1) $\quad A_p = \emptyset$ for all sufficiently large primes p

(2) $\quad B_2 = C_2 = L^n$

$\quad B_p = C_p = \emptyset \quad$ for $p > 2$.

If we merely assume that $VQ = \emptyset$ then (2) obviously remains valid; however there is no guarantee that (1) holds as is illustrated by the following:

<u>Example</u>. Let $Q = (x_2, x_3, \ldots, x_p, \ldots)$ be the infinite set (indexed by the primes) defined by

$$(1) \qquad x_2 = e_2$$

$$(2) \qquad \begin{cases} x_p \equiv e_2 \ (q) & \text{for all primes } q < p \\ x_p \equiv e_p \ (p) \end{cases}$$

where x_p is any root of the congruences (2) and $(e_2, e_3, \ldots, e_p, \ldots) = L^n$ is a linear ordering of L^n (also indexed by the primes).

It is evident that VQ is empty; for if e_p is any point of L^n then e_p can not see x_p modulo p. To prove that $A_p \neq \emptyset$, let p be any prime. We compute

$$r_p(X_pQ) = r_p(Q) \leq \pi(p)$$

where $\pi(p)$ is the number of primes less that or equal to p. But since $\pi(p)$ clearly satisfies $0 < \pi(p) < p^n$, neither X_pQ nor V_pQ can be empty. It follows that A_p, being a finite intersection of non-empty, independent, periodic sets, is itself non-empty.

The set Q constructed in this example can be used as another example for which the Density Theorem does not hold. We have $D(VQ) = 0$ and

$$\prod_p \left(1 - \frac{r_p(Q)}{p^n}\right) \geq \prod_p \left(1 - \frac{\pi(p)}{p^n}\right).$$

This last product is clearly not zero for $n \geq 3$. However for $n = 2$ the factors in this product are asymptotic to those in the product

$$\prod_p \left(1 - \frac{1}{p \log p}\right)$$

which diverges to zero.

Although our discussion has shown that there need be no intimate relation between A_p, B_p and C_p, the following theorem shows how A_p, B_p and C_p may be used to represent VQ. It also gives a relation between the functions p_A, p_B and p_C which is valid in all cases.

Theorem 3.2. Let Q be any subset of L^n. Then the sets A_p, B_p and C_p are periodic and have densities given by

$$D(A_p) = \frac{r_p(Q)}{p^n} \prod_{q<p} \left(1 - \frac{r_q(Q)}{q^n}\right)$$

$$D(B_p) = \frac{r_p(V^2Q)}{p^n} \prod_{q<p} \left(1 - \frac{r_q(V^2Q)}{q^n}\right)$$

$$D(C_p) = \left(1 - \frac{r_p(VQ)}{p^n}\right) \prod_{q<p} \frac{r_q(VQ)}{q^n}$$

Furthermore we may represent VQ in terms of these sets as follows:

$$VQ = L^n - \bigcup_p A_p = L^n - \bigcup_p B_p = L^n - \bigcup_p C_p .$$

The functions p_A, p_B and p_C are related by

(3.6) $$p_A(x) \geq p_B(x) \geq p_C(x)$$

for all $x \in L^n$.

Proof: The fact that A_p, B_p and C_p are periodic sets with densities as indicated follows immediately from their definitions and equation (2.6). To prove the second assertion, we write

$$(\bigcup_p A_p)' = \bigcap_p A_p' = \bigcap_p V_pQ = VQ$$

$$(\bigcup_p B_p)' = V(V^2Q) = VQ \text{ and}$$

$$(\bigcup_p C_p)' = \bigcap_p C_p' = \bigcap_p X_p(VQ) = VQ.$$

It follows from these equations that $p_A(x) = 1$ if and only if $x \in VQ$, and similarly for $p_B(x) = 1$ and $p_C(x) = 1$. We now show that $p_B(x) = p \neq 1$ implies that $p_A(x) \geq p$; the proof relating p_C and p_B is similar and will not be given. Let $x \in L^n$ and assume $p_B(x) = p$ for some prime p. Then we have

$$x \in B_p \subseteq \bigcap_{q<p} V_q(V^2Q) \subseteq \bigcap_{q<p} V_qQ.$$

This implies that $x \notin A_q$ for all $q < p$. Therefore, since $p_A(x) \neq 1$ (because $x \notin VQ$), we must have $p_A(x) \geq p_B(x)$.

