Pacific Journal of Mathematics

ABELIAN GROUPS AND PACKING BY SEMICROSSES

DEAN ROBERT HICKERSON AND SHERMAN K. STEIN

Vol. 122, No. 1 January 1986

PACIFIC JOURNAL OF MATHEMATICS
Vol. 122, No. 1, 1986

ABELIAN GROUPS AND PACKING BY SEMICROSSES

DEAN HICKERSON AND SHERMAN STEIN

Motivated by a question about geometric packings in n-dimensional Euclidean space, $\mathbf{R}^n$, we consider the following problem about finite abelian groups. Let n be an integer, $n \geq 3$, and let k be a positive integer. Let $g(k,n)$ be the order of the smallest abelian group in which there exist n elements, $a_1, a_2, \ldots, a_n$, such that the kn elements ia_j, $1 \leq i \leq k$, are distinct and not 0. We will show that for n fixed, $g(k,n) \sim 2\cos(\pi/n)k^{3/2}$.

The geometric question concerns certain star bodies, called "semicrosses", which are defined as follows:

If k and n are positive integers, a (k,n)-semicross consists of $kn+1$ unit cubes in $\mathbf{R}^n$, a "corner" cube parallel to the coordinate axes together with n arms of length k attached to faces of the cube, one such arm pointing in the direction of each positive coordinate axis. Let K, the "semicross at the origin", be the semicross whose corner cube is $[0,1]^n$. Then every semicross is a translate of K; i.e. has the form $v+K$ for some vector v.

A family of translates $\{v+K\colon v \in H\}$ is called an integer lattice packing if H is an n-dimensional subgroup of Z^n and, for any two vectors v and w in H, the interiors of $v+K$ and $w+K$ are disjoint. We shall examine how densely such packings pack $\mathbf{R}^n$ for large k, and show that, for $n \geq 3$, this density is asymptotic to

$$\frac{n \sec \pi/n}{2\sqrt{k}}.$$

(For $n=1$ or 2 the density is 1 for every k.)

This result contrasts with the already known result for crosses. (A (k,n)-cross consists of $2kn+1$ unit cubes, a center cube with an arm of length k attached to each face.) As shown in **[St1]**, for $n \geq 2$ the integer lattice packing density of the (k,n)-cross is asymptotic to $2n/k$.

0. Preliminary matters. Suppose M is a set of nonzero integers, G is an abelian group, and n is a positive integer. We say that M n-packs G if there is a set $S \subseteq G$ such that $|S| = n$ and the elements ms with $m \in M$ and $s \in S$ are distinct and nonzero. Such a set S is called a packing set.

Let $S(k) = \{1, \ldots, k\}$ and $F(k) = \{\pm 1, \ldots, \pm k\}$. Then, as shown in **[St1]**, there is a relation between integer lattice packings by the (k, n)-semicross (resp. cross) and n-packings of finite abelian groups by $S(k)$ (resp. $F(k)$). We now develop this connection.

We will designate each unit cube in $\mathbf{R}^n$ with edges parallel to the coordinate axes by its vertex with minimal coordinates. Thus K, the (k, n)-semicross at the origin, is the union of the $kn + 1$ cubes designated by $(0, 0, \ldots, 0)$, $(i, 0, \ldots, 0), \ldots,$ and $(0, \ldots, 0, i)$ with $1 \le i \le k$.

Let H be an integer packing lattice for K, i.e. an n-dimensional subgroup of Z^n such that the interiors of $v + K$ for $v \in H$ are pairwise disjoint. Let $G = Z^n/H$, $f\colon\ Z^n \to G$ be the natural homomorphism, $e_i \in Z^n$ be the unit vector in the ith coordinate direction, and $a_i = f(e_i)$. Then it is easy to show that the kn elements ia_j with $1 \le i \le k$ and $1 \le j \le n$ are distinct and nonzero; that is, $S(k)$ n-packs G with packing set $\{a_1, \ldots, a_n\}$.

Conversely, suppose $S(k)$ n-packs a finite abelian group G with packing set $\{a_1, \ldots, a_n\}$. Let $H = \{(x_1, \ldots, x_n) \in Z^n\colon x_1 a_1 + \cdots + x_n a_n = 0\}$. Then H is an integer packing lattice for the (k, n)-semicross. Moreover, the density of this packing is $(kn + 1)/|G^*|$, where G^* is the subgroup generated by $a_1, \ldots, a_n$.

Thus, finding the densest integer lattice packing by the (k, n)-semicross is equivalent to finding the smallest abelian group G such that $S(k)$ n-packs G. Let $g(k, n)$ be the order of the smallest such group. Clearly $g(k, n) \ge kn + 1$, with equality if $n = 1$ or $n = 2$. Our main result is given in the following theorem.

THEOREM 1. *For $n \ge 3$,*

$$\lim_{k \to \infty} \frac{g(k, n)}{k^{3/2}} = 2 \cos \frac{\pi}{n}.$$

Since the integer lattice packing density of the (k, n)-semicross is $(kn + 1)/g(k, n)$, this density is asymptotic to $n \sec(\pi/n)/2\sqrt{k}$ as $k \to \infty$.

