ON A QUADRATIC DIOPHANTINE INEQUALITY

FRED SUPNICK

1. Introduction. Let $C$ be an $n$-cube and $S$ the $n$-sphere circumscribed about $C$. Keeping $C$ fixed let $S$ be moved so that its center falls at some point $P$ inside or on $C$. We pose the problem: How can vertices of $C$ falling inside or on $S_P$ (the subscript denotes the center) be selected?

Analytically expressed, let $C$ be the unit $n$-cube the coordinates of whose vertices are zeros or ones (on a Cartesian coordinate system in $E_n$). Let $P$ be the point $(x_1, \cdots, x_n)$ with $0 \leq x_i \leq 1$ ($i = 1, \cdots, n$). $S_P$ is of diameter $n^{1/2}$. We seek lattice points $(y_1, \cdots, y_n)$ $y_i = 0$ or $1$ ($i = 1, \cdots, n$) satisfying

\[ \sum_{i=1}^{n} (x_i - y_i)^2 \leq n/4. \]  

Thus, trivially, one point $(y_1, \cdots, y_n)$ may always be obtained if we let $y_i = 0$ if $x_i < 1/2$ and $y_i = 1$ if $x_i > 1/2$.

Of course, one obvious method would be to substitute (the coordinates of) the vertices of $C$ into (1.1) and to select those which satisfy it; however, except for small $n$ this is a prohibitive operation (even with mechanical aid). The problem therefore is one of minimizing the number of operations in obtaining solutions of the desired type.

In this paper we obtain a process for immediately associating with any $(x_1, \cdots, x_n)$ ($0 \leq x_i \leq 1$, $i = 1, \cdots, n$, $n \geq 4$) a class of lattice points $(y_1, \cdots, y_n)$ $y_i = 0$ or $1$ ($i = 1, \cdots, n$) satisfying (1.1).

We note that a lemma to a theorem of D. Warncke and the author\(^1\) establishes the following class of solutions for the case $n = 4$: Let $(x_{i_1}, \cdots, x_{i_4})$ be a rearrangement $G$ of $(x_1, \cdots, x_4)$ for which

\[ |x_{i_1} - 1/2| \leq |x_{i_2} - 1/2| \leq |x_{i_3} - 1/2| \leq |x_{i_4} - 1/2|. \]

Let $y_{i_1}' = 0$ and $y_{i_1}'' = 1$, and

\[ y_{ij}' = y_{ij}'' = 0 \quad \text{if} \quad x_{ij} \leq 1/2 \]

\[ y_{ij}' = y_{ij}'' = 1 \quad \text{if} \quad x_{ij} > 1/2 \]

for $j = 2, 3, 4$. Applying $G^{-1}$ to $(y_1', \cdots, y_4')$ and $(y_1'', \cdots, y_4'')$ we obtain lattice points $(y_1', \cdots, y_4')$ and $(y_1'', \cdots, y_4'')$ respectively (with coordinates zeros or ones) satisfying (1.1).

Received by the editors September 2, 1959, and, in revised form, March 16, 1960.


164
2. Some definitions and statement of results. An ordered set of integers \((a_1, \ldots, a_r) (1 \leq a_1 < a_2 < \cdots < a_r, 1 \leq r \leq \lfloor n/r \rfloor, n \geq 4)\) will be called a primary set of order \(r\) if

\[
a_i \leq (n - 3) - 4(r - i) \quad (i = 1, \ldots, r).
\]

Let \((x_1, \ldots, x_n) (0 \leq x_i \leq 1, i = 1, \ldots, n; n \geq 4)\) be arbitrarily chosen (but held fixed in the following argument). Let \((x_{i_1}, \ldots, x_{i_n})\) be a rearrangement \(H\) of \((x_1, \ldots, x_n)\) for which

\[
\left| x_{i_1} - \frac{1}{2} \right| \leq \left| x_{i_2} - \frac{1}{2} \right| \leq \cdots \leq \left| x_{i_n} - \frac{1}{2} \right|.
\]

Let \(z_1, \ldots, z_n\) denote \(x_{i_1}, \ldots, x_{i_n}\) respectively.

