APPLICATIONS OF THE HARDY-RAMANUJAN PARTITION THEORY TO LINEAR DIOPHANTINE PROBLEMS

by
Michael Anshel and Dorian Goldfeld[1]

§1. Introduction and summary of results

In 1918 G.H. Hardy and S. Ramanujan [**H-R**] gave an asymptotic formula for the now classic partition function $p(n)$ which equals the number of unrestricted partitions of n. The value of $p(n)$ is precisely the number of solutions in nonnegative integers to the linear diophantine equation

$$1 \cdot y_1 + 2 \cdot y_2 + \quad \cdots \quad + n \cdot y_n = n.$$

Hardy and Ramanujan proved that

$$p(n) \sim \frac{1}{4n\sqrt{3}} \; e^{\pi\sqrt{\frac{2n}{3}}} \tag{1}$$

and actually obtained a more precise asymptotic formula where the error tends to 0 as $n \to \infty$. It was quite suprising at the time to find by analytic methods an asymptotic formula for an integer valued function (which grows exponentially) which was correct up to a term which rapidly approached zero! The method they developed to prove this result was subsequently refined by Hardy and Littlewood and is now generally referred to as the Hardy-Littlewood method. The key to proving (1) is the fact that the generating function

$$\begin{aligned} \phi(\tau) &= \prod_{m=1}^{\infty} (1 - e^{2\pi i m\tau})^{-1} \\ &= \sum_{m=0}^{\infty} p(m) \; e^{2\pi i m\tau} \end{aligned} \tag{2}$$

satisfies the modular relation [**H-R**]

$$\phi(\tau) = \epsilon \; \sqrt{\frac{c\tau + d}{i}} \; e^{\frac{\pi i}{12}(\tau - \frac{a\tau+b}{c\tau+d})} \; \phi(\frac{a\tau + b}{c\tau + d}) \tag{3}$$

for all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in PSL(2, \mathbb{Z})$, where ϵ is a certain 24^{th} root of unity.

We shall now give higher dimensional versions of the Hardy-Ramanujan partition theory and apply it to the following linear diophantine problem.

[1]Supported in part by NSF grant DMS-87-02169

Given positive integers k, t, nonnegative integers $w_{i,j}$ for $1 \le i \le k,\ 1 \le j \le t$ and nonnegative integers $n_1, ..., n_k$ consider the linear diophantine problem

$$
\begin{aligned}
n_1 &= w_{1,1}\, y_1 + w_{1,2}\, y_2 + \cdots + w_{1,t}\, y_t \\
n_2 &= w_{2,1}\, y_1 + w_{2,2}\, y_2 + \cdots + w_{2,t}\, y_t \\
&\ \ \vdots \\
n_k &= w_{k,1}\, y_1 + w_{k,2}\, y_2 + \cdots + w_{k,t}\, y_t
\end{aligned} \tag{4}
$$

which can be written succinctly as

$$N = WY \tag{5}$$

where $N = (n_1, ..., n_k)$, and W denotes the matrix $W = (w_{i,j})$. Here N, W are fixed and given, and

$$Y = \begin{pmatrix} y_1 \\ \vdots \\ y_t \end{pmatrix}$$

consists of nonnegative integral variables.

It was pointed out by Euler in 1748 [**Eu**], (see also [**Sch**]) that the number of nonnegative integral solutions to (4) is precisely equal to the coefficient of $x_1^{n_1} \cdots x_k^{n_k}$ in the expansion of

$$R(x_1, ..., x_k) = \left(1 - (x_1^{w_{1,1}} \cdots x_k^{w_{k,1}})\right)^{-1} \cdots \left(1 - (x_1^{w_{1,t}} \cdots x_k^{w_{k,t}})\right)^{-1}.$$

In the case of one equation (i.e. $k = 1\ \ n_1 = n$, etc.) let $N(n)$ denote the number of solutions of

$$w_1 y_1 + \cdots + w_t y_t = n.$$

Then (see [**Sch**])

$$\lim_{n\to\infty} \frac{N(n)}{n^{k-1}} = \frac{1}{(k-1)!\, w_1 \cdots w_t}.$$

One of the principal difficulties of working with $R(x_1, ..., x_k)$ is that it doesn't have the nice properties of a modular function. Our approach is to follow Hardy and Ramanujan and develop instead a generalized partition theory for the linear diophantine problem (4). This will enable us to get sharp estimates for the solutions of (4). It seems likely that this method is capable of further refinements and improvements and should ultimately lead to asymptotic results. This would require, however, a higher dimensional version of the Hardy-Littlewood method.