This result should be compared with the corresponding result for crosses. Let $h(k, n)$ be the order of the smallest abelian group G such that $F(k)$ n-packs G. Clearly $h(k, n) \ge 2kn + 1$, with equality if $n = 1$. As shown in **[St1]** for $n \ge 2$,

$$\lim_{k \to \infty} \frac{h(k, n)}{k^2} = 1.$$

Since the integer lattice packing density of the (k, n)-cross is $(2kn + 1)/h(k, n)$, this density is asymptotic to $2n/k$ as $k \to \infty$.

Throughout the remaining sections, $C(m)$ denotes the cyclic group of order m, Z/mZ.

1. Motivation. In [St1] it was shown that for any integer $b > 1$, $S(b^2 - b)$ 3-packs $C(b^3 + 1)$ with packing set $\{1, -b, (-b)^2\}$. Since $(-b)^3 = 1$ in $C(b^3 + 1)$, the packing set is a subgroup of the multiplicative structure of the ring $Z/[(b^3 + 1)Z]$. In these 3-packings, $k = b^2 - b$ and the order of the group is $b^3 + 1$, which is asymptotic to $k^{3/2}$ for large k.

This method also gives some information in the case of 4-packings and 6-packings. It can be shown that for an odd integer b greater than 1, $S((b^2 - 1)/2)$ 4-packs $C((b + 1)(b^2 + 1)/2)$. The packing set is the (multiplicative) subgroup $\{1, -b, (-b)^2, (-b)^3\}$, with $(-b)^4 = 1$ since $(b + 1)(b^2 + 1)/2$ divides $b^4 - 1$. Observe that, since $k = (b^2 - 1)/2$ and the order of the group is $(b + 1)(b^2 + 1)/2$, the order of the group is asymptotic to $\sqrt{2}\,k^{3/2}$.

Similarly, for $b \equiv 1 \pmod 6$ and greater than 1, $S((b^2 + b - 2)/3)$ 6-packs $C((b^2 + b + 1)(b + 1)/3)$ with packing set $\{1, -b, (-b)^2, (-b)^3, (-b)^4, (-b)^5\}$, again a group since $(-b)^6 = 1$. In this case, the order of the group is asymptotic to $\sqrt{3}\,k^{3/2}$.

In these cases the order m of the group is a polynomial of degree 3 in b and the number k is a polynomial of degree 2 in b. Since these polynomials have rational coefficients, $\lim_{b \to \infty} m^2/k^3$ is necessarily rational. However, according to Theorem 1, only in the cases $n = 3$, 4, and 6 is

$$\lim_{k \to \infty} \frac{g(k, n)^2}{k^3}$$

rational, since only for these $n \geq 3$ is $\cos^2 \pi/n$ rational.

To obtain Theorem 1, we will modify this approach. While we will still consider packing sets in cyclic groups of the form $\{1, -b, (-b)^2, \ldots, (-b)^{n-1}\}$, we do not demand that they form a subgroup, that is, that $(-b)^n = 1$. Our argument is motivated by a relation between pairs of elements in these packings. To express their relation we introduce the diagram in Fig. 1.1:

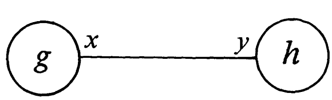

FIGURE 1.1

In this diagram g and h are elements in some abelian group and x and y are positive integers such that $xg + yh = 0$.

In the 3-, 4-, 6-packings mentioned earlier, the relations expressed by the three diagrams in Fig. 1.2 are valid:

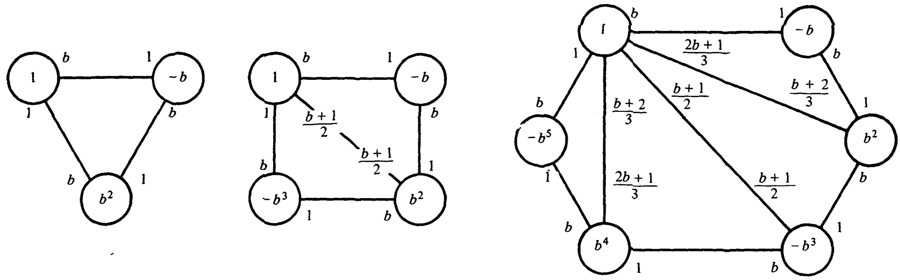

FIGURE 1.2

Along each edge $x = (1 - \alpha)b + \alpha$ and $y = \alpha b + (1 - \alpha)$ for some rational $\alpha \in [0, 1]$. (For $r = 3$, $\alpha = 0$ or 1; for $r = 4$, $\alpha = 0$, $1/2$, or 1; for $r = 6$, $\alpha = 0$, $1/3$, $1/2$, $2/3$, or 1.) Furthermore, in any triangle in Fig. 1.2 labelled as in Fig. 1.3, we have $xx'x'' + yy'y'' = m$, the order of the group.

