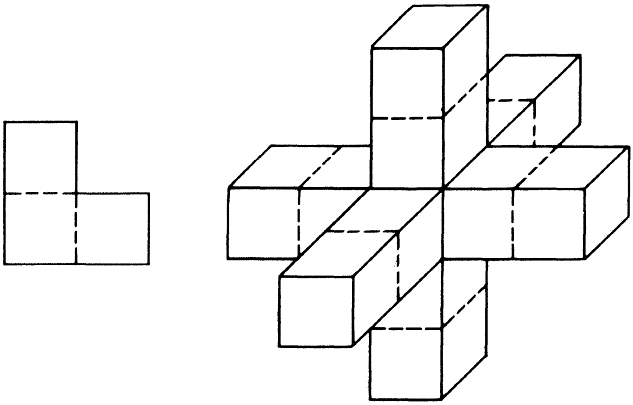
ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 16, Number 2, Spring 1986

TILING, PACKING, AND COVERING BY CLUSTERS

SHERMAN STEIN

The theory of packing, covering, and tiling by translates of a convex set or by a star body grew mainly out of Minkowski's work in the geometry of numbers. More recently, Bambah, Davenport, Mahler, Mordell, Rogers, and others have pursued questions in this area for their intrinsic geometric interest. (See Gruber's survey **[16]** for a review of the results and open problems.) Sometimes a star body which is of no particular intrinsic interest is ingeniously constructed to provide an example confirming or refuting a conjecture. One of the objectives of this survey is to present a family of star bodies which in the past twenty years have been the object of varied investigations on their own right, have suggested new geometric, algebraic, and combinatorial questions and provided a rich and convenient source of examples.

These star bodies are the cross and semicross. For a nonnegative real number k and a positive integer n, the (k, n)-cross in Euclidean n-space,



(1,2)-semicross (2,3)-cross

FIGURE 1

AMS Classification 05 B 30, 40, 45, 20D 60, 52A 43.

Received by the editors on October 12, 1982 and in revised form on October 15, 1984.

Copyright © 1986 Rocky Mountain Mathematics Consortium

$\mathbf{R}^n$, consists of a unit cube together with $2n$ arms of length k attached at each of the $2n$ facets. (Its volume is $2kn + 1$.) The (k, n)-semicross is formed similarly; it consists of a unit cube together with n arms of length k attached at non-opposite facets. In $\mathbf{R}^3$ it forms a tripod. Figure 1 shows the (1, 2)-semicross and the (2, 3)-cross.

Because of their simplicity, especially when k is an integer, the cross and semicross are accessible by various approaches. The following three theorems illustrate some of the significant results already obtained. (The terms "tiles", "lattice", "packing", and "covering" are defined in §I.)

1. *The* (4, 10)-*cross tiles* $\mathbf{R}^{10}$ *but not in a lattice manner.*

This is the first star body with this property found in any dimension. See [**44**] and the review by Bambah [**2**]. Later, Szabó in [**51**] showed that the (3/2, 5)-cross has the same property.

2. *Translates of the* (2, 2)-*cross cover the plane less densely than does any lattice family of its translates.*

It is easy to construct a non-lattice covering of the plane by translates of the (2, 2)-cross with density 9/8. (Loomis in [**28**] showed that the covering constant of the (2, 2)-cross is in fact 9/8.) However, Rooney [**40**] has shown that any lattice covering by translates of the (2, 2)-cross has density at least 9/7. This example may be contrasted with the star body constructed in [**3**], which has the same property but is much more complicated.

3. *When k is large, arbitrary translates of the* $(k, 3)$-*semicross pack* R^3 *much more densely than does any lattice-family of translates.*

More precisely,

$$\lim_{k\to\infty} \frac{\text{lattice packing density of } (k, 3)\text{-semicross}}{\text{packing density of } (k, 3)\text{-semicross}} = 0.$$

(The corresponding limit for the $(k, 3)$-cross is 1.) This contrasts with the theorem of Rogers [**38**] which asserts that, for a plane convex body, the lattice-packing density equals the packing density. It will be compared in §IV to an example of Davenport and Rogers [**7**], as interpreted by Groemer [**15**], which concerns the relation of a star body to lattices and to general point sets.