Let

$$\mathcal{S}(N, W) = \sum_{N=WY} \Big(\prod_{j=1}^{t} p(y_j) \Big)$$

where the sum ranges over nonnegative integral solutions in Y to the linear diophantine equation (4). We now construct a generating function in several variables for $\mathcal{S}(N, W)$.

For arbitrary variables $x_i,\ \ i = 1, 2, \dots, k,\ \ $ let

$$X_j = \prod_{i=1}^{k} (x_i)^{w_{i,j}}. \tag{6}$$

Define

$$F(x_1, ..., x_k) = \prod_{j=1}^{t} \prod_{r=1}^{\infty} (1 - (X_j)^r)^{-1}.$$

It follows that

$$\begin{aligned} F(x_1, ..., x_k) &= \prod_{j=1}^{t} \prod_{r=1}^{\infty} \left(1 + {X_j}^r + {X_j}^{2r} + {X_j}^{3r} + \cdots\right) \\ &= \prod_{j=1}^{t} \Big(\sum_{m=0}^{\infty} p(m)\, {X_j}^m \Big) \\ &= \prod_{j=1}^{t} \Big(\sum_{m=0}^{\infty} p(m) \prod_{i=1}^{k} (x_i)^{m w_{i,j}} \Big) \\ &= \sum_{m_1=0}^{\infty} \sum_{m_2=0}^{\infty} \cdots \sum_{m_t=0}^{\infty} p(m_1)p(m_2)\cdots p(m_t) \prod_{i=1}^{k} (x_i)^{\left[\sum_{j=1}^{t} m_j w_{i,j}\right]}. \end{aligned}$$

Hence, we obtain

$$F(x_1, ..., x_k) = \sum_{n_1=0}^{\infty} \cdots \sum_{n_k=0}^{\infty} \mathcal{S}(N, W)\, {x_1}^{n_1} \cdots {x_k}^{n_k}. \tag{7}$$

Now, let

$$f(\tau) = \sum_{n=1}^{\infty} a(n) e^{2\pi i n \tau}$$

be an arbitrary holomorphic modular form for $\mathrm{SL}(2, \mathbb{Z})$ with nonnegative Fourier coefficients $a(n)$. Assume that

$$f(\tau) = (c\tau + d)^{-s} f\left(\frac{a\tau + b}{c\tau + d}\right)$$

for all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL(2, \mathbb{Z})$, so that $f(\tau)$ has weight s.

Let us define

$$\mathcal{S}_\ell(N, W) = \sum_{N = WY} p(y_1) \cdots p(y_\ell)\, a(y_{\ell+1}) \cdots a(y_t).$$

Since we have the Hecke estimate (see **[Gu]**)

$$a(n) \ll n^{\frac{s}{2}}$$

and

$$p(n) \sim \frac{1}{4n\sqrt{3}} \; e^{\pi\sqrt{\frac{2n}{3}}}$$

we see that $\mathcal{S}_\ell(N,W)$ counts the solutions to $N = WY$ and selectively weights (stresses) $y_1, \ldots, y_\ell$.

By an argument similar to the proof of (7), we see that $\mathcal{S}_\ell(N,W)$ is precisely the coefficient of $e^{2\pi i n_1 \tau_1} \cdots e^{2\pi i n_k \tau_k}$ in

$$\prod_{j=1}^{\ell} \phi\Big(\sum_{i=1}^{k} \tau_i w_{i,j}\Big) \cdot \prod_{j=\ell+1}^{t} f\Big(\sum_{i=1}^{k} \tau_i w_{i,j}\Big).$$

We can now state our final results.