Now, each primary set \((a_1, \ldots, a_r)\) induces a partition\(^2\)

\[
\{1, \ldots, n\} = F + N
\]

where

\[
(2.3) \quad F = \{a_1, \ldots, a_r\}, \quad N = \{1, \ldots, n\} - \{a_1, \ldots, a_r\}.
\]

Let \(k\) range over \(\{1, \ldots, n\}\):

(i) if \(k \in F\), let

\[
(2.4) \quad p_k = \begin{cases} 0 & \text{if } z_k > 1/2, \\ 1 & \text{if } z_k \leq 1/2; \end{cases}
\]

(ii) if \(k \in N\), let

\[
(2.5) \quad p_k = \begin{cases} 0 & \text{if } z_k \leq 1/2, \\ 1 & \text{if } z_k > 1/2. \end{cases}
\]

Now, because of (2.1), with each element \(a_i\) of \(F\) (cf. (2.3)) may be associated integers \(b_i, c_i, d_i\) of \(N\) (cf. (2.3)) such that \(a_i < b_i < c_i < d_i\), holds for \((i = 1, \ldots, r)\), and such that (the intersection) \(\{a_j, b_j, c_j, d_j\} \cap \{a_k, b_k, c_k, d_k\}\) is null for all pairs \(j, k \in \{1, \ldots, r\}\) \((j \neq k)\). Recalling the solutions for the case \(n = 4\) (cf. the end of §1) we have,

\[
(z_a - p_a)^2 + (z_b - p_b)^2 + (z_c - p_c)^2 + (z_d - p_d)^2 \leq 1
\]

for \((i = 1, \ldots, r)\). We note that \((z_i - p_i)^2 \leq 1/4\) for each element \(i\) of

\[
\{1, \ldots, n\} - \sum_{i=1}^{r} \{a_i, b_i, c_i, d_i\}
\]

\(^2\) We use the symbol \(\{ \}\) to denote “unordered set”. The operations “+”, “−”, “•” between unordered sets are those in common usage in set theory.
(if indeed there are such). Therefore \( \sum_{k=1}^{n} (x_k - p_k)^2 \leq n/4 \). Applying \( H^{-1} \) to \( (p_1, \cdots, p_n) \) we obtain a lattice point \( (y_1, \cdots, y_n) (y_i = 0 \text{ or } 1) \) satisfying (1.1). We call \( (y_1, \cdots, y_n) \) an \( (H)\)-lattice-point (since it depends on \( H \)) associated with the primary set \( (a_1, \cdots, a_r) \). The lattice point obtained by letting \( y_i = 0 \) if \( x_i \leq 1/2 \) and \( y_i = 1 \) if \( x_i > 1/2 \) \((i = 1, \cdots, n)\) will be referred to as the \( (H)\)-lattice-point associated with the null set (which we here call the "primary set of order zero" for convenience of exposition).

**Statement of results.** Let \( A_{i,j} \) denote the element in the \( i \)'th row and \( j \)'th column of the double array:

\[
\begin{array}{cccccccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots \\
0 & 0 & 0 & 0 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & \cdots \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 22 & 30 & 39 & 49 & \cdots \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 140 & 200 & 272 & 357 & 456 & \cdots \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 969 & \cdots \\
\cdots \\
\end{array}
\]

i.e., (i) if \( i = 1 \), then \( A_{i,j} = 1 \) for all positive integers \( j \), (ii) if \( i > 1 \), then \( A_{i,j} = 0 \) for each positive integer \( j \leq 4(i-1) \), and

\[
A_{i,j} = \sum_{k=4(i-2)+1}^{j-1} A_{i-1,k}
\]

for each positive integer \( j > 4(i-1) \).

First an algorithm is given (cf. §4) for listing all primary sets of order \( r \) \((1 \leq r \leq \lfloor n/4 \rfloor)\), and the following theorem concerning the "length" of a complete listing is established:

**Theorem 1.** For a given \( n \geq 4 \), the total number of primary sets of orders 0, 1, \cdots, \( \lfloor n/4 \rfloor \) is

\[
\theta = 1 + \sum_{j=1}^{n-3} \sum_{i=1}^{\lfloor n/4 \rfloor} A_{i,j}.
\]

**Theorem 2.** (i) Each primary set (which may be the primary set of order zero) has one and only one associated \( (H)\)-lattice-point, and (ii) distinct primary sets have distinct associated \( (H)\)-lattice-points.