As we shall see in Theorem 3.3 the inequalities (3.6) confirm our observations on the relative strengths of (2.9), (3.2) and (3.4). This theorem is the first extension of the Density Theorem to infinite sets Q. Before stating the theorem, we insert the following definition.

Definition 3.2. We define the set A(K) by

$$A(K) = \{ x \in L^n \mid p_A(x) \geq K |x| > 0 \}$$

where x is the "sup. norm" of x defined by

$$|x| = |(x_1, \ldots, x_n)| = \max (|x_1|, \ldots, |x_n|).$$

We make analogous definitions for the sets B(K) and C(K) in terms of p_B and p_C respectively.

It should be noted that by (3.6) we have

$$A(K) \supseteq B(K) \supseteq C(K). \tag{3.7}$$

Theorem 3.3. Let Q be an infinite subset of L^n. Then a necessary and sufficient condition that VQ have a density* given by

$$D(VQ) = \prod_p D(V_p Q) \tag{3.8}$$

---

* We shall prove the sufficiency only for rectangular regions with uniform dimensions (n-cubes). The proof can be easily modified to include a rectangular solid expanding to L^n in such a manner that the ratio between the longest side and the shortest side remains bounded.

is that

(3.9) $$\lim_{K\to\infty} \bar{D}(A(K)) = 0.$$

Similarly

(3.10) $$D(VQ) = \prod_p D(V_p(V^2Q)) \quad \text{if and only if}$$

(3.11) $$\lim_{K\to\infty} \bar{D}(B(K)) = 0, \quad \text{and}$$

(3.12) $$D(VQ) = \prod_p D(X_p(VQ)) \quad \text{if and only if}$$

(3.13) $$\lim_{K\to\infty} \bar{D}(C(K)) = 0.$$

Proof: We shall prove only the second of these statements. The proofs for the other two are essentially a matter of replacing "B" with "A" or "C" throughout the proof which is given here.

We first prove that (3.10) implies (3.11). We have

$$\begin{aligned} B(K) &= \{x \mid p_B(x) \geq K|x| > 0\} \\ &\subseteq \{x \mid p_B(x) \geq K\} \\ &= \bigcup_{p\geq K} B_p = (VQ \cup \bigcup_{p<K} B_p)' \quad . \end{aligned}$$

Therefore if R is any rectangular subset*, we have

---

* Or any subset of L^n which is being used to compute the density of VQ.

$$D_R(B(K)) \leq 1 - D_R(VQ) - \sum_{p<K} D_R(B_p).$$

Letting R expand to cover L^n, we find by a simple computation that

$$\overline{D}(B(K)) \leq 1 - \underline{D}(VQ) - \sum_{p<K} D(B_p)$$

(3.14) $$= \prod_{p<K} D(V_p(V^2Q)) - \underline{D}(VQ),$$

from which (3.11) follows by assuming (3.10) and allowing K to tend to infinity.

To prove that (3.11) implies (3.10), we assume that the rectangular sets R used to compute D(VQ) are equilateral. We write $R = R_{a,b}$ and we set $d = b_1 - a_1$ (the length of a side of R). Using Theorem 3.2 and the fact that the B_p's are disjoint, we may write

$$D_R(VQ) = 1 - \sum_p D_R(B_p).$$

Let P be any prime, let K be any positive number, and choose d so that $dK > P$. Then by a computation similar to that used in the proof of Theorem 2.3, we can write

(3.15) $$D_R(VQ) = D_R\Big(\bigcap_{p \leq P} V_p(V^2Q)\Big) - \sum_{P<p<Kd} D_R(B_p)$$

$$- D_R(x \mid p_B(x) \geq Kd).$$

To estimate $D_R(B_p)$, we write

$$D_R(B_p) \leq D_R(X_p(V^2Q)).$$

Then we cover R by n-cubes of dimension p and use the same argument used in proving Theorem 2.3 to show that

$$D_R(B\ ) \leq (2K)^n \frac{r_p(V^2Q)}{p^n} .$$

To estimate the last term in (3.15), we assume that R has been chosen large enough to contain the origin. We have then

$$D_R(x \mid p_B(x) \geq Kd) \leq D_R(B(K))$$

since $Kd \geq K|x|$ for all $x \in R$. Combining these results in (3.15), we conclude that

$$(3.16) \quad D_R(VQ) \geq D_R(\bigcap_{p \leq P} V_p(V^2Q)) - (2K)^n \sum_{P<p<Kd} \frac{r_p(V^2Q)}{p^n}$$
$$- D_R(B(K)).$$