Theorem (1) *Let $\delta_1, \delta_2, ..., \delta_k$ be arbitrary nonnegative real numbers. Let $q \geq 1$, and define $C = \phi\left(\frac{i}{q+(1/q)}\right)$, and $\Lambda_j = \sum_{i=1}^{k} \delta_i \, w_{i,j}$. Then we have*

$$\mathcal{S}(N,W) \;\leq\; C^t \, e^{2\pi[n_1\delta_1 + \cdots + n_k\delta_k]} \prod_{\substack{j=1 \\ \Lambda_j < \frac{1}{q+(1/q)}}}^{t} \Big(\sqrt{q} + \sqrt{1/q}\Big)^{\frac{1}{2}} \; {\Lambda_j}^{\frac{1}{4}} \, e^{\frac{\pi}{12}\left[-\Lambda_j + (\Lambda_j)^{-1}\right]}.$$

Theorem (2) *Let $\delta_1, \delta_2, ..., \delta_k$ be arbitrary nonnegative real numbers. Let $q, q' \geq 1$, $C_\phi = \phi\left(\frac{i}{q+(1/q)}\right)$, $C_f = f\left(\frac{i}{q'+(1/q')}\right)$, and $\Lambda_j = \sum_{i=1}^{k} \delta_i w_{i,j}$, where f is an arbitrary holomorphic modular form of weight s for $SL(2,\mathbb{Z})$.*

Then we have the estimate

$$\mathcal{S}_\ell(N,W) \leq e^{2\pi[n_1\delta_1 + \cdots + n_k\delta_k]} \, U_\phi \, V_f$$

where

$$U_\phi = {C_\phi}^{\ell} \prod_{\substack{j=1 \\ \Lambda_j < \frac{1}{q+(1/q)}}}^{\ell} \Big(\sqrt{q} + \sqrt{1/q}\Big)^{\frac{1}{2}} \; {\Lambda_j}^{\frac{1}{4}} \, e^{\frac{\pi}{12}\left[-\Lambda_j + (\Lambda_j)^{-1}\right]},$$

and

$$V_\phi = {C_f}^{t-\ell} \prod_{\substack{j=\ell+1 \\ \Lambda_j < \frac{1}{q'+(1/q')}}}^{\ell} \Big[\Big(\sqrt{q'} + \sqrt{1/q'}\Big) \; \Lambda_j\Big]^{-s}.$$

Let $B_\ell(N,W)$ denote the bound for $\mathcal{S}_\ell(N,W)$ given in theorem (2). Since very precise asymptotics exist for $p(n)$, it is possible to remove the weights without considerable loss of accuracy. In this manner we obtain:

Theorem (3) *If $N = WY$ admits a solution Y, then for arbitrary nonnegative real numbers $\delta_1, \cdots, \delta_k$ we have*

$$\sum_{j=1}^{\ell} \sqrt{y_j} \leq \frac{1}{2}\Big[\Big(\sum_{i=1}^{k} n_i\delta_i\Big) + \sum_{j=1}^{\ell}\Big(\sum_{i=1}^{k} \delta_i w_{i,j}\Big)^{-1}\Big].$$

Assume there exists a solution Y of $N = WY$ so that $p(y_1)\cdots p(y_\ell)\, a(y_{\ell+1})\cdots a(y_t)$ is minimal subject to $a(y_{\ell+1})\cdots a(y_t) \geq 1$, where the $a(n)$ are nonnegative Fourier coefficients of an arbitrary modular form f of weight s as in theorem (2).

Let

$$\mathcal{N} = \sum_{N=WY} 1.$$

Then we have

$$\Big(\sum_{j=1}^{\ell} \sqrt{y_j}\Big) + \log(\mathcal{N}) \leq \frac{1}{A}\log\left(B_\ell(N, W)\right) + \kappa\ell$$

where $A = 2(1 - \log(\frac{4}{3}) - \frac{\log 7}{\sqrt{7}}) = .68915...$, and $\kappa = 1$. If all the y_j, $(j = 1, \cdots, \ell)$ are sufficiently large, then we may take $\kappa = 0$ and A arbitrarily close to $\pi\sqrt{\frac{2}{3}}$.