We thus have the following constructive process for obtaining vertices of \( C \) inside or on \( S_p \):

**Step 1.** Once \( n \geq 4 \) is specified, list all \( \theta \) primary sets. This may be done by the algorithm of §4.

**Step 2.** Once \( (x_1, \cdots, x_n) \) is specified determine a rearrangement \( H \)
yielding \((z_1, \ldots, z_n)\). Fixing attention on each primary set in turn, apply (2.4) and (2.5) to \((z_1, \ldots, z_n)\), thus obtaining \((p_1, \ldots, p_n)\); we then apply \(H^{-1}\) to \((p_1, \ldots, p_n)\) and obtain an \((H)\)-lattice-point satisfying (1.1).

Remark. If \((x_1, \ldots, x_n)\) is such that \(|x_i - 1/2| \neq |x_j - 1/2|\) for all pairs \(i, j\) \((i \neq j)\), then there is only one rearrangement \(H\) satisfying (2.2). If \((x_1, \ldots, x_n)\) is such that \(|x_i - 1/2| = |x_j - 1/2|\) for some pair \(i, j\) \((i \neq j)\), let

\[
H_1: (x_{i_1}, \ldots, x_{i_n}), \quad H_2: (x_{j_1}, \ldots, x_{j_n}), \ldots
\]

be all the rearrangements of \((x_1, \ldots, x_n)\) such that

\[
\begin{align*}
|x_{i_1} - 1/2| & \leq \cdots \leq |x_{i_n} - 1/2|, \\
|x_{j_1} - 1/2| & \leq \cdots \leq |x_{j_n} - 1/2|, \ldots
\end{align*}
\]

Let all \(\theta\) \((H_1)\)-lattice-points be obtained. To find those \((H_2)\)-lattice-points which are not \((H_1)\)-lattice-points, we need only consider primary sets \((a_1, \ldots, a_r)\) such that \((j_{a_1}, \ldots, j_{a_r}) \not\in i_{a_1}, \ldots, i_{a_r})\).

3. A lemma. Let \(\Delta_r(n)\) \((1 \leq r \leq \lfloor n/4 \rfloor)\) denote the matrix in the upper left-hand corner of (2.6) consisting of all elements \(A_{i,j}\) \((i = 1, \ldots, r; j = 1, \ldots, n - 3)\). It will be convenient to introduce a new designation for an arbitrary element of \(\Delta_r(n)\), say \(s_{i,k}\), where \(i\) indicates the \(i\)th row from the top (as before), but \(k\) now indicates the \(k\)th column from the right; (thus \(A_{i,j} = s_{i,k}\) where \(k = n - 2 - j\) \((j = 1, \ldots, n - 3)\)).

Lemma. Let \(s_{i,k}\) \((i > 1)\) be any nonzero element of \(\Delta_m(n)\) \((m = \lfloor n/4 \rfloor)\) such that \(s_{i,k+1}\) is not zero. Then

\[
s_{i,k} = s_{i,k+1} + s_{i-1,k+2} + s_{i-2,k+3} + \cdots + 1.
\]

Proof. From (2.7) it follows that \(s_{i,k} = s_{i,k+1} + s_{i-1,k+1}\). Since \(s_{i-1,k+1} = s_{i-1,k+2} + s_{i-2,k+2}\), we obtain

\[
s_{i,k} = s_{i,k+1} + s_{i-1,k+2} + s_{i-2,k+2}.
\]

Repeating this argument on the last term of (3.2), etc., we finally obtain (3.1).