We may assume that $\sum r_p(V^2Q) / p^n$ converges since otherwise there is nothing to prove. If we let R expand to cover L^n in (3.16), we obtain

$$\underline{D}(VQ) \geq \prod_{p \leq P} D(V_p(V^2Q)) - (2K)^n \sum_{p > P} \frac{r_p(V^2Q)}{p^n} - \overline{D}(B(K)).$$

If we allow P to tend to infinity, this becomes

$$(3.17) \qquad \underline{D}(VQ) \geq \prod_p D(V_p(V^2Q)) - \overline{D}(B(K)).$$

Equation (3.10) follows by letting K tend to infinity and using (3.11).

We have the following corollary (to the proof of the theorem) which again refers to the "equilateral" density.

Corollary. Let Q be an infinite subset of L^n. Then we can make the following estimates on the size of VQ:

$$\prod_p \frac{r_p(VQ)}{p^n} - \overline{C} \leq \underline{D}(VQ) \leq \overline{D}(VQ) \leq \prod_p \frac{r_p(VQ)}{p^n} - \underline{C} ,$$

where

$$(3.18) \qquad \begin{aligned} \overline{C} &= \lim_{K\to\infty} \overline{D}(x \mid p_C(x) \geq K|x|) \quad \text{and} \\ \underline{C} &= \lim_{K\to\infty} \underline{D}(x \mid p_C(x) \geq K|x|) . \end{aligned}$$

The proof of this result follows from the analogues of (3.14) and (3.17) for the case of C(K) rather than B(K). The limits defining $\overline{C}$ and $\underline{C}$ exist, of course, since the functions of K involved are both monotonically decreasing and bounded below by zero.

The following corollary is evident from (3.18).

Corollary. Let Q be an infinite subset of L^n. Then if $\underline{C} = \overline{C} = C$, VQ has a density given by

$$D(VQ) = \prod_p \frac{r_p(VQ)}{p^n} \cdot C .$$

In particular, if the sets C(K) have densities for sufficiently large K, then

$$D(VQ) = \prod_p \frac{r_p(VQ)}{p^n} \cdot \lim_{K\to\infty} D(C(K)) .$$

Both of the above corollaries may also be stated in terms of the sets A(K) and B(K).

We now return to our discussion of the relative merits of our three representations of VQ, namely

$$VQ = L^n - \bigcup_p A_p = L^n - \bigcup_p B_p = L^n - \bigcup_p C_p \quad .$$

Each of these expressions leads to a different product for computing the density of VQ ((3.8), (3.10) or (3.12)). We have discussed the relations between these products, but it is interesting to see what they become in terms of the sets A(K), B(K) and C(K). From (3.7) we have

$$\lim_{K\to\infty} \overline{D}(A(K)) \geq \lim_{K\to\infty} \overline{D}(B(K)) \geq \lim_{K\to\infty} \overline{D}(C(K)) .$$

This relation shows us again that (3.8) implies (3.10) which in turn implies (3.12). The sets given in Theorem 3.1 may be taken for examples in which (3.8) does not hold, but for which (3.10) and (3.12) are valid. As I stated earlier, I have no examples in which (3.12) holds and (3.10) does not. In fact, I have no examples for which (3.10) does not hold.

In order to prove that (3.10) or (3.12) holds in general we must analyze the sets $B(K)$ or $C(K)$ in greater detail. The crux of the whole problem of the density of VQ for infinite sets Q seems to be in a deeper understanding of these sets or, equally, in a deeper analysis of the functions p_B and p_C. The sets themselves are very difficult to handle directly. The functions are only defined by implicit relations on the sets $X_p(V^2Q)$ and $X_p(VQ)$ which are not so easy to work with. As an alternative approach we might try to prove the relation

$$r_p(VQ) + r_p(V^2Q) = p^n$$

which, as mentioned earlier, would at least show that (3.10) and (3.12) are identical. However this problem appears to be more complicated than a direct attack on (3.10) or (3.12).