To optimize the bounds in the previous theorems it is necessary to choose $\delta_1, ...\delta_k$ so that

$$n_1\delta_1 + \cdots + n_k\delta_k \;\approx\; \sum^{\ell}\Big(\sum^{k} \delta_i w_{i,j}\Big)^{-1}.$$

If all the δ_i, $(i = 1, ..., k)$ are equal to some fixed δ then we may take

$$\delta = \left[\Big(\sum_{i=1}^{k} n_i\Big)^{-1} \cdot \sum_{j=1}^{\ell}\Big(\sum_{i=1}^{k} w_{i,j}\Big)^{-1}\right]^{\frac{1}{2}}.$$

In this manner we obtain the estimate

$$\sum_{j=1}^{\ell} \sqrt{y_j} \leq \Big(\sum_{i=1}^{k} n_i\Big)^{\frac{1}{2}} \cdot \Big(\sum_{j=1}^{\ell}\Big(\sum_{i=1}^{k} w_{i,j}\Big)^{-1}\Big)^{\frac{1}{2}}.$$

We now obtain from theorem (3) a bound for the length $\sum_{j=1}^{t} y_j$ of the solution Y for the linear diophantine equation $N = WY$. We have

$$\sum_{j=1}^{t} y_j \leq \Big(\sum_{j=1}^{t} \sqrt{y_j}\Big) \cdot \Big(\max_{1\leq j\leq t} \sqrt{y_j}\Big).$$

Putting $\ell = 1$ in theorem (3) we see that

$$\sqrt{y_j} \leq \frac{1}{2}\Big[\Big(\sum_{i=1}^{k} n_i\delta_i\Big) + (\Lambda_j)^{-1}\Big].$$

Hence

$$\sum_{j=1}^{t} y_j \le B(N,W)$$

with

$$B(N,W) = \frac{1}{4}\Big[\Big(\sum_{i=1}^{k} n_i\delta_i\Big) \ + \ \sum_{j=1}^{t}(\Lambda_j)^{-1}\Big] \cdot \max_{1\le j\le t}\Big[\Big(\sum_{i=1}^{k} n_i\delta_i\Big) + (\Lambda_j)^{-1}\Big].$$

With the choice of δ given above, it follows that

$$B(N,W) = \Big(\sum_{i=1}^{k} n_i\Big) \cdot \Big[\sum_{j=1}^{\ell}\Big(\sum_{i=1}^{k} w_{i,j}\Big)^{-1}\Big]^{\frac{1}{2}} \cdot \max_{1\le j\le t}\Big(\sum_{i=1}^{k} w_{i,j}\Big)^{-\frac{1}{2}}. \tag{8}$$

Note that bounds of the above type may be useful in determining small solutions to the diophantine problem (4).

§2. Elementary proof that $e^{-A}e^{A\sqrt{m}} \leq p(m)$

In this section, we give an elementary proof that for all integers $m = 0, 1, 2, 3, ...$

$$p(m) \;\geq\; e^{-A}e^{A\sqrt{m}} \tag{9}$$

for $A = 2(1 - \log(\frac{4}{3}) - \frac{\log 7}{\sqrt{7}}) = .68915...$ Since $p(0) = 1 > e^{-A}$, we consider only the case $m \geq 1$.

Let us define $p_r(m)$ as the number of partitions of m into at most r parts. A generating function for $p_r(m)$ is given by

$$\sum_{m=0}^{\infty} p_r(m)x^m \;=\; \Big[(1-x)(1-x^2)\cdots(1-x^r)\Big]^{-1}.$$

Then $p_r(m)$ satisfies the recurrence relation

$$p_r(m) = p_{r-1}(m) + p_{r-1}(m-r) + p_{r-1}(m-2r) + \cdots \tag{10}$$

Following Hardy and Ramanujan **[H-R]**, we use (10) to prove, by induction, that

$$p_r(m) \geq \frac{rm^{r-1}}{(r!)^2}. \tag{11}$$

Clearly (11) is true for $r = 1$. Assuming it is true for $r \geq 1$, we have

$$\begin{aligned} p_{r+1}(m) &\geq \frac{r}{(r!)^2}\left[m^{r-1} + (m-r+1)^{r-1} + (m-2r-2)^{r-1} + \cdots\right] \\ &\geq \frac{m^r}{[(r+1)(r!)]^2} \\ &= \frac{(r+1)m^r}{((r+1)!)^2}\,. \end{aligned}$$