4. An algorithm. Let \(S_r\) denote the sum of the elements of the \(r\)th row of \(\Delta_r(n)\) \((1 \leq r \leq \lfloor n/4 \rfloor, n \geq 4)\). Let \(q_0\) be an integer satisfying \(1 \leq q_0 \leq S_r\). We shall associate with \(q_0\) a primary set \((j_0, j_1, \ldots, j_{r-1})\) as follows:

1. Determination of \(j_0\). We notice that
where \( v_0 = (n - 3) - (r - 1)4 \); there are \((r - 1)4\) zeros to the left of \(s_{r.,v_0}\) in the last row of \(\Delta_r(n)\). Then from (4.1) we see that there is one and only one integer \(j_0\) satisfying 1 \(\leq j_0 \leq (n - 3) - (r - 1)4\) such that

\[
\sum_{j=j_0+1}^{v_0} s_{r,j} < q_0 \leq \sum_{j=j_0}^{v_0} s_{r,j}
\]

(here and below, expressions of the form \(\sum_{j=A}^{B} U_j\) where \(B < A\) are to be taken as zero).

2. Determination of \(j_1\). We notice that

\[
s_{r,0} = s_{r-1,v_1} + s_{r-1,v_1-1} + \cdots + s_{r-1,v_0+1}
\]

where \(v_1 = (n - 3) - (r - 2)4\); there are \((r - 2)4\) zeros to the left of \(s_{r-1,v_1}\) in the \((r - 1)\)st row of \(\Delta_r(n)\). Let 

\[
q_1 = q_0 - \sum_{j=j_0+1}^{v_0} s_{r,j} ;
\]

then 1 \(\leq q_1 \leq s_{r,j_0}\). From (4.3) we see that there is one and only one integer \(j_1\) satisfying \(j_0 < j_1 \leq (n - 3) - (r - 2)4\) such that

\[
\sum_{j=j_1+1}^{v_1} s_{r-1,j} < q_1 \leq \sum_{j=j_1}^{v_1} s_{r-1,j}.
\]

3. Let us suppose that integers \(j_0, j_1, \ldots, j_{i-1}\) have been determined, each \(j_g\) \((g \in \{1, 2, \ldots, i - 1\})\) being the only integer which satisfies

\[
j_{g-1} < j_g \leq (n - 3) - (r - (g + 1))4 = v_g
\]

and

\[
\sum_{j=j_0+1}^{v_g} s_{r-g,j} < q_g \leq \sum_{j=j_g}^{v_g} s_{r-g,j},
\]

where 

\[
q_g = q_{g-1} - \sum_{j=j_{g-1}+1}^{v_{g-1}} s_{r-(g-1),j},
\]

i.e., 

\[
q_g = q_0 - \left( \sum_{j=j_0+1}^{v_0} s_{r,j} + \sum_{j=j_1+1}^{v_1} s_{r-1,j} + \cdots + \sum_{j=j_{g-1}+1}^{v_{g-1}} s_{r-(g-1),j} \right).
\]
We show how to determine $j_i$. We notice that (if $r - (i - 1) \geq 2$)

\[
s_{r - (i - 1), j_{i-1}} = s_{r - i, v_i} + s_{r - i, (v_i + 1)} + \cdots + s_{r - i, (v_i + (i - 1))},
\]

where $v_i = v_0 + 4i$; there are $(r - (i + 1))4$ zeros to the left of $s_{r - i, v_i}$ in the $(r - i)$th row of $\Delta_r(n)$. Let

\[
q_i = q_{i-1} - \sum_{j = j_i - 1}^{v_i - 1} s_{r - (i - 1), j}.
\]

Then, letting $g = i - 1$ in (4.6), and subtracting the left sum, we obtain

\[
1 \leq q_i \leq s_{r - (i - 1), j_{i-1}}.
\]

From (4.7) we see that there is one and only one integer $j_i$ satisfying

\[
j_{i-1} < j_i \leq (n - 3) - (r - (i + 1))4 = v_i
\]
such that

\[
\sum_{j = j_i + 1}^{v_i} s_{r - i, j} < q_i \leq \sum_{j = j_i}^{v_i} s_{r - i, j}.
\]

Repeatedly selecting the $j_i$ as described in (3) (immediately above), we finally obtain the primary set $(j_0, \ldots, j_{r - 1})$ which we associate with $q_0$.