It should not be thought from the above discussion that Theorem 3.3 gives us no direct information on the validity of (3.8), (3.10) or (3.12). As a matter of fact, we can use the theorem to show, for a large class of infinite sets Q, that VQ does have a density which is given by (3.8). In order to simplify the notation, we write

$p(x) = p_A(x)$ and

$$P(x) = \begin{cases} p(x)/|x| & \text{if } x \neq (0,0,\ldots,0) \\ 0 & \text{if } x = (0,0,\ldots,0) \end{cases}.$$

To show that (3.8) holds, we must show that

$$\lim_{K\to\infty} \overline{D}(x \mid P(x) \geq K) = 0.$$

We first consider a simple example in L^3. Let Q be an infinite subset of L^3 which lies entirely in the (x_1,x_2)-plane. If $x \in L^3$ is such that $p(x) = p$ for some prime p, then

$$x \in A_p \subseteq X_p Q.$$

Therefore we must have

$$x \equiv x' \ (p) \text{ for some } x' \in Q.$$

But looking at the last components of x and x' we have

$$p \mid x_3 - x_3' = x_3 .$$

Thus if $x_3 \neq 0$ we have

$$p(x) = p \leq |x_3| \leq |x|$$

which also holds if $p(x) = 1$ and $x_3 \neq 0$. Therefore we have $P(x) \leq 1$ for all points x except possibly some in the (x_1,x_2)-plane. This last set obviously has zero density and therefore

$$D(A(K)) = 0 \text{ for } K > 1.$$

Thus we have proven (3.8) for any set Q which lies entirely in the (x_1, x_2) plane. It is evident that this result may be extended to any set lying entirely in a subset of L^n of the form

$$x_i = \text{constant} \qquad \text{for some } i = 1, \dots, n.$$

If Q is the finite union of such sets, it is equally clear that the same argument will be valid. We may, in fact, prove the following theorem.

<u>Theorem 3.4.</u> Let $a = (a_1, \dots, a_n)$ be a vector with rational components and let α and β be real numbers. We say that a set Q_i is subdimensional (with respect to L^n) if for some a, α and β we can write

$$Q_i \subseteq \left\{ x \in L^n \;\middle|\; \alpha \leq \sum_{j=1}^{n} a_j x_j \leq \beta \right\} .$$

Let Q be a subset of L^n which can be represented as a finite union of subdimensional sets, say

$$Q = \bigcup_i Q_i .$$

Then Q has a density which is given by

$$D(VQ) = \prod_p D(V_p Q) = \prod_p \left(1 - \frac{r_p(Q)}{p^n}\right).$$

Proof: Let $x \varepsilon L^n$ and let $p(x) = p$ (we allow $p = 1$ in this case). Then either $p(x) = 1$ or $x \varepsilon X_p Q$ and in either case we have

(3.19) $$x \equiv x' \ (p) \text{ for some } x' \varepsilon Q.$$

By the hypothesis of the theorem, x' must satisfy a releation of the form

$$\alpha \leq a_1 x_1' + \ldots + a_n x_n' \leq \beta \quad \text{for some } a, \alpha \text{ and } \beta.$$

We may assume without loss of generality that $a_1, a_2, \ldots, a_n$, α and β are <u>integers</u>. Then by (3.19) we have

$$p \mid a_1(x_1 - x_1') + \ldots + a_n(x_n - x_n') = D.$$

Therefore either $D = 0$, which can happen only for a set of zero density, or

$$p \leq |D| \leq |a_1||x_1| + \ldots + |a_n||x_n| + |a_1 x_1 + \ldots + a_n x_n|$$
$$\leq (|a_1| + \ldots + |a_n|)\,|x| + \max(|\alpha|, |\beta|).$$

Thus, except for a set of zero density, we have

$$P(x) = p/|x| \leq |a_1| + \ldots + |a_n| + \max(|\alpha|, |\beta|).$$

Since there are only a finite number of possible values for

$a_1, \ldots, a_n, \alpha$ and β, $P(x)$ is a bounded function of x except possibly on a set of density zero, and the result follows by Theorem 3.3.

This theorem demonstrates the possibility of obtaining definite results from Theorem 3.3. The following theorem, though not quite as explicit, gives an interesting condition for (3.8), (3.10), or (3.12) to hold.

Theorem 3.5. Let Q be an infinite subset of L^n, and define the function P(x) by

$$P(x) = \begin{cases} p(x)/|x| & \text{if } |x| \neq 0 \\ 0 & \text{if } |x| = 0 \end{cases}$$

where p(x) is either $p_A(x)$, $p_B(x)$ or $p_C(x)$. Then if

$$\text{(3.20)} \qquad \overline{\lim_{R \to L^n}} \frac{1}{N(R)} \sum_{x \in R} P(x)$$

is finite, VQ has a density given by equation (3.8), (3.10), or (3.12) respectively.