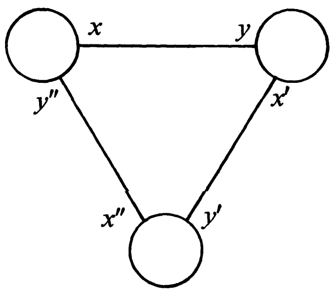

FIGURE 1.3

These observations suggest that we look for packings in cyclic groups of the form $\{(-b)^i \mid 0 \leq i \leq n - 1\}$ with the relations shown in Fig. 1.4, where $x_r = (1 - \alpha_r)b + \alpha_r$ and $y_r = \alpha_r b + (1 - \alpha_r)$. Moreover we demand the equality $xx'x'' + yy'y'' = m$ in each triangle.

FIGURE 1.4

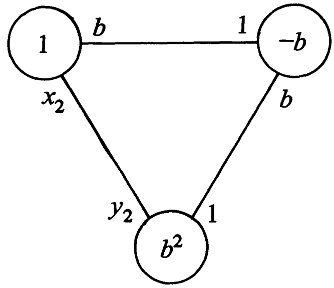

FIGURE 1.5

Note that $\alpha_1 = 0$. Denote α_2 by α. Then the triangle displayed in Fig. 1.5 gives $m = b^2(\alpha b + (1 - \alpha)) + ((1 - \alpha)b + \alpha)$, hence

$$m = (b + 1)\left(\alpha(b - 1)^2 + b\right).$$

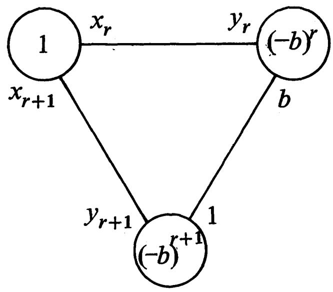

FIGURE 1.6

More generally, the triangle shown in Fig. 1.6 shows that

$$m = (b + 1)\left((1 - \alpha_r)\alpha_{r+1}(b - 1)^2 + b\right).$$

Thus $(1 - \alpha_r)\alpha_{r+1} = \alpha$, giving the recursion

$$\alpha_{r+1} = \frac{\alpha}{1 - \alpha_r},$$

which will play a central role in the argument.

With these observations in mind, the construction is straightforward: Solve the recursion, making sure that $0 \le \alpha_r \le 1$ for $1 \le r \le n - 1$, restrict b so that all x_r and y_r are integers, and then see how large k can be for that choice of b. The size of k is the substance of Lemma 2.1; note that since in the construction $x_r + y_r = b + 1$, k may be as large as $m/(b + 1) - 1 = \alpha(b - 1)^2 + b - 1$ so, for large b, $m/k^{3/2} \approx 1/\sqrt{\alpha}$.

The proof of Theorem 1 consists of two parts. First we construct for large k an n-packing for $S(k)$ in a cyclic group of order approximately $2\cos(\pi/n)k^{3/2}$. This will show that

$$\overline{\lim_{k\to\infty}} \frac{g(k,n)}{k^{3/2}} \leq 2\cos\pi/n,$$

which is Theorem 2. We then establish in Theorem 3 a lower bound for $g(k,n)$ which will imply that

$$\underline{\lim_{k\to\infty}} \frac{g(k,n)}{k^{3/2}} \geq 2\cos\pi/n.$$

Taken together, Theorems 2 and 3 yield Theorem 1.

2. A construction for group packings. We begin with the proofs of several lemmas. The first one gives a criterion for a 2-packing of $S(k)$ in $C(m)$. Its importance lies in the fact that a set $\{a_1,\ldots,a_n\}$ provides an n-packing for $S(k)$ if and only if every subset of two elements provides a 2-packing.

LEMMA 2.1. *Let m, x, and y be positive integers and let a and b be integers such that* $\gcd(a,b,m)=1$ *and* $xa\equiv -yb \pmod m$. *Let* $0<k<m/(x+y)$. *Then $S(k)$ 2-packs $C(m)$, with packing set $\{a,b\}$.*

Proof. Assume the contrary. Then we have $Xa\equiv Yb \pmod m$ for some integers X and Y, with $0\leq X,\ Y\leq k$ and not both 0. The congruences $xa\equiv -yb$ and $Xa\equiv Yb \pmod m$ imply the congruences $(Xy+Yx)a\equiv 0$ and $(Xy+Yx)b\equiv 0 \pmod m$. Since $\gcd(a,b,m)=1$, it follows that $Xy+Yx\equiv 0 \pmod m$. However,

$$0<Xy+Yx\leq ky+kx=k(x+y)<m,$$

a contradiction.

LEMMA 2.2. *Let $n\geq 3$ be an integer and let p and q be positive integers such that $p<q$ and* $\gcd(p,q)=1$. *Let $\alpha=p/q$. Define $\alpha_1=0$ and $\alpha_{r+1}=\alpha/(1-\alpha_r)$ for $r\geq 1$. Suppose $0\leq\alpha_r\leq 1$ for $1\leq r\leq n-1$. Write $\alpha_r=p_r/q_r$, where p_r and q_r are nonnegative integers with* $\gcd(p_r,q_r)=1$. *Suppose $b>1$ is an integer such that $b\equiv 1 \pmod L$ and* $\gcd(b,p)=1$ *where* $L=\operatorname{lcm}(q_1,q_2,\ldots,q_{n-1})$. *Let $m=(b+1)(\alpha(b-1)^2+b)$ and $k=\alpha(b-1)^2+b-1$. Then m and k are integers and $S(k)$ n-packs $C(m)$ with packing set $\{1,-b,(-b)^2,\ldots,(-b)^{n-1}\}$. Also*

$$\lim_{b\to\infty}\frac{m^2}{k^3}=\frac{1}{\alpha}.$$

(*Some examples of this construction are given after the proof of Theorem* 2.)