From the manner in which $(j_0, \ldots, j_{r - 1})$ was selected we may now show that

\[
q_0 = 1 + \sum_{k=0}^{r-1} \sum_{j=j_k+1}^{v_k} s_{r-k, j}.
\]

**Proof of (4.11).** Let

\[
\beta_k = \sum_{j=j_k+1}^{v_k} s_{r-k, j}.
\]

Then from (4.8) $q_0 = q_1 + \beta_0$, $q_1 = q_2 + \beta_1$, \ldots; therefore

\[
q_0 = q_{r-1} + \beta_{r-2} + \beta_{r-3} + \cdots + \beta_0.
\]

But from (4.10), since $s_{1, 1} = 1$

\[
q_{r-1} = \sum_{j=j_{r-1}}^{v_{r-1}} s_{1, j} = 1 + \beta_{r-1},
\]

and (4.13) becomes

\[
q_0 = 1 + \sum_{k=0}^{r-1} \beta_k.
\]

Substituting (4.12) into (4.14) we obtain (4.11).
5. The number of primary sets \((a_1, \cdots, a_r)\). With any integer \(g_0 (1 \leq g_0 \leq S_r)\) we have associated a primary set \((j_0, j_1, \cdots, j_{r-1})\) determined as in §4.

We now show that any primary set \((h_0, h_1, \cdots, h_{r-1})\) is an associate of an integer \(I\) satisfying \(1 \leq I \leq S_r\).

(A) Let

\[
I = 1 + \sum_{k=0}^{r-1} \sum_{j=h_k+1}^{v_k} S_{r-k,j}.
\]

It is clear that \(I \geq 1\). We first prove that

\[
I \leq S_r.
\]

Proof of (5.2). (i) Suppose there are at least two nonzero terms in the last row of \(\Delta_r(n)\). Then

\[
1 + \sum_{k=0}^{r-1} \sum_{j=h_k+1}^{v_k} S_{r-k,j} \leq 1 + \sum_{k=0}^{r-1} \sum_{j=k+2}^{v_k} S_{r-k,j}
\]

\[
= 1 + \sum_{k=1}^{r-1} \sum_{j=k+2}^{v_k} S_{r-k,j} + \sum_{j=2}^{v_0} S_{r,j}
\]

\[
= 1 + \sum_{k=1}^{r-1} S_{r-(k-1),k+1} + \sum_{j=2}^{v_0} S_{r,j}
\]

\[
= s_{r,1} + \sum_{j=2}^{v_0} s_{r,j} = S_r.
\]

(ii) Suppose there is only one nonzero term in the last row of \(\Delta_r(n)\). Then

\[
1 + \sum_{k=0}^{r-1} \sum_{j=h_k+1}^{v_k} S_{r-k,j} \leq 1 + \sum_{k=0}^{r-1} \sum_{j=k+2}^{v_k} S_{r-k,j}
\]

\[
= 1 + \sum_{k=1}^{r-1} \sum_{j=k+2}^{v_k} S_{r-k,j}
\]

\[
= 1 + \sum_{k=2}^{r-1} \sum_{j=k+2}^{v_k} S_{r-k,j} + \sum_{j=3}^{v_1} S_{r-1,j}
\]

\[
= 1 + \sum_{k=2}^{r-1} S_{r-(k-1),k+1} + \sum_{j=3}^{v_1} S_{r-1,j}
\]

\[
= s_{r-1,2} + \sum_{j=3}^{v_1} s_{r-1,j}
\]

\[
= s_{r,1} = S_r.
\]
(B) We now show that the primary set \((h_0, h_1, \ldots, h_{r-1})\) is an associate of \(I\) (as defined by (5.1)) which we write as follows:

\[
I = 1 + \sum_{j=0}^{n_0} s_{r, j} + \sum_{j=1}^{n_1} s_{r-1, j} + \cdots + \sum_{j=r}^{n_r} s_{1, j}.
\]