Proof: The theorem states that if P(x) is "averagable" (more properly has an "upper average") then

$$\lim_{K \to \infty} \overline{D}(x \mid P(x) \geq K) = 0.$$

We assume that this last condition does not hold and show that (3.20) is infinite. Assume that

$$\lim_{K\to\infty} \overline{D}(x \mid P(x) \geq K) = g > 0.$$

Then for a fixed K there exist "arbitrarily large" R such that

$$D_R(x \mid P(x) \geq K) \geq g/2.$$

For such an R we have

$$\frac{1}{N(R)} \sum_{x \in R} P(x) \geq KD_R(x \mid P(x) \geq K) \geq Kg/2.$$

Therefore the expression in (3.20) is at least as large as Kg/2, and since we can take K as large as we please (3.20) is infinite.

We close this section with an elementary but interesting result which shows that "at least half" of the sets of visible points have zero density.

Theorem 3.6. Let Q and VQ be conjugate pairs of sets of visible points ($V^2Q = Q$). Then at least one of them must have zero density.

Proof: We may assume that one of the sets has a positive upper density, since otherwise there is nothing to prove. By symmetry we may take $\overline{D}(VQ) > 0$. This implies

$$\prod_p \left(1 - \frac{r_p(Q)}{p^n}\right) > 0.$$

Therefore $r_p(Q)/p^n$ tends to zero as p increases without bound.

But we clearly have

$$Q \subseteq X_p Q \qquad \text{for all } p.$$

It follows that

$$\overline{D}(Q) \leqslant D(X_p Q) = \frac{r_p(Q)}{p^n} \quad .$$

Letting p tend to infinity, we obtain

$$\overline{D}(Q) \leqslant 0.$$

This completes the proof of the theorem.

§ 4. The Average Values of a Class of Functions in L^n.

In this section we prove an identity which contains the Density Theorem for finite sets as a special case. As will be seen, the techniques we use have no obvious extension to infinite sets Q.

We begin with the definition of the average of a function in L^n.

Definition 4.1. Let f be a real valued function defined on L^n. The average value of f on L^n is defined by the following limit (if it exists)

$$\lim_{R \to L^n} \frac{1}{N(R)} \sum_{x \in R} f(x)$$

where $R \to L^n$ is defined as in Definition 2.1.

For convenience we restrict ourselves to uniform rectangular sets $R = R_{a,b}$, and we write $r = b_i - a_i$ for the common dimension of R.

We now define two functions which will play a basic role in our subsequent analysis.

Definition 4.2. Let Q be a finite subset of L^n and let x be a point of L^n. We define the functions d(x) and F(x) as follows:

$$d(x) = \begin{cases} \gcd(x_1, x_2, \ldots, x_n) & \text{if } x \neq (0,0,\ldots,0) \\ 0 & \text{if } x = (0,0,\ldots,0) \end{cases}$$

$$F(x) = \operatorname{lcm}_{y \in Q} d(x-y).$$

It is easy to see how we can relate the functions $d(x)$ and $F(x)$ to visibility problems. For example, two points x and y are mutually visible if and only if $d(x-y) = 1$. And the point x can see Q if and only if $F(x) = 1$. In fact, it is proved in [2] that the density of VQ is the average value of the function $\sum_{d|F(x)} \mu(d)$ where μ is the Möbius function.

We now state the fundamental result of this section as follows:

<u>Theorem 4.1.</u> Let Q be a finite set consisting of k points of L^n, $n \geq 2$. Let $g(m)$ and $G(m)$ be multiplicative arithmetic functions which are related by the equation

$$G(m) = \sum_{d|m} g(d),$$

and define $G(0) = 0$. Assume that $g(m)$ satisfies a relation of the form

$$|g(m)| \leq Am^a \tag{4.1}$$

for some constants A and a. Then, if the inequality*

$$n > 1 + k^2 a \tag{4.2}$$

---

* Note that if $a \leq 0$, this condition is automatically satisfied.

holds, the function $G(F(x))$ has an average value in L^n which is given by the absolutely convergent Euler product

$$(4.3) \qquad \prod_p \left(1 + \sum_{i=1}^{\infty} \frac{r_{p^i}(Q)g(p^i)}{p^{ni}}\right).$$

Proof: The fact that the product converges absolutely follows from the inequalities (4.1), (4.2) and $r_{p^i}(Q) \leq k$. We begin our proof of the theorem by expressing the sum for computing the average of $G(F(x))$ in terms of the function $g(d)$. We then break this sum into three pieces which we call S_1, S_2 and S_3. We handle each of these pieces separately.