Proof. Note that $\alpha_2 = \alpha$, $p_2 = p$, and $q_2 = q$. By the definition of L, $b \equiv 1 \pmod{q}$. Thus

$$k = \frac{p}{q}(b-1)^2 + b - 1$$

is an integer. Since $m = (b+1)(k+1)$, m is also an integer.

We next show that $\gcd(b, m) = 1$. Assume that $d = \gcd(b, m)$ is greater than 1. Then d divides

$$m = (b+1)\left(\frac{p(b-1)^2}{q} + b\right)$$

but is relatively prime to $b + 1$ and $b - 1$. Thus d divides p, contradicting the assumption that $\gcd(b, p) = 1$.

Since $\gcd(b, m) = 1$, it follows that, for $0 \le e < f \le n - 1$, $\{(-b)^e, (-b)^f\}$ is a packing set if and only if $\{1, (-b)^{f-e}\}$ is. Thus it suffices to show that for $1 \le e \le n - 1$, $S(k)$ 2-packs $C(m)$ with packing set $\{1, (-b)^e\}$.

For $1 \le e \le n - 1$ let $x_e = \alpha_e + (1 - \alpha_e)b$ and $y_e = (1 - \alpha_e) + \alpha_e b$. Note that x_e and y_e are positive and that

$$x_e = b + \frac{p_e}{q_e}(1 - b)$$

is an integer since $b \equiv 1 \pmod{q_e}$. Also, $x_e + y_e = b + 1$, so y_e is an integer.

We will show inductively that m divides $x_e + y_e(-b)^e$. Consider $e = 1$. We have $x_1 = b$ and $y_1 = 1$, hence $x_1 + y_1(-b)^1 = 0$, which is divisible by m. This checks the assertion for $e = 1$.

Suppose the result holds for some $e < n - 1$. It may be shown by algebra that

$$x_{e+1} + y_{e+1}(-b)^{e+1} = \frac{1-(-b)^e}{1+b}m + \alpha_{e+1}(1-b)\left(x_e + y_e(-b)^e\right).$$

Note that $[1 - (-b)^e]/(1 + b)$ is an integer. Writing $\alpha_{e+1} = p_{e+1}/q_{e+1}$, we see that $\alpha_{e+1}(1 - b) = (p_{e+1}/q_{e+1})(1 - b)$ is an integer since q_{e+1} divides $b - 1$. Since m divides $x_e + y_e(-b)^e$ it follows that m divides $x_{e+1} + y_{e+1}(-b)^{e+1}$ and the induction is complete.

Since

$$0 < k = \frac{m}{b+1} - 1 < \frac{m}{b+1} = \frac{m}{x_e + y_e},$$

we may apply Lemma 2.1 with a, b, x, and y replaced by 1, $(-b)^e$, x_e, and y_e respectively. That lemma implies that $S(k)$ 2-packs $C(m)$ with packing set $\{1,(-b)^e\}$.

That

$$\lim_{b\to\infty}\frac{m^2}{k^3}=\frac{1}{\alpha}$$

is clear.

Note that the conditions $b \equiv 1 \pmod L$ and $\gcd(b,p)=1$ are satisfied for infinitely many b; just let $b \equiv 1 \pmod{pL}$. In fact, it can be shown by induction that $\gcd(p,L)=1$ and therefore for any integer a the simultaneous congruences $b \equiv a \pmod p$ and $b \equiv 1 \pmod L$ are solvable. Choosing a relatively prime to p forces b to be relatively prime to p.

LEMMA 2.3. *Let $n \geq 3$ be an integer and let $\alpha < 1$ be a positive rational number. Define $\alpha_1 = 0$ and $\alpha_{r+1} = \alpha/(1-\alpha_r)$ for $r \geq 1$. Suppose $0 \leq \alpha_r \leq 1$ for $1 \leq r \leq n-1$. Then for each positive integer k there is an integer $m(k)$ such that $S(k)$ n-packs $C(m(k))$ and*

$$\lim_{k\to\infty}\frac{(m(k))^2}{k^3}=\frac{1}{\alpha}.$$

Proof. Let k be a positive integer. Let k' and k'' be consecutive terms in the sequence of k's produced in Lemma 2.2, $k' < k \leq k''$. Let m' and m'' be the corresponding values in the sequence of m's. Then $S(k)$ n-packs $C(m'')$ and

$$\frac{(m'')^2}{k^3}=\left(\frac{k''}{k}\right)^3\frac{(m'')^2}{(k'')^3}.$$

by the construction in Lemma 2.2, $\lim_{k\to\infty}(k''/k')=1$ and $\lim_{k\to\infty}(m'')^2/(k'')^3=1/\alpha$. Letting $m(k)=m''$, the proof is complete.