This proves (11). But $p(m) \geq p_r(m)$ for any r. Choosing $r = [\sqrt{m}\,]$, where $[x]$ denotes the smallest integer $\geq x$, we obtain

$$p(m) \;\geq\; \frac{[\sqrt{m}\,]m^{\sqrt{m}}}{m\big([\sqrt{m}\,]!\big)^2}. \tag{12}$$

By Stirling's asymptotic formula, (see Gradshteyn and Ryzhik **[G-R]**), we have that

$$[\sqrt{m}\,]! \;=\; \frac{\sqrt{2\pi}}{e}\Big([\sqrt{m}\,]+1\Big)^{[\sqrt{m}\,]+\frac{1}{2}} \cdot \Big(e^{-[\sqrt{m}\,]}\Big) \cdot \Big(1 + \frac{\theta}{12([m]+1)}\Big)$$

where $|\theta| \leq 1$ uniformly for $m = 1, 2, 3, ...$

Now, for $m \geq B$, and $[\sqrt{m}\,]+1 \leq \sqrt{m}+2 \leq \big(1+\frac{2}{\sqrt{B}}\big)\sqrt{m}$, it follows that for $m \geq B > 3$

$$\big([\sqrt{m}\,]!\big)^2 \;\leq\; \frac{2\pi}{e^2}\left(\frac{37}{36}\right)^2 \cdot \Big(m^{(\sqrt{m})+\frac{1}{2}}\Big) \cdot e^{-2[\sqrt{m}\,]} \cdot \left(1 + \frac{2}{\sqrt{B}}\right)^{2[\sqrt{m}\,]+1}.$$

Combining this result with (12) yields

$$p(m) \;\geq\; \frac{e^2}{2\pi}\big(\frac{36}{37}\big)^2 \cdot \left(1+\frac{2}{\sqrt{B}}\right)^{-1} \cdot \frac{1}{\sqrt{m}} \cdot e^{2\left[1-\log\,(1+\frac{2}{\sqrt{B}})\right]\sqrt{m}}.$$

Since

$$\frac{1}{m} \;\leq\; C^{-\frac{\log\,7}{\sqrt{7}}\sqrt{m}}$$

for all $m \geq 1$, we have, upon choosing $B = 36$ that

$$p(m) \;\geq\; C_1 e^{C_2\sqrt{m}} \qquad\qquad (m \geq 36)$$

with $C_1 = \frac{3}{8\pi}\big(\frac{36}{37}\big)^2 e^2$ and $C_2 = 2\big(1-\log\,\frac{4}{3}\big) - \frac{\log\,7}{\sqrt{7}}$). On the other hand, one easily checks that

$$p(m) \geq e^{-C_2} e^{C_2\sqrt{m}} \tag{13}$$

for $1 \leq m \leq 36$, and since $e^{-C_2} < C_1$ we obtain the inequality (13) for all integers $m \geq 0$.

§3. Proofs of theorems

The proofs of theorems (1),(2), and (3) are based on the following lemmas.

Lemma (1) *Let $\tau = \theta + i\delta$ be in the upper half plane. Then the function*

$$\phi(\tau) = \sum_{n=0}^{\infty} p(n) e^{2\pi i n\tau}$$

satisfies the estimate

$$|\phi(\tau)| \leq \begin{cases} (\delta)^{\frac{1}{4}} \left(\sqrt{q}+\sqrt{1/q}\right)^{\frac{1}{2}} \phi\big(\frac{i}{q+(1/q)}\big)\, e^{\frac{\pi}{12}[-\delta+\delta^{-1}]}, & \text{if } 0<\delta<\frac{1}{q+(1/q)}; \\ \phi\big(\frac{i}{q+(1/q)}\big) & \text{if } \delta \geq \frac{1}{q+(1/q)}, \end{cases}$$

where $q \geq 1$ is arbitrary.