We may neglect those x for which $F(x) = 0$ and then we have

$$\frac{1}{N(R)} \sum_{x \in R} G(F(x)) = \frac{1}{N(R)} \sum_{x \in R} \sum_{d \mid F(x)} g(d)$$

$$= \frac{1}{N(R)} \sum_{x \in R} \sum_{\substack{d \mid F(x) \\ d \leq D}} g(d) + \frac{1}{N(R)} \sum_{x \in R} \sum_{\substack{d \mid F(x) \\ D < d < r}} g(d)$$

$$+ \sum_{x \in R} \sum_{\substack{d \mid F(x) \\ d \geq r}} g(d)$$

$$= S_1 + S_2 + S_3 ,$$

say, where D is a positive constant smaller than r.

We can rearrange the sum S_1 as follows:

$$S_1 = \sum_{d \leq D} g(d) \frac{1}{N(R)} \sum_{\substack{x \in R \\ d | F(x)}} 1 = \sum_{d \leq D} g(d)\, D_R(x \mid d|F(x)). \tag{4.4}$$

Now we prove that the sets $A_d = \{x \mid d|F(x)\}$ are periodic and we compute their densities. First assume that d is a power of a prime. Then the condition $d|F(x)$ is equivalent to the condition that d divides $d(x-y)$ for some point $y \in Q$. We can write this as follows:

$$A_d = \{x \mid x \equiv y \ (d) \text{ for some } y \in Q\}.$$

Therefore A_d is a periodic set and we have

$$D(A_d) = r_d(Q)/d^n .$$

But if d is a composite number, the condition $d|F(x)$ is equivalent to the condition that each prime power appearing in the prime power factorization of d should divide $F(x)$. Therefore we can write A_d as the intersection of independent periodic sets, and a simple application of equation (2.6) shows that the density of A_d, $D(A_d)$ is a multiplicative function of d. Returning to (4.4), we can write

$$\lim_{R \to L^n} S_1 = \sum_{d \leq D} g(d)\, D(A_d).$$

If we allow D to tend to infinity, we obtain

$$\lim_{D\to\infty} \lim_{R\to L^n} S_1 = \sum_d g(d)\, D(A_d).$$

This series is absolutely convergent and, in fact, has the Euler product given by (4.3). Therefore to complete the proof, it suffices to show that

$$(4.5) \qquad \lim_{D\to\infty} \overline{\lim_{R\to L^n}} |S_2| = 0 \quad \text{and}$$

$$(4.6) \qquad \lim_{R\to L^n} |S_3| = 0.$$

First we turn to the sum S_2. We have, by analogy with (4.4),

$$S_2 = \sum_{D<d<r} g(d)\, D_R(A_d).$$

We can estimate the size of the factors $D_R(A_d)$ as we did in the proof of the Density Theorem for finite sets. We find that

$$0 \leq D_R(A_d) \leq 2^n D(A_d).$$

Therefore

$$|S_2| \leq 2^n \sum_{D<d<r} g(d)\, D(A_d),$$

from which (4.5) is evident.

To prove (4.6), notice that if R is large enough to enclose the origin as well as all the points of Q then $d(x-y) \leq r$ for all points

$x \in R$ and $y \in Q$. Therefore, under these conditions, we have

$$F(x) = \operatorname*{lcm}_{y \in Q} d(x-y) < r^k .$$

We can then write

$$|S_3| \leqslant \frac{1}{N(R)} \sum_{x \in R} \sum_{\substack{d|F(x) \\ r \leqslant d < r^k}} g(d)$$

$$\leqslant \frac{1}{N(R)} \sum_{\substack{x \quad R \\ r \leqslant F(x) < r^k}} \sum_{d|F(x)} A r^{ak}$$