LEMMA 2.4. *Let $\alpha > 1/4$, $\alpha_1 = 0$, and $\alpha_{r+1} = \alpha/(1-\alpha_r)$. Let $\theta = \cos^{-1}(1/(2\sqrt{\alpha}))$. Then for any positive integer $r < \pi/\theta$,*

$$\alpha_r=\sqrt{\alpha}\,\frac{\sin(r-1)\theta}{\sin r\theta}=1-\sqrt{\alpha}\,\frac{\sin(r+1)\theta}{\sin r\theta}.$$

The inductive proof is omitted.

LEMMA 2.5. *Let $n \geq 3$, $1/4 < \alpha \leq \frac{1}{4}\sec^2(\pi/n)$. Define α_r as in Lemma 2.4. Then $0 < \alpha_r < 1$ for $2 \leq r \leq n-2$ and $0 < \alpha_{n-1} \leq 1$.*

Proof. We have

$$1 > \frac{1}{2\sqrt{\alpha}} \geq \cos\frac{\pi}{n}.$$

Thus $\theta = \cos^{-1}(1/(2\sqrt{\alpha}))$ is less than or equal to π/n, or equivalently, $n \leq \pi/\theta$. By Lemma 2.4, $\alpha_r > 0$ for $r = 2, 3, \dots, n-1$ and $\alpha_r < 1$ for $2 \leq r \leq n-2$. Moreover $\alpha_{n-1} \leq 1$, with equality holding only if $\alpha = \frac{1}{4}\sec^2(\pi/n)$.

THEOREM 2. *For any integer* $n \geq 3$

$$\overline{\lim_{k\to\infty}} \frac{g(k,n)}{k^{3/2}} \leq 2\cos\frac{\pi}{n}.$$

Proof. Let $\varepsilon > 0$. Pick a rational number $\alpha > 1/4$ such that

$$4\cos^2\frac{\pi}{n} + \frac{\varepsilon}{2} > \frac{1}{\alpha} \geq 4\cos^2\frac{\pi}{n}.$$

Define α_r as above. Then, by Lemmas 2.3 and 2.5, for k suitably large,

$$\frac{g(k,n)^2}{k^3} < \frac{1}{\alpha} + \frac{\varepsilon}{2} < 4\cos^2\frac{\pi}{n} + \varepsilon.$$

Hence

$$\overline{\lim_{k\to\infty}} \frac{g(k,n)}{k^{3/2}} \leq 2\cos\frac{\pi}{n}, \text{ as claimed.}$$

We illustrate the construction for $n = 3, 4, 6$, and then 5. The first three cases coincide with the constructions given above.

For $n = 3$, $\frac{1}{4}\sec^2(\pi/n) = 1$, a rational number which we may take as α. We then have $\alpha_1 = 0$, $\alpha_2 = 1$, so $p = L = 1$. Thus b may be any integer > 1,

$$m = (b+1)\big((b-1)^2 + b\big) = (b+1)(b^2 - b + 1) = b^3 + 1$$

and

$$k = m/(b+1) - 1 = b^2 - b.$$

For $n = 4$, $\frac{1}{4}\sec^2(\pi/n) = 1/2$, a rational number which we may take as α. Then we have $\alpha_1 = 0$, $\alpha_2 = 1/2$, $\alpha_3 = 1$, so $p = 1$ and $L = 2$. Thus b must be odd. Moreover,

$$m = (b+1)\big(\tfrac{1}{2}(b-1)^2 + b\big) = (b+1)(b^2+1)/2$$

and $k = (b^2 - 1)/2$.

For $n = 6$, $\frac{1}{4}\sec^2(\pi/n) = 1/3$, which we may take as α. We have $\alpha_1 = 0$, $\alpha_2 = 1/3$, $\alpha_3 = 1/2$, $\alpha_4 = 2/3$, $\alpha_5 = 1$, so $p = 1$ and $L = 6$. Hence $b \equiv 1 \pmod 6$,

$$m = (b+1)(b^2+b+1)/3 \quad \text{and} \quad k = (b^2+b-2)/3.$$

In each of these cases $\frac{1}{4}\sec^2(\pi/n)$ is rational and so can be used as α. For other values of n this is not possible. Since

$$\cos^2\frac{\pi}{n} = \frac{1+\cos(2\pi/n)}{2},$$

we see that $(1/4)\sec^2(\pi/n)$ is rational if and only if $\cos(2\pi/n)$ is. But $\cos(2\pi/n)$, for $n \geq 3$, generates a field of degree $\varphi(n)/2$ over the rational field, so is rational only when $n = 3$, 4, or 6.

For other values of n, we must let α be a rational number less than $\frac{1}{4}\sec^2(\pi/n)$. For example, consider the case $n = 5$. We have $\frac{1}{4}\sec^2(\pi/5) = (3-\sqrt{5})/2$. We may choose any rational number less than $(3-\sqrt{5})/2 \approx 0.382$ but as close to it as we please to serve as α, say $\alpha = 3/8$. With this choice we have $\alpha_1 = 0$, $\alpha_2 = 3/8$, $\alpha_3 = 3/5$, and $\alpha_4 = 15/16$. Thus $p = 3$ and $L = 80$, so we choose $b \equiv 1$ or $161 \pmod{240}$. We have $m = (b+1)(3b^2+2b+3)/8$, $k = (3b^2+2b-5)/8$, and $\lim m^2/k^3 = 8/3$. Choosing $b = 241$ gives a 5-packing with $m^2/k^3 \approx 2.682$.