Proof: If $\delta \geq \frac{1}{q+(1/q)}$, then clearly

$$|\phi(\tau)| \;\leq\; \sum_{n=0}^{\infty} p(n) e^{\frac{-2\pi n}{q+(1/q)}} \;\; .$$

On the other hand, if $0 < \delta < \frac{1}{q+(1/q)}$, and $\theta \in \mathbb{R}$, we can always choose integers c, d with $1 \leq c \leq \sqrt{\frac{q}{\delta}}$ so that

$$0 \leq |c\theta + d| \leq \sqrt{\delta/q}.$$

Since

$$Im\left(\frac{a\tau+b}{c\tau+d}\right) \;=\; \frac{\delta}{(c\theta+d)^2+(c\delta)^2}$$

it follows that

$$\frac{1}{q+(1/q)} \;\leq\; Im\left(\frac{a\tau+b}{c\tau+d}\right) \;\leq\; \delta^{-1}.$$

With this choice of c, d we then obtain from (3) that

$$|\phi(\tau)| \;\leq\; (\delta)^{\frac{1}{4}}\left(\sqrt{q}+\sqrt{1/q}\right)^{\frac{1}{2}}\;\phi\left(\frac{i}{q+(1/q)}\right)\;e^{\frac{\pi}{12}[-\delta+\delta^{-1}]}.$$

Lemma (2) *Let $\tau=\theta+i\delta$ be in the upper half plane. Let*

$$f(\tau)=\sum_{n=0}^{\infty}a(n)e^{2\pi in\tau}$$

be a holomorphic modular form of weight s for $SL(2,\mathbb{Z})$. Then we have

$$|f(\tau)|\leq\begin{cases}\delta^{-\frac{s}{2}}\left(\sqrt{q}+\sqrt{1/q}\right)^{-s}\;f\left(\frac{i}{q+(1/q)}\right) & \text{if } 0<\delta<\frac{1}{q+(1/q)}\\ f\left(\frac{i}{q+(1/q)}\right) & \text{if } \frac{1}{q+(1/q)}<\delta\end{cases}$$

where $q>1$ is arbitrary.

Proof: The proof is the same as the proof of lemma (1) except that instead of (3) we use the modular relation

$$f(\tau)=(c\tau+d)^{-s}f\left(\frac{a\tau+b}{c\tau+d}\right).$$

Proof of Theorems (1), (2):

Let $\tau_r=\theta_r+i\delta_r$ be in the upper half plane for $1\leq r\leq k$. We easily see from (7) that

$$(14)\quad \mathcal{S}(N,W) \;=\; D\int_0^1\cdots\int_0^1 F\left(e^{2\pi i\tau_1},...,e^{2\pi i\tau_k}\right)e^{-2\pi i\sum_{r=1}^{k}n_r\theta_r}\;d\theta_1\cdots d\theta_k$$

where

$$D \;=\; e^{2\pi[n_1\delta_1+\cdots+n_k\delta_k]}.$$

But

$$F\left(e^{2\pi i\tau_1},...,e^{2\pi i\tau_k}\right) \;=\; \prod_{j=1}^{t}\phi\Big(\sum_{i=1}^{k}\tau_i w_{i,j}\Big).$$

It immediately follows from Lemma (1) that
(15)

$$|F\left(e^{2\pi i\tau_1},...,e^{2\pi i\tau_k}\right)| \;\leq\; C^t \prod_{\substack{j=1 \\ \Lambda_j < \frac{1}{q+(1/q)}}}^{t} \left(\sqrt{q}+\sqrt{1/q}\right)^{\frac{1}{2}} \left(\Lambda_j\right)^{\frac{1}{4}} e^{\frac{\pi}{12}\left[-\Lambda_j+(\Lambda_j)^{-1}\right]}$$

where

$$\Lambda_j = \sum_{i=1}^{k} \delta_i w_{i,j}$$

and

$$C = \phi\left(\frac{i}{q+(1/q)}\right).$$

The proof of Theorem (1) is completed after the bound (15) is substituted into equation (14).

The proof of theorem (2) is exactly the same, except we use the generating function

$$F_\ell\left(e^{2\pi i\tau_1},\cdots,e^{2\pi i\tau_k}\right) = \prod_{j=1}^{\ell}\phi(\Lambda_j)\cdot\prod_{j=\ell+1}^{t} f(\Lambda_j)$$

and the bounds given in lemmas (1) and (2).