We recall that \(h_k\) by definition satisfies \(1 \leq h_0 < h_1 < \cdots < h_{r-1}\) and \(h_k \leq (n-3) - (r - (k+1))4 = v_k\); also, that in determining the primary set associated with a given integer \(g_0\) \((1 \leq g_0 \leq S_r)\) there is one and only one selection \(j_i\) possible at each step (cf. (1), (2), (3) of §4). Thus, if we can show that

\[
\sum_{j=0}^{v_0} s_{r, j} < I \leq \sum_{j=0}^{v_0} s_{r, j}
\]

then \(j_0 = h_0\). And, if we can show that if \(j_0 = h_0, j_1 = h_1, \ldots, j_{i-1} = h_{i-1}\) then

\[
\sum_{j=0}^{v_i} s_{r-i, j} < q_i' \leq \sum_{j=0}^{v_i} s_{r-i, j}
\]

where

\[
q_i' = 1 + \sum_{j=h_i+1}^{v_i} s_{r-i, j} + \sum_{j=1}^{v_{i+1}} s_{r -(i+1), j} + \cdots + \sum_{j=1}^{v_r} s_{1, j},
\]

then \(j_i = h_i\) \((i = 1, \ldots, r-1)\).

The left inequalities of (5.3) and (5.4) are obvious. The right inequalities of (5.3) and (5.4) will be true if we can show that

\[
1 + \sum_{j=h_i+1}^{v_i+1} s_{r-(i+1), j} + \sum_{j=h_i+2}^{v_{i+1}} s_{r -(i+2), j} + \cdots + \sum_{j=h_r-1}^{v_r} s_{1, j} \leq s_{r-i, h_i},
\]

for \(i \geq 0\) (and then add \(\sum_{j=h_i+1}^{v_i+1} s_{r-i, j}\) to both sides).

**Proof of (5.6).** **Case I.** Suppose \(s_{r-i, h_{i+1}} \neq 0\). Then

\[
\sum_{j=h_i+1}^{v_i+1} s_{r-(i+1), j} \leq \sum_{j=h_i+2}^{v_{i+1}} s_{r -(i+1), j} = s_{r-i, h_i+1}
\]

\[
\sum_{j=h_i+2}^{v_{i+2}} s_{r -(i+2), j} \leq \sum_{j=h_i+3}^{v_{i+2}} s_{r -(i+2), j} = s_{r-(i+1), h_i+2}
\]

\[\vdots\]

\[
\sum_{j=h_r-1}^{v_r} s_{1, j} \leq \sum_{j=h_i+(r-i)}^{v_r} s_{1, j} = s_{2, h_i+(r-i)},
\]

for \(i \geq 0\).
But by the lemma of §3,

\[ s_{r-i, h_i} = s_{r-i, h_i+1} + s_{r-(i+1), h_i+2} + \cdots + s_{2, h_i+r-(i+1)} + 1. \]

Therefore (5.6) is true (in this case) for \( i \geq 0 \).

Case II. Suppose \( s_{r-i, h_i+1} = 0 \). Then, using the ideas appearing in the proof of Case I, the left side of (5.6) is less than or equal to

\[ 1 + \left( \sum_{j=h_i+2}^{v_i+1} s_{r-(i+1), j} \right) + s_{r-(i+1), h_i+2} + s_{r-(i+2), h_i+3} + \cdots + s_{2, h_i+r-(i+1)} \]

\[ = \left( \sum_{j=h_i+2}^{v_i+1} s_{r-(i+1), j} \right) + s_{r-(i+1), h_i+1} = \sum_{j=h_i+1}^{v_i+1} s_{r-(i+1), j} = s_{r-i, h_i} \]

for \( i \geq 0 \).

6. The number of primary sets \((a_1, \cdots, a_r)\) (continued). In §4 we have associated with each integer \( g_0 \) \((1 \leq g_0 \leq S_r)\) a primary set \((j_0, j_1, \cdots, j_{r-1})\). In §5 we have shown that each primary set \((h_0, h_1, \cdots, h_{r-1})\) is the associate of an integer \( I \) \((1 \leq I \leq S_r)\). We show that this correspondence is 1-1 reciprocal:

(i) Each integer \( g_0 \) \((1 \leq g_0 \leq S_r)\) has one and only one associated primary set \((j_0, j_1, \cdots, j_{r-1})\) because in selecting the \( j_i \)'s one and only one \( j_i \) can be selected at each step (cf. §4).