These three results suggest that in questions about star bodies the cross and semicross should be kept well in mind.

This survey is devoted mainly to known results due to Everett, Galovich, Hamaker, Hickerson, Loomis, Newman, Stein, and Szabó. It also includes some unpublished work of Hickerson and some questions and results that suggest lines of further investigation. Some of these questions might be quite easy, but some, such as I-3, we expect will offer a substantial challenge.

We begin with a discussion of objects called "clusters", which are unions of a finite number of cubes from the standard lattice of cubes, and then, as the outline indicates, consider the cross and semicross, which are special clusters and which motivate the remaining sections. §II is geometric and §III, §IV, and §V are algebraic.

I. Clusters. We begin with a few definitions, present some theorems about families of clusters, and conclude with a discussion of what is known about clusters in $\mathbf{R}^1$, the real line.

A. *Definitions.* Let $\mathbf{Z}$ denote the set of integers as well as the ring and additive group of integers. Let n be a positive integer. With each element $(x_1, x_2, \ldots, x_n) \in \mathbf{Z}^n$ associate a unit cube in $\mathbf{R}^n$ with edges parallel to the coordinate axes, namely the cube, $\{(y_1, y_2, \ldots, y_n) | y_i \in \mathbf{R},\ x_i \leqq y_i \leqq x_i + 1\}$. The cube is therefore recorded by its vertex with smallest coordinates. If the x_i are integers, it is called a standard cube. A cluster K is the finite union of some of these cubes.

Let A be a discrete set of points in $\mathbf{R}^n$, that is, a set without limit points. For convenience we will also speak of the points in A as vectors. For $v \in A$, let $v + K = \{v + x | x \in K\}$, which is called a translate of K by the vector v. If the union of the sets $v + K$, for $v \in A$, is $\mathbf{R}^n$, we say that the family of translates covers $\mathbf{R}^n$. Note that the coordinates of the vectors v need not be integers.

Let int K denote the interior of K. Let A again be a discrete set of vectors. If, for any pair of distinct elements v and v' in A, $(v + \text{int } K) \cap (v' + \text{int } K) = \emptyset$, then the family of translates $\{v + K | v \in A\}$ is called a packing of $\mathbf{R}^n$. A family of translates that is both a covering and a packing is called a tiling of $\mathbf{R}^n$. If there is such a family, K is said to tile $\mathbf{R}^n$.

Observe that we are considering only translates of K. For this reason we will not include recent work, such as that of Barnes [5, 6], which permits more general motions.

The density of a discrete set A is defined as follows. For a positive real number s, let $Q(s)$ be the cube $\{(x_1, x_2, \ldots, x_n) \mid |x_i| \leqq s\}$, which has volume $(2s)^n$. Let $I(s)$ be the number of elements of A that lie in $Q(s)$. If

$$\lim_{s \to \infty} \frac{I(s)}{(2s)^n}$$

exists, it is called the density of A. If K is a cluster with volume $v(K)$ and A has density d, the family of translates $\{v + K | v \in A\}$ is said to have density $dv(K)$. In the case of a packing this can be thought of as the fraction of space occupied by the translates. In the case of a covering this quantity is at least 1 and records the average number of times a typical point in space is covered by translates of K.

The packing constant of K, denoted $\delta(K)$, is defined as the supremum of the densities of all packings by K that have densities. ("Packing by K" is short for "packing by translates of K".) It is not hard to show that there is a packing by K which has the density $\delta(K)$. The covering constant of K, denoted $\theta(K)$, is defined as the infimum of the densities of all coverings by K that have densities. There is a covering with density $\theta(K)$.