It is well known (see [1]) that the divisor function $d(m) = \sum_{t|m} 1$ is of smaller order than m^{ϵ} for any positive power ϵ. Therefore we can write

$$(4.7) \qquad |S_3| \leqslant A' r^{ak+\epsilon k} \frac{1}{N(R)} \sum_{\substack{x \in R \\ F(x) \geq r}} 1$$

$$= A' r^{ak+\epsilon k} D_R(x \,|\, F(x) \geq r),$$

where A' is a positive constant depending on ϵ and A. To estimate the density in R of the set $\{x \mid F(x) \geq r\}$ we observe that

$$\{x \mid F(x) \geq r\} \subseteq \{x \mid d(x-y) \geq r^{1/k} \text{ for some } y \varepsilon Q\}$$

$$\subseteq \bigcup_{y \varepsilon Q} \bigcup_{d \geq r^{1/k}} \{x \mid d(x-y) = d\}$$

$$\bigcup_{y \varepsilon Q} \bigcup_{d \geq r^{1/k}} \{x \mid x \equiv y \ (d)\} .$$

Therefore

$$D_R(x \mid F(x) \geq r) \leq \sum_{y \varepsilon Q} \sum_{d \geq r^{1/k}} D_R(x \mid x \equiv y \ (d)) .$$

But since these last sets are periodic, we may use equation 2.3 to write

$$D_R(x \mid x \equiv y \ (d)) \leq 2^n D(x \mid x \equiv y \ (d))$$

$$\leq 2^n / d^n .$$

Returning to (4.7), we have

$$|S_3| \leq A' r^{ak+\epsilon k} \sum_{y \varepsilon Q} \sum_{d \geq r^{1/k}} 2^n / d^n$$

$$\leq 2^n k A' r^{ak+\epsilon k} \int_{r^{1/k}}^{\infty} \frac{dt}{t^n}$$

$$\leq \frac{2^n k A'}{n-1} r^{ak+\epsilon k - \frac{n-1}{k}} \tag{4.8}$$

But by condition (4.2) it follows that $ak - \frac{n-1}{k} < 0$, and if we take ϵ sufficiently small in (4.8), we can guarantee that the coefficient of r is negative. Therefore, letting r tend to infinity, equation (4.6) is evident. This completes the proof of the theorem.

In the proof of this theorem we only used the condition that $n > 1 + k^2 a$ in showing that the product (4.3) was convergent and in estimating S_3. We could have proved the theorem under the alternative assumptions that $n > k(a+1)$ and the product (4.3) is absolutely convergent. Neither of the conditions $n > 1 + k^2 a$ or $n > k(a+1)$ is "best possible"; however we have proved the following:

__Corollary.__ Let Q be a finite subset of $L^n, n \geq 2$. Then VQ has a density which is given by

$$(4.9) \qquad D(VQ) = \prod_p \left(1 - \frac{r_p(Q)}{p^n}\right).$$

Proof: Take $g(m) = \mu(m)$.

As we mentioned earlier, Rearick [2] has proved this result for a set Q consisting of __two__ points of L^n or of k mutually visible points of L^n. It is interesting to see how the Density Theorem may be stated in these cases. First we let Q be a subset of L^n which consists of k mutually visible points. Then each point of Q leaves a distinct least positive residue modulo p for any fixed prime p. Therefore $r_p(Q) = k$ for all primes p* and equation (4.9) becomes

---

* We must have $k \leq 2^n$, since there are at most 2^n points of L^n which are mutually visible in pairs.

(4.10) $$D(VQ) = \prod_p \left(1 - \frac{k}{p^n}\right).$$

In the case where Q consists of two points $x, y \in L^n$, a simple computation shows that

$$r_p(Q) = \begin{cases} 2 & \text{if } p \nmid d(x-y), \\ 1 & \text{if } p \mid d(x-y). \end{cases}$$

Therefore, in this case, we may express the density of VQ as follows:

$$D(VQ) = \prod_{p \mid d(x-y)} \left(1 - \frac{1}{p^n}\right) \prod_{p \nmid d(x-y)} \left(1 - \frac{2}{p^n}\right)$$

(4.11) $$= C \prod_{p \mid d(x-y)} \frac{p^n - 1}{p^n - 2}$$

where C is the constant given by the infinite product

$$C = \prod_p \left(1 - \frac{2}{p^n}\right).$$

Equations (4.10) and (4.11) are the expressions of the Density Theorem which were obtained by Rearick.

REFERENCES

1 G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Third Edition, Oxford (1954).

2 D. F. Rearick, Some Visibility Problems in Point Lattices, Ph.D. Thesis, California Institute of Technology (1960).

3 J. Christopher, Am. Math. Monthly, 63, No. 6, 399-401 (1956).