(ii) Integers \( g_0 \) and \( g_1 \) \((1 \leq g_0 \leq S_r, 1 \leq g_1 \leq S_r, g_0 \neq g_1)\) cannot be associated with the same primary set \((h_0, h_1, \cdots, h_{r-1})\). For in the contrary case \( g_0 \) and \( g_1 \) would each be equal to the right side of (4.11), and therefore to each other, which is impossible.

Thus there are \( S_r \) primary sets of order \( r \). If \( r \) now varies over the range \( 1 \leq r \leq \lceil n/4 \rceil \), then there are as many primary sets of positive order as the sum of the terms of \( \Delta_m(n) \) \((m = \lceil n/4 \rceil)\). Adjoining the primary set of order zero we have Theorem 1 as stated.

7. Proof of Theorem 2. Proof of (i). We recall that \((z_1, \cdots, z_n)\) is fixed. Let a primary set \((a_1, \cdots, a_r)\) (which may be of order zero) be given. Then with each \( k \) \((k \in \{1, \cdots, n\})\) (2.4) or (2.5) associates one and only one integer \( p_k (= 0 \text{ or } 1) \) accordingly as \( k \) belongs to \( F \) (which may be null) or to \( N \) (cf. (2.3)). Thus with each primary set is associated one and only one \( n \)-tuple \((p_1, \cdots, p_n)\). Applying \( H^{-1} \) to \((p_1, \cdots, p_n)\) we obtain the unique lattice point associated with the primary set \((a_1, \cdots, a_r)\).

Proof of (ii). Let distinct primary sets

\[ (7.1) \quad (a_1, \cdots, a_r) \text{ and } (a_1', \cdots, a_r') \]
be given \((r \geq s); (a'_1, \cdots, a'_s)\) may be the null set). Then (2.4) and (2.5) associate with (7.1)

\[(7.2) \quad (p_1, \cdots, p_n) \quad \text{and} \quad (p'_1, \cdots, p'_n)\]

respectively. Since the primary set (7.1) are distinct, there must be an \(a_i\) such that \(a_i \in \{a'_1, \cdots, a'_s\}\). The \(n\)-tuplets (7.2) will be distinct since \(p_{a_i} \neq p'_{a_i}\). Therefore the lattice points associated with the primary sets (7.1) will be distinct.

CITY COLLEGE, NEW YORK

SUBGROUPS OF THE UNIMODULAR GROUP

IRVING REINER

Following the notation of [3], we let \(\Gamma\) denote the proper unimodular group consisting of all \(2 \times 2\) matrices with rational integral elements and determinant +1. For \(m\) a positive integer, define the principal congruence group \(\Gamma(m)\) by

\[(1) \quad \Gamma(m) = \{X \in \Gamma: X \equiv I \pmod{m}\},\]

where \(I\) denotes the identity matrix in \(\Gamma\), and where congruence of matrices is interpreted as elementwise congruence.

For \(p\) a prime, we know from [2] that \(\Gamma(p)\) is a free group with a finite set \(S\) of generators. If we define

\[(2) \quad T_m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix},\]

then \(S\) may be chosen to include \(T_p\). For each fixed integer \(s\), we may define a group \(\Omega(p, s)\) consisting of all power products of the generators in \(S\) for which the exponent sum for each generator is a multiple of \(s\). In [3] it was shown that each \(\Omega(p, s)\) is a normal subgroup of \(\Gamma\) of finite index in \(\Gamma\). Furthermore, if \(s > 1\) and \((s, p) = 1\), it was proved that \(\Omega(p, s)\) does not contain any principal congruence group.

Let \(\Delta(m)\) denote the normal subgroup of \(\Gamma\) which is generated by \(T_m\). Obviously \(\Delta(m) \subseteq \Gamma(m)\). Recently, Brenner [1] raised the following questions:

A. Does \(\Delta(m) = \Gamma(m)\) for all \(m\)?

Received by the editors May 2, 1960.

1 This research was supported by the Office of Naval Research.