It follows by a technique introduced in [29] that if K consists of k cubes, then $\theta(K) \leqq 1 + 1/2 + \cdots + 1/k$, hence is at most $1 + \log k$. (See also [33], [46], [21], [22].) This estimate is asymptotically the best possible result, as shown in [33].

Let $v_1, v_2, \ldots, v_n$ be n linearly independent vectors in $\mathbf{R}^n$. The set

$$\Lambda = \{x_1v_1 + x_2v_2 + \cdots + x_nv_n | x_i \in Z\}$$

is called a lattice. A set $S \subseteq \mathbf{R}^n$ is a lattice if and only if it is a discrete subgroup of $\mathbf{R}^n$ and does not lie in any $(n - 1)$-dimensional plane. The vectors $v_1, v_2, \ldots, v_n$ are the edges of a fundamental parallelepiped of Λ with volume equal to $|\det(v_1, v_2, \ldots, v_n)|$. This volume, which is positive, is the same for all choices of bases for the lattice and is called the determinant of the lattice, denoted $\det(\Lambda)$. The cube $Q(s)$ mentioned earlier contains, when s is large, approximately $(2s)^n/\det(\Lambda)$ points of Λ. In other words, the density of Λ is the same as the reciprocal of its determinant. Thus the density of a family of translates of K by Λ is

$$\frac{\text{volume of } K}{\det(\Lambda)}.$$

In case the family of translates of K by Λ is a packing we call it a lattice packing. Similarly, we speak of a lattice covering and a lattice tiling.

Minkowski noticed that a lattice packing by K can be described in quite a different manner. Assume that the family $\{v + K | v \in \Lambda\}$ forms a packing. Then if

$$v_1 + k_1 = v_2 + k_2, \qquad v_1, v_2 \in \Lambda, k_1, k_2 \in \text{int } K,$$

we have

$$v_1 = v_2 \text{ and } k_1 = k_2.$$

Thus $v_1 - v_2 = k_2 - k_1$ implies that $v_1 - v_2 = 0$. Introduce the difference body of the interior of K, (denoted "int K"),

$$\text{int } K - \text{int } K = \{k_2 - k_1 | k_2, k_1 \in \text{int } K\}$$

(If K is convex and centrally symmetric, $K - K = 2K$, which is homothetic to K. This is not the case when K is just a star body.) Thus the translates of K by the lattice Λ form a packing if and only if the intersection of Λ with int K − int K consists only of the origin. Such a lattice is called an admissible lattice for int K − int K. The problem of determining how dense a lattice packing by K can be is equivalent, therefore, to determining how small the determinant of an admissible lattice of int K − int K can be.

The notion of an admissible lattice generalizes to sets that are not necessarily difference bodies. If S is a star body containing the origin in its interior, a lattice Λ is admissible for S if the origin is the only point of Λ that lies in the interior of S. Since Λ is centrally symmetric, it is no loss of generality to assume that S is as well. (Otherwise, replace S by $S \cup (-S)$. For a set X in $\mathbf{R}^n$, $-X$ is $\{-x | x \in X\}$.) The minimal determinant of admissible lattices for S is called the critical number of S.

The notion of an admissible lattice generalizes to that of an admissible set. A set C is admissible for the star body S containing the origin in its interior if, for each $c \in C$, the interior of the translate $c + S$ contains no other element of C than c. In particular, it is easy to show that a set C is admissible for a difference body $K - K$ if and only if the family of translates of K by C is a packing.

Packing families can be looked at another way. Again, let S be a star body. Assume that the family $\{v + S | v \in C\}$ is a packing. Then the interior of any translate of S, $x + S$, contains at most one member of $-C$. For if $x + s_1 = -c_1$ and $x + s_2 = -c_2$, it follows that $c_2 + s_2 = c_1 + s_1$, and therefore $c_1 = c_2$. The converse holds. Let C be a set such that each translate of int K contains at most one element of $-C$. Assume that $(c_1 + \text{int } S) \cap (c_2 + \text{int } S) \neq \emptyset$. Then there are $s_1, s_2 \in \text{int } S$ and $c_1, c_2 \in C$ such that $c_1 + s_1 = c_2 + s_2$ or $c_1 = c_2 + s_2 - s_1$. The translate of int S by $c_2 - s_1$ contains both c_1 and c_2, in violation of the assumption on C.