By choosing rational numbers closer to $\frac{1}{4}\sec^2(\pi/5)$ but less than it, we may produce 5-packings of $S(k)$ with m^2/k^3 as close as we please to $4\cos^2(\pi/5) = (3+\sqrt{5})/2$.

3. A lower bound on $g(k,n)$. We next develop a sequence of lemmas that will give a lower bound on $g(k,n)$ for $n \geq 3$. The approach makes use of the smallest positive integers x and y in diagrams of the type shown in Fig. 1.1. Let t be the largest of the sums $x + y$ for all pairs g and h in the packing sets that will be considered. On the one hand, it will be shown that $m \leq \frac{1}{4}t^3\sec^2(\pi/n)$, so $t \geq (4m)^{1/3}\cos^{2/3}(\pi/n)$. On the other hand, it will be shown that $m \geq (k+1)t - t^2/4$ and from this that $t \leq 2(k+1) - 2\sqrt{(k+1)^2 - m}$. Combining the two inequalities for t yields an inequality linking k and m from which Theorem 3 will follow.

LEMMA 3.1. *If* $m < (k+1)^2$ *and* $S(k)$ *2-packs an abelian group* G *of order* m *with packing set* $\{\alpha, \beta\}$, *then there are integers* x *and* y *such that* $1 \leq x, y \leq k$, $x\alpha + y\beta = 0$, *and* $m \geq (k+1)(x+y) - xy$.

Proof. Consider the $(k+1)^2$ elements $X\alpha + Y\beta$ in G with $0 \leq X, Y \leq k$. Since $|G| < (k+1)^2$, some two of these must be equal; say $X\alpha + Y\beta = X'\alpha + Y'\beta$ with $X \geq X'$. Then $(X - X')\alpha = (Y' - Y)\beta$, where $0 \leq X - X' \leq k$ and $-k \leq Y' - Y \leq k$. However, since $\{\alpha, \beta\}$ is a packing set for $S(k)$, we must have $1 \leq X - X' \leq k$ and $-k \leq Y' - Y \leq -1$. In other words, $(X - X')\alpha + (Y - Y')\beta = 0$ with $1 \leq X - X' \leq k$ and $1 \leq Y - Y' \leq k$. Pick integers x and y so that (x, y) is as close as possible to $(0,0)$ such that $x\alpha + y\beta = 0$, $1 \leq x \leq k$, and $1 \leq y \leq k$. We will show that $m \geq (k + 1)(x + y) - xy$.

Consider the elements $X\alpha + Y\beta$ with $0 \leq X, Y \leq k$ and either $X < x$ or $Y < y$. There are $(k + 1)(x + y) - xy$ such elements; we claim that they are distinct.

For suppose two are equal, say $X\alpha + Y\beta = X'\alpha + Y'\beta$ with $X \geq X'$. As before, $1 \leq X - X', Y - Y' \leq k$ and $(X - X')\alpha + (Y - Y')\beta = 0$. Furthermore, either $X < x$ or $Y < y$, so either $X - X' < x$ or $Y - Y' < y$. If both inequalities hold, then $(X - X', Y - Y')$ contradicts the choice of (x, y). So assume, without loss of generality, that $X - X' < x$ and $Y - Y' \geq y$. Then $(x - (X - X'))\alpha = ((Y - Y') - y)\beta$; $1 \leq x - (X - X') \leq k$ and $0 \leq (Y - Y') - y \leq k - y < k$, contradicting the fact that $\{\alpha, \beta\}$ is a packing set for $S(k)$. Hence the $(k + 1)(x + y) - xy$ elements are distinct, implying that $m \geq (k + 1)(x + y) - xy$.

LEMMA 3.2. *Assume that $\{\alpha, \beta, \gamma\}$ is a packing set for $S(k)$ in a group G of order $m < 2(k + 1)^{3/2}$. Then $\{\alpha, \beta, \gamma\}$ generates G.*

Proof. Let H be the subgroup of G generated by $\{\alpha, \beta, \gamma\}$. As was shown in **[St1]**, $(k + 1)^3 \leq |H|^2$. If H is a proper subgroup of G, $|H| \leq |G|/2$. Thus

$$(k + 1)^3 \leq \frac{m^2}{4}$$

so $m \geq 2(k + 1)^{3/2}$. This contradiction establishes the lemma.

Let α, β, γ be nonzero elements in $C(p)$ for some prime p. Assume that a, a', b, b', c, c' are integers not divisible by p such that

$$a\beta + a'\gamma = b\gamma + b'\alpha = c\alpha + c'\beta = 0.$$

Then, in the field $\mathrm{GF}(p)$ we have

$$\frac{a}{a'} = -\frac{\gamma}{\beta}, \frac{b}{b'} = -\frac{\alpha}{\gamma}, \frac{c}{c'} = -\frac{\beta}{\alpha}.$$

Thus, in $\mathrm{GF}(p)$,

$$\frac{a}{a'}\frac{b}{b'}\frac{c}{c'} = -1 \quad \text{so } abc + a'b'c' = 0.$$

That is, $p | abc + a'b'c'$. The next lemma generalizes this fact to all finite abelian groups.