Proof of Theorem (3):
If the linear diophantine problem $N = WY$ has a solution Y, then it follows from the Cauchy-Schwartz inequality that

$$\begin{aligned}\sum_{j=1}^{\ell}\sqrt{y_j} &= \sum_{j=1}^{\ell}\sqrt{y_j}\cdot\sqrt{\Lambda_j/\Lambda_j} \\ &\leq \left[\left(\sum_{j=1}^{\ell} y_j\Lambda_j\right)\cdot\sum_{j=1}^{\ell}(\Lambda_j)^{-1}\right]^{\frac{1}{2}} \\ &\leq \frac{1}{2}\sum_{i=1}^{k} n_i\delta_i + \frac{1}{2}\sum_{j=1}^{\ell}(\Lambda_j)^{-1}.\end{aligned}$$

since

$$\sum_{j=1}^{\ell} y_j\Lambda_j \leq \sum_{j=1}^{t} y_j\Lambda_j = \sum_{i=1}^{k} n_i\delta_i.$$

If we have a solution $y_1 = m_1, \ldots, y_t = m_t$ with

$$p(m_1)\cdots p(m_\ell)\, a(m_{\ell+1})\cdots a(m_t)$$

minimized subject to

$$a(m_{\ell+1})\cdots a(m_t) \geq 1,$$

then

$$\mathcal{N}\cdot p(m_1)\cdots p(m_\ell) \leq \mathcal{S}_\ell(N,W).$$

It now follows from theorem (2) that

$$\sum_{j=1}^{\ell} \log\left(p(m_j)\right) \,+\, \log \mathcal{N} \leq \log\left(B_\ell(N,W)\right).$$

The completion of the proof follows easily from the lower bound (9)

$$\log\left(p(m_j)\right) \geq A\sqrt{m_j} \,-\, A,$$

and the asymptotic formula (3).

§4. Applications to equations in HNN groups

We apply the Hardy-Ramanujan partition theory developed above to the investigation of equations in HNN groups and relate the existence of solutions (and associated bounds) in special cases to a linear diophantine problem of Frobenius.

The groups we have in mind are a subclass of the HNN groups investigated in [**An**] in connection with Hilbert's tenth problem and in [**An-M**] in connection with fragments of Peano arithmetic.

By the class of linear vector groups (LVA) we understand the HNN groups $G = G(q_1, ..., q_t)$ given by the generators and relations

$$< a_1, ..., a_t,\, b;\, a_1^{-1} b a_1 = b^{q_1},\ \ldots\ , a_t^{-1} b a_t = b^{q_t} > \tag{16}$$

where the exponents $q_1, ..., q_t$ are distinct rational integers and each $q_i \geq 2$. Let $p_1, ..., p_k$ denote the distinct prime divisors of the exponents q_i so that each q_i factors as

$$q_i = {p_1}^{w_{i,1}} \cdots {p_k}^{w_{i,k}}, \qquad (i = 1, ..., t) \tag{17}$$

with nonnegative integer exponents $w_{i,1}, ..., w_{i,k}$. In addition, call a positive integer n admissible for G if its positive prime divisors are among $p_1, ..., p_k$.

A positive conjugate power equation for $G = G(q_1, ..., q_t)$ is given by

$$b^n = x^{-1} b x \tag{18}$$

where n is a positive integer termed the parameter and x is a positive word (i.e. one containing no negative exponents in the generating symbols $a_1, ..., a_t, b$).

It is a consequence of [**An**] or [**An-M**] that (18) has a solution provided n is admissible for G and (4) takes the form $N = (n_1, \ldots, n_k),\ n = p_1^{n_1} \cdots p_k^{n_k}$, where W consists of the $w_{i,j}$ given in (17) and each y_j in $Y = (y_1, \cdots, y_t)$ denotes the number of occurrences of a_i in the word x. Also, if x is a solution to (18), then insertion or deletion of a b symbol anywhere in the word x results in another solution to (18).