Covering families can also be described in terms of "blocking sets". A set B in R^n is a blocking set for the set K if every translate of K contains at least one element of B. It is easy to check that this is equivalent to the assertion that the set of translates of $-K$ by B is a covering. How sparse a blocking set K can have determines how sparsely translates of K can cover.

For a cluster K the lattice-packing constant $\delta_\Lambda(K)$ and the lattice-covering constant $\theta_\Lambda(K)$ are defined as follows.

The lattice-packing constant is

$$\delta_\Lambda(K) = \sup \frac{\text{volume of } K}{\det \Lambda},$$

for all lattices Λ such that translates of K by Λ form a packing. The lattice-covering constant is

$$\theta_\Lambda(K) = \inf \frac{\text{volume of } K}{\det \Lambda},$$

for all lattices Λ such that the translates of K by Λ form a covering. It is known that, for each compact star body K, the bounds $\delta_\Lambda(K)$ and $\theta_\Lambda(K)$ are assumed by some lattices.

In **[58]** vonWolff constructed a star body in $\mathbf{R}^2$ for which its densest admissible set is denser than its densest admissible lattice. Groemer **[15]** observed that a construction of Davenport and Rogers [7], made for another purpose, can be used to answer a more demanding question. For each positive integer m is there a star body $S(m)$ such that

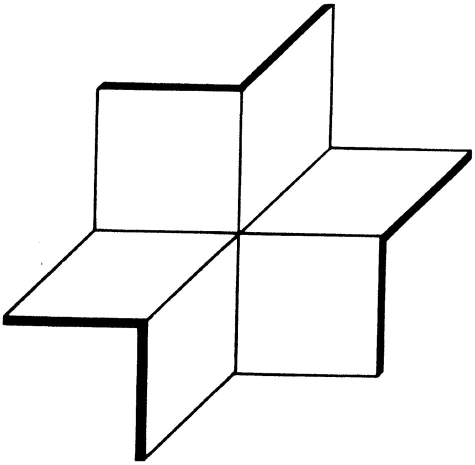
$$\text{(I-1)} \qquad \frac{\text{density of densest admissible point set for } S(m)}{\text{density of densest admissible lattice for } S(m)} < \frac{1}{m}$$

The rather complicated example to show that the answer is "yes" is constructed in $\mathbf{R}^2$. A much simpler example, in $\mathbf{R}^3$, can be based on the $(k, 3)$-semicross. Let s_k be the $(k, 3)$-semicross and K_k its difference body, $s_k - s_k$. K_k is composed of six rectangular parallelepipeds (of sides 2 by $k + 1$ by $k + 1$) that intersect in a cube of width 2, as shown in Figure I-1. It was shown in **[47]** that

$$\lim_{k\to\infty} \frac{\delta_\Lambda(s_k)}{\delta(s_k)} = 0.$$

Hence, K_k, for k suitably large, will serve as an $S(m)$ in (I-1).

Up to this point the coordinates of the translating vectors have been any real numbers. We will consider cases where all these coordinates are rational or all are integers. If they are all rational, we will speak of a **Q**-packing, **Q**-covering, or **Q**-tiling. If, furthermore, the vectors form a lattice, we will speak of a **Q**-lattice packing, etc. In case they are integers, we will speak of a **Z**-packing, or **Z**-lattice packing, and so on.



Difference body of semicross, $s_k - s_k$
FIGURE I–1

A set of translating vectors may exhibit a periodicity without necessarily forming a lattice. Let Λ be a lattice and let $h_1, h_2, \ldots, h_r$ be a finite number of vectors in $\mathbf{R}^n$ such that $h_i + \Lambda$ and $h_j + \Lambda$ are disjoint if $i \neq j$. The union of the sets, $h_1 + \Lambda$, $h_2 + \Lambda$, . . . , $h_r + \Lambda$ is called a periodic set. (It has also been called a "lattice with a base" by Zassenhaus [**59**] and others. See also [**45**, p. 455].) Rogers [**39**, p. 25] used the same term, "periodic", but restricted Λ to be a lattice generated by the special vectors $(s, 0, \ldots, 0), (0, s, \ldots, 0), \ldots, (0, \ldots, 0, s)$, for some positive real number s.

Consider a family of translates of K that pack with density $\delta(K)$. Let ε be a positive number. Select a large cube $Q(s)$ such that the set of translates of K that lie in that cube pack at least $\delta(K) - \varepsilon$ times the volume of cube. From this fact it follows readily that there is a periodic packing by K with density at least $\delta(K) - \varepsilon$. This implies that the supremum of packing densities by translates of K by periodic families is equal to $\delta(K)$. It is no surprise that the constructions of packings that are denser than any lattice packing use periodic packings.

Multiple packings, multiple coverings, or multiple tilings can also be defined. However, the only cluster for which any of these have been examined is the unit cube. Multiple tilings by the cube were studied by Hajós [**17**], Robinson [**37**], and Szabó [**52**] in a series of papers growing out of the affirmative answer to a conjecture of Minkowski; i.e., in a lattice tiling of $\mathbf{R}^n$ by a unit cube, some two of the translates share a complete $n - 1$ dimensional facet. (Hence the tiling is a union of infinite tubes.)

We shall not consider multiple tilings, except to observe that, for a cluster that consists of k units cubes, there is a k-fold tiling, consisting of all the translates by vectors with integer coordinates.

We restrict our attention to translates of a single cluster. It turns out that the problem of determining whether translates of a finite set of clusters tile the plane is recursively unsolvable. (See [1] or [36] for instance.) Whether this is true for the family of congruent copies of a single cluster is not known.

B. *The shift theorem.* Hajós [17], in his work on lattice tiling by cubes, replaced a lattice tiling by a **Q**-lattice tiling. This reduction works for clusters as well, and we will sketch the argument behind it.

THEOREM I-1. *If there is a lattice tiling by the cluster K, then there is a* **Q**-*lattice tiling by K.*

The reasoning goes as follows. Consider a coordinate axis, say the first, x_1, for which not all of the vectors in the lattice Λ have a rational entry. On Λ introduce the equivalence relation $v \sim v'$ if the first coordinate of $v - v'$ is rational. Let W be the equivalence class containing the origin, that is, the elements of Λ with rational first coordinate. W is a discrete subgroup of Λ. Observe that the union, B, of the family $\{w + K | w \in W\}$ is a cylinder with the x_1-axis as generator.

Let $w_1, w_2, \ldots, w_r$ be a basis for W in the sense that each element in W is a unique linear combination $z_1w_1 + z_2w_2 + \cdots + z_rw_r$, $z_i \in \mathbf{Z}$. Extend $w_1, w_2, \ldots, w_r$ to a basis for Λ. This is possible, since any element v of Λ that lies in the vector space spanned by $w_1, w_2, \ldots, w_r$ is already in W. (Otherwise, since the x_1-coordinate of v is irrational, the elements v, $2v$, $3v, \ldots$ are incongruent modulo W. Each is equivalent to a unique element in the fundamental parallelepiped determined by $w_1, w_2, \ldots, w_r$, and these elements are distinct from each other. This contradicts the assumption that the set Λ has no limit points.)

Let $w_1, w_2, \ldots, w_r, w_{r+1}, \ldots, w_n$, be this new basis of Λ. The first coordinate of w_{r+1} is irrational. Let e_{r+1} be the vector $(0, \ldots 0, 1, 0 \ldots, 0)$, 0's everywhere except at the $(r + 1)$st coordinate. Let $w'_{r+1} = w_r + te_{r+1}$, where t is any real number chosen to make the $(r + 1)$st coordinate of w'_{r+1} rational. Let Λ' be the lattice with basis $w_1, \ldots, w_r, w'_{r+1}, w_{r+2}, \ldots, w_n$. Because the translates of K by W form a prism parallel to x_1 axis, it follows that the translates of K by Λ' still form a tiling.

This procedure may be repeated step by step with the remaining vectors $w_{r+2}, \ldots, w_n$ to produce a basis for a lattice Λ'' in which all vectors have a rational x_1-coordinate and translates of K by Λ'' tile.

Beginning with this lattice, treat the x_2-coordinate in the same manner, then the x_3-coordinate, and so on, finally producing a lattice with only rational coordinates and such that translates of K by vectors in this lattice still tile. This completes the argument.

It is not the case that a cluster that **Q**-lattice tiles necessarily **Z**-lattice tiles. As Hickerson pointed out in [**23**], the cluster consisting of two squares in the plane, separated horizontally by one square, **Q**-lattice tiles the plane by the lattice with basis (1, 1/2) and (4, 0) buts does not **Z**-lattice tile the plane.

However, Everett and Hickerson in [**8**] showed that, for some purposes, there is no loss of generality in assuming that the translation vectors of a cluster have only integer coordinates. Their shift theorem asserts that if you move each cube in each cluster of a packing slightly to coincide with a standard cube, the new set of translates still forms a packing. The shift amounts to the n-dimensional analog of "rounding down to the nearest integer". In the following statement of the shift theorem, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x.

THEOREM I-2. (The Shift Theorem). *Let K be a cluster and Λ be a discrete set of vectors in $\mathbf{R}^n$. For each vector $v = (x_1, x_2, \ldots, x_n) \in \Lambda$ let $v^* = (\lfloor x_1 \rfloor, \lfloor x_2 \rfloor, \ldots, \lfloor x_n \rfloor)$. Let $\Lambda^* = \{v^* | v \in \Lambda\}$. Then, if the family of translates of K by Λ is a packing* (*covering, tiling*), *the family of translates of K by Λ^* is also a packing* (*covering, tiling*). *In the case of packings the shift is one-to-one, and if Λ has a density, so does Λ^* and the two densities are equal.*

However, the shift does not preserve the notion of a lattice. That is, the shift of a lattice is not necessarily a lattice. In fact, it almost never is. We can see this in two ways. First, let Λ be a lattice in $\mathbf{R}^n$ with non-integral determinant. Recall that the number of elements of Λ in a large cube is asymptotic to the quotient, Volume of cube/det Λ. If the shift of Λ, Λ^*, were a lattice, then det Λ^* would be an integer, hence not equal to det Λ. But the number of elements of Λ^* in a large cube would be asymptotic to the number of elements of Λ in a large cube, since the shift moves no point more than the fixed distance $\sqrt{n}$.

Second, let Λ be a lattice in $\mathbf{R}^n$ which has only the origin in the cube $0 \leqq x_i \leqq 2$, $1 \leqq \mathrm{i} \leqq n$. Assume that there is a point $P = (a_1, a_2, \ldots, a_n) \in \Lambda$ with positive coordinates not all of which are integers. The shift of P is $(\lfloor a_1 \rfloor, \lfloor a_2 \rfloor, \ldots, \lfloor a_n \rfloor)$ and the i^{th} coordinate of the shift of $-P$ is $-\lfloor a_i \rfloor - 1$ if $a_i \notin \mathbf{Z}$ and $-\lfloor a_i \rfloor$ if $a_i \in \mathbf{Z}$. If the shift, Λ^*, were a lattice, then -(shift of P + shift of $-P$) would be in Λ^*. Thus Λ^* would contain a point of the form $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$, where each ε_i is 0 or 1, but not all ε_i are 0. Hence Λ would have a point other than the origin in the cube of width 2 described above. Thus Λ^* is not a lattice.

Observe that the shift is one-to-one if and only if the lattice Λ intersects the cube $0 \leqq x_i < 1$, $1 \leqq i \leqq n$, only at the origin.

QUESTION I-1. What is the necessary and sufficient condition that the shift of a lattice is a lattice? Assume that the shift is one-to-one.

The shift of a rational lattice is clearly a periodic set.

QUESTION I-2. When is the shift of a lattice that is not rational a periodic set? Assume that the shift is one-to-one.

QUESTION I-3. Are the packing and covering constants of a cluster rational?

QUESTION I-4. Are the lattice-packing and lattice-covering constants of a cluster rational? Is there an algorithm for determining these constants?

QUESTION I-5. Is there, for every cluster, a periodic packing (covering, tiling) with a density equal to its densest packing (covering, tiling)?

QUESTION I-6. For which clusters does the densest **Z**-lattice (**Q**-lattice) packing give the densest lattice packing? The densest packing?

QUESTION I-7. For which clusters does the sparsest **Z**-lattice (**Q**-lattice) covering give the sparsest lattice covering? The sparsest covering?

C. *Clusters in the line.* The problem of covering $\mathbf{R}^1$ by translates of a finite cluster was considered by Newman **[37]**. By the shift theorem, this problem is equivalent to covering $\mathbf{R}^1$ by integer translates of the cluster, hence, to covering **Z** by the translates of a finite set $K \subseteq \mathbf{Z}$. (The notions of covering, packing, or tiling $\mathbf{Z}^n$ by translates of a subset of $\mathbf{Z}^n$ are defined much like their analogs in Euclidean space. However, the condition, "disjoint interiors", which appears in geometric packings, is now replaced simply by "disjoint".)

It is easy to show that any set $K \subseteq Z$ with one or two elements tiles **Z**. Newman showed that any set K with three elements has a covering density of at most 6/5, with the covering density of $K = \{0, 1, 3\}$ being 6/5. Moreover, letting $c(r)$ denote the least upper bound of the covering density of K, for all sets $K \subseteq Z$ with r elements, Newman proved that $c(r) \sim \log r$. As mentioned earlier, this result holds in all dimensions. He conjectured that $c(4) = 4/3$. Weinstein **[57]** showed that it is at most $4/3 + 8/303$. In **[56]** he investigated coverings in groups.

Newman, in **[34]**, turned to the problem of determining which finite sets of integers, K, tile Z by translates. He solved this problem completely when $|K|$ is a power of a prime, obtaining the following result.

THEOREM I-3. *Let $K = \{a_1, a_2, \ldots, a_r\}$ be a set of r distinct integers, where $r = p^a$ is a prime power. For $1 \leqq i < j \leqq n$, let e_{ij} denote the highest power of p that divides $a_i - a_j$. Then K tiles Z by translates if and only if there are at most a distinct e_{ij}.*

If r is prime, this theorem says that the a_i are all congruent modulo p^e and incongruent modulo p^{e+1} for some non-negative integer e. (The sufficiency of this condition is not hard to establish.)

QUESTION I-8. When does a set of six integers $\{a_1, a_2, a_3, a_4, a_5, a_6\}$ tile Z?

In case K has three elements, we may normalize them to be 0, a, and b, with a and b relatively prime. The theorem then asserts that $K = \{0, a, b\}$ tiles $\mathbf{Z}$ if and only if the elements 0, a, and b are incongruent modulo 3. Newman remarked, "Surely this special case deserves to have a completely trivial proof-but we have not been able to find one". We include this recent elementary proof, which is due to Dean Hickerson.

The proof makes use of the following fact. Let A and S be subsets of $\mathbf{Z} \times \mathbf{Z}$. Assume that every translate of $-A$ contains exactly one member of S. Then A tiles $\mathbf{Z} \times \mathbf{Z}$ by translates by elements of S. (Similar results for clusters are discussed in §I-A.)