LEMMA 3.3. *Let G be a finite abelian group of order m. Let α, β, and γ generate G and let a, b, c, a', b', c' be integers such that*

$$a\beta + a'\gamma = b\gamma + b'\alpha = c\alpha + c'\beta = 0;$$

as in Fig. 3.1.

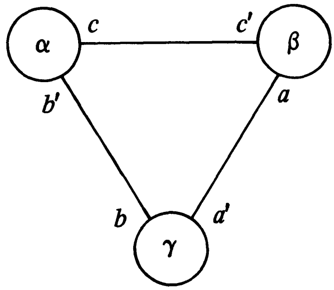

FIGURE 3.1

Then

$$m | abc + a'b'c'.$$

Proof. Consider the Z-lattice in R^3,

$$L = \{(x, y, z) | x\alpha + y\beta + z\gamma = 0\}.$$

Since α, β, γ generate G, $Z^3/L \simeq G$, and thus $|Z^3/L| = m$. Let K be the lattice generated by $(0, a, a')$, $(b', 0, b)$, $(c, c', 0)$. The determinant

$$\begin{vmatrix} 0 & a & a' \\ b' & 0 & b \\ c & c' & 0 \end{vmatrix}$$

is equal to $abc + a'b'c'$. Since K is a sublattice of L, $|Z^3 \colon L|$ divides $|Z^3 \colon K|$. That is, m divides $abc + a'b'c'$, which was to be proved.

We now begin the proof of Theorem 3, which will incorporate further lemmas at the appropriate points in the argument.

THEOREM 3. *If $n \geq 3$, $k \geq 1$, $m \geq 1$, and $S(k)$ n-packs an abelian group of order m, then*

$$k + 1 \leq \left(4\cos^2\frac{\pi}{n}\right)^{-1/3} m^{2/3} + \frac{1}{4}\left(4\cos^2\frac{\pi}{n}\right)^{1/3} m^{1/3}.$$

Proof. Suppose not. Then

$$k + 1 > \left(x + \frac{1}{4x}\right)\sqrt{m} \quad \text{where } x = \left(4\cos^2\frac{\pi}{n}\right)^{-1/3} m^{1/6}.$$

But $x + 1/4x \geq 1$ for $x > 0$, so $m < (k+1)^2$.

Let the packing set be $\{g_0, \ldots, g_{n-1}\}$. Let $K = k + 1$. By Lemma 3.1, for $i \neq j$, there are integers a_{ij} with $1 \leq a_{ij} \leq k$, $a_{ij}g_i + a_{ji}g_j = 0$, and $m \geq K(a_{ij} + a_{ji}) - a_{ij}a_{ji}$.

LEMMA 3.4. *Let m, K, a, a' be positive real numbers such that a, $a' \leq K$ and $K^2 \geq m \geq K(a + a') - aa'$. Let $t = a + a'$. Then $t \leq 2K - 2\sqrt{K^2 - m}$.*

Proof. We have $m \geq Kt - aa'$. Since $a + a' = t$, the largest possible value of aa' is $t^2/4$. Hence $m \geq Kt - t^2/4$ so $t^2 - 4Kt \geq -4m$. Completing the square shows that $(2K - t)^2 \geq 4K^2 - 4m$ and, since $2K - t \geq 0$, $2K - t \geq \sqrt{4K^2 - 4m}$, from which the lemma follows.

Proof of Theorem 3 *continued*. Let $t = \max_{0 \leq i < j \leq n-1}(a_{ij} + a_{ji})$. By Lemma 3.4, $t \leq 2K - 2\sqrt{K^2 - m}$.

Note that

$$K > \left(4\cos^2\frac{\pi}{n}\right)^{-1/3} m^{2/3} + \frac{1}{4}\left(4\cos^2\frac{\pi}{n}\right)^{1/3} m^{1/3} > \left(\frac{m}{2}\right)^{2/3}$$

so $m < 2K^{3/2}$. By Lemma 3.2, if i, j, and l are distinct indices between 0 and $n - 1$, then $\{g_i, g_j, g_l\}$ generates G. By Lemma 3.3, $m | a_{ij}a_{jl}a_{li} + a_{ji}a_{lj}a_{il}$ so $m \leq a_{ij}a_{jl}a_{li} + a_{ji}a_{lj}a_{il}$.

Let $b_{ij} = a_{ij}/t$. Then we have $b_{ij} \geq 0$, $b_{ij} + b_{ji} \leq 1$, and $m \leq t^3(b_{ij}b_{jl}b_{li} + b_{ji}b_{lj}b_{il})$. The next two lemmas will allow us to derive a relationship between m, t, and n from these inequalities.

LEMMA 3.5. *Let n be an integer ≥ 3. Let x_1, $x_2, \ldots, x_{n-1}$ be real numbers, $0 \leq x_i \leq 1$. Then there are distinct indices j and l such that*

$$x_j(1 - x_l) \quad \textit{and} \quad x_l(1 - x_j)$$

are both less than or equal to $\frac{1}{4}\sec^2(\pi/n)$. This is best possible in the sense that $\frac{1}{4}\sec^2(\pi/n)$ cannot be replaced by a smaller number.