A solution x to (18) is called standard provided it is monotone nondecreasing in the generating symbols $a_1, \ldots, a_t$ and in the syllable sequence corresponding to each a_i. Thus x contains no subword of the form $a_i u a_j$ where $i > j$, nor a subword containing succesive a_i-syllables a_i^r, a_i^s, $r > s \geq 1$, (e.g. $a_1^3 b a_1^2$). In addition,

we call two standard solutions equivalent provided their a_i-syllable sequences are the same (e.g. $ba_1^2b^2a_1^2a_2^5ba_2^6$ and $a_1^2b^2a_1^2ba_2^5b^3a_2^6b$ each give rise to the syllable sequence $a_1^2, a_1^2, a_2^5, a_2^6$). We call the equivalence classes of standard solutions (18) the standard solution types of that equation.

The number of standard solution types of G to (18) is precisely given by $\mathcal{S}(N, W)$. To see this note that each standard solution type is determined by its a_i-syllable sequence. These syllable sequences are in turn in one-to-one correspondence with the partitions defined by the linear diophantine system (4) associated with the parameter n and the presentation (16) of G.

From theorem (1), equation (8), and the remarks above, we obtain.

Corollary (1) *Let $G = G(q_1, \ldots, q_t)$ be a linear vector group. Then it is decidable whether or not a positive power equation (18) has a solution x in G. If one such solution exists, then there exists a solution x involving only the generators $a_1, \ldots, a_t$. The word length of x denoted $|x|$ satisfies the bound*

$$|x| \leq B(N, W),$$

with $B(N, W)$ given by (8) and the number of standard solution types is precisely $\mathcal{S}(N, W)$. Moreover, N, W, $B(N, W)$, and $\mathcal{S}(N, W)$ together with its bound given in theorem (1) are effectively computable from the parameter n of (18) and the exponents of G given in (16).

Let $w_1, w_2, ..., w_t$ be positive relatively prime integers satisfying $w_i \geq 2$. The classical linear diophantine problem of Frobenius **[Sch]** is to find the largest positive integer $g(w_1, w_2, ..., w_t)$ which is not a linear combination of nonnegative integral multiples of the w_i, $i = 1, 2, ...t$. The Frobenius problem occurs cryptomorphically in solving (18) for a certain class of linear vector groups.

By a linear vector group $G = G(q_1, ..., q_t)$ of the Frobenius problem, we mean one such that $q_i = p^{w_i}$, p a fixed positive prime and w_i, $i = 1, .., t$ are distinct positive relatively prime integers $1 < w_1 < \cdots < w_t$.

Corollary (2) *If $G = G(p^{w_1}, ..., p^{w_t})$ is a linear vector group of the Frobenius problem and $n \geq g(w_1, ..., w_t)+1$, then the positive power equation admits a solution x and $|x| \leq B(N, W)$ with $B(N, W)$ given by (8).*

BIBLIOGRAPHY

[An] M.Anshel, *Vector groups and the equality problem for vector addition systems,* Math. Comp. **32**, (1978), 614-616.

[An-M] M. Anshel and K. McAloon, *Reducibilities among decision problems for HNN groups, vector addition systems and subsystems of Peano arithmetic,* Proc. Amer. Math. Soc. vol. **89**, Number 3 (1983), 425-429.

[**Eu**] L.Euler, Introductio in Analysin Infinistorum, vol.1, M.-M Bousquet, Lausanne 1748 [German translation by H. Maser: Einleitung in die Analysis des Unendlichen Erster Teil. Springer, Berlin, (1885) [reprinted; 1983]].

[**G-R**] I.S. Gradsteyn and I.M. Ryzhik, Tables of Integrals Series and Products, Academic Press (1965), 937.

[**Gu**] R.C. Gunning, Lectures on modular forms, Annals of Math. Studies Number **48**, Princeton Univ. Press, (1962).

[**H-R**] G.H. Hardy and S. Ramanujan, *Asymptotic formulae in combinatorial analysis,* Proc. London Math. Soc. (2) **17**, (1918), 75-115.

[**Sch**] A. Schrijver, Theory of Linear and Integer Programming, John Wiley and Sons (1986), 375-376.

Michael Anshel
Department of Computer Sciences
The City College of the City University of New York
New York, New York 10031

Dorian Goldfeld
Department of Mathematics
Columbia University
New York, New York 10027