Assume that the set of translates of $\{0, a, b\}$ by the vectors in the set $C \subseteq \mathbf{Z}$ tile Z. Without loss of generality, we assume that $0 \in C$. Let $S \subseteq \mathbf{Z} \times \mathbf{Z}$ be the set of ordered pairs (x, y), such that x and y are integers and $xa + yb \in C$. Let K^* be the three ordered pairs, (0, 0), (1, 0), and (0, 1). (Think of K^* as the analog in $\mathbf{Z} \times \mathbf{Z}$ of a (1, 2)-semicross.)

We assert that K^* tiles $\mathbf{Z} \times \mathbf{Z}$, with S as the set of translation vectors. To show this, consider $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ and the representation of $xa + yb$ as an element of $c + K$, $c \in C$. Exactly one of the numbers $xa + yb$, $(x - 1)a + yb$, and $xa + (y - 1)b$ is in C. In other words, exactly one of the points (x, y), $(x - 1, y)$, and $(x, y - 1)$ is in S. Thus, K^* tiles $\mathbf{Z} \times \mathbf{Z}$ by translates of the elements in S.

Note that $(0, 0) \in S$. A sketch shows that $S = \{(x, y) | x \equiv y (\text{mod } 3)\}$. Since $(b, -a) \in S$, $b \equiv -a (\text{mod } 3)$. Thus, since a and b are relatively prime they are, in some order, congruent to 1 and 2 modulo 3. Thus 0, a, and b are incongruent modulo 3. This completes Hickerson's "completely trivial" proof.

Incidentally, this argument shows that C consists of the multiples of 3.

We are not aware of any work on packings of $\mathbf{Z}$ by translates of finite sets of integers. However, it was shown in **[42]** and **[14]** that, for any set K of three integers, $\mathbf{Z}$ is the union of disjoint congruent copies of K, that is, of translations of K and of its reflection, $-K$. This implies that translates of K (or perhaps of $-K$) pack $\mathbf{Z}$ with density at least 1/2. (The packing constructed is periodic, hence the density exists.) But $-K$ packs $\mathbf{Z}$ just as densely as K does. Consequently, any set of three integers packs $\mathbf{Z}$ with density at least 1/2. Hickerson has shown that any three integers pack with density at least 3/4. (Note that $\{1, 2, 4\}$ packs with density 3/4.)

The proof of the next theorem illustrates a method for determining the packing density of a finite set of integers.

THEOREM I-4. *For any positive integer a, the packing constant of $K = \{0, a, 2a + 1\}$ is $3a/(3a + 1)$.*

PROOF. The translates of K by the integers congruent to $0, 1, 2, \ldots,$ or $a - 1 (\mathrm{mod}\ 3a + 1)$ form a packing of $\mathbf{Z}$ with density $3a/(3a + 1)$. We will show that no packing by K can have density larger than $3a/(3a + 1)$.

The union of the translates of K in a packing with density larger than $3a/(3a + 1)$ must contain some set of $3a + 1$ consecutive integers. All that remains is to show that the union of a disjoint family of translates of K cannot contain $3a + 1$ consecutive integers.

Let $A \subseteq Z$ be a set such that the family $\{v + \{0, a, 2a + 1\} | v \in A\}$ is pairwise disjoint and contains $3a + 1$ consecutive integers, which, without loss of generality, may be assumed to be $1, 2, \ldots, 3a + 1$.

Imagine an empty cell above each of these $3a + 1$ integers on the real line. Place in the cell at integer i one of the three numbers $0, a, 2a + 1$, according as $i = v + 0$, $v + a$, or $v + 2a + 1$ for some $v \in A$, respectively.

For $1 \leqq i \leqq 3a$, if there is an a at cell i, then cell $i + 1$ can contain neither 0 nor $2a + 1$, hence must contain a. Consequently, the cells occupied by a form a single unbroken interval which stretches from the leftmost cell