Proof. Let $\alpha = \frac{1}{4}\sec^2(\pi/n)$, $\alpha_1 = 0$ and $\alpha_{i+1} = \alpha/(1 - \alpha_i)$. By Lemmas 2.4 and 2.5, $0 = \alpha_1 < \alpha_2 < \cdots < \alpha_{n-1} = 1$, and the interval $[0, 1]$ is partitioned into $n - 2$ sections, $[\alpha_1, \alpha_2]$, $[\alpha_2, \alpha_3], \ldots, [\alpha_{n-2}, \alpha_{n-1}]$. Hence some section, say $[\alpha_p, \alpha_{p+1}]$, contains a pair x_j and x_l, $l \neq j$. We then have

$$x_j(1 - x_l) \leq \alpha_{p+1}(1 - \alpha_p) = \alpha$$

and

$$x_l(1 - x_j) \le \alpha_{p+1}(1 - \alpha_p) = \alpha.$$

To show that this result is best possible, consider the sequence $x_i = \alpha_i$, $i = 1, 2, \ldots, n-1$. Note that $x_{i+1}(1 - x_i) = \alpha$. Thus, if $j > i$, $x_j(1 - x_i) \ge \alpha$. Hence, if $j \ne l$ at least one of $x_j(1 - x_l)$ and $x_l(1 - x_j)$ is $\ge \alpha = \frac{1}{4}\sec^2(\pi/n)$.

LEMMA 3.6. *Let n be an integer ≥ 3. For $0 \le i$, $j \le r - 1$, $i \ne j$, let b_{ij} be nonnegative real numbers such that $b_{ij} + b_{ji} \le 1$. Then for some j and l, $0 < j < l \le r - 1$,*

$$b_{0j}b_{jl}b_{l0} + b_{j0}b_{lj}b_{0l} \le \tfrac{1}{4}\sec^2\frac{\pi}{n}.$$

Proof. Let $x_i = b_{0i}$, $i = 1, 2, \ldots, n-1$. By Lemma 3.5, there are distinct indices j and l such that $x_j(1 - x_l)$ and $x_l(1 - x_j)$ are both $\le \frac{1}{4}\sec^2(\pi/n)$. Then

$$\begin{aligned} b_{0j}b_{jl}b_{l0} + b_{j0}b_{lj}b_{0l} &\le (b_{jl} + b_{lj})\max(b_{0j}b_{l0}, b_{j0}b_{0l}) \\ &\le 1 \cdot \max\big(b_{0j}(1 - b_{0l}), b_{0l}(1 - b_{0j})\big) \le \tfrac{1}{4}\sec^2(\pi/n). \end{aligned}$$

Proof of Theorem 3 *continued.* By Lemma 3.6 we have $m \le (t^3/4)\sec^2(\pi/n)$ so $t \ge (4\cos^2(\pi/n))^{1/3}m^{1/3}$. Combining this with the inequality $t \le 2K - 2\sqrt{K^2 - m}$ proved above, we obtain $C \le 2K - 2\sqrt{K^2 - m}$, where $C = (4\cos^2(\pi/n))^{1/3}m^{1/3}$. Hence $2\sqrt{K^2 - m} \le 2K - C$. Squaring and simplifying gives $K \le m/C + C/4$ from which Theorem 3 follows.

For $n \ge 3$, Theorem 3 implies that

$$\varliminf_{k \to \infty} \frac{g(k, n)}{k^{3/2}} \ge 2\cos\frac{\pi}{n}.$$

Combining this with Theorem 2 completes the proof of Theorem 1.

4. Some questions. For $n = 3$ and 4 a stronger version of Theorem 3 holds, namely $k + 1 \le (4\cos^2(\pi/n))^{-1/3}m^{2/3}$. The case $n = 3$ is treated in **[St1]** and the case $n = 4$ by Hickerson through a method that does not seem to generalize to larger values of n. These facts suggest two questions.

Let $n \ge 3$ and $k \ge 1$. Is $g(k, n)/(k + 1)^{3/2} \ge 2\cos(\pi/n)$?

For $n \ge 3$ what is the exact value of $g(k, n)$?

The cases $n = 3$, 4, and 6 also suggest the following question:

Let $g'(k, n)$ be the smallest value of m for which $S(k)$ n-packs $C(m)$ with a packing set which is a multiplicative subgroup of the ring of integers mod m. What is $\lim_{k\to\infty}(g'(k,n)/k^{3/2})$? Even for $n = 5$ the answer is not known.

See **[St2]** for further information about $g(k,n)$ and a discussion of related problems.

References

[St 1] S. Stein, *Packing of R^n by certain error spheres*, IEEE Trans. Information Theory, IT-30, (1984) 356–363.

[St 2] _____, *Tiling, packing, and covering by clusters*, (a survey, to appear in Rocky Mountain Journal of Mathematics).

Received June 14, 1984.

University of California
Davis, CA 95616

Pacific Journal of Mathematics

Vol. 122, No. 1 January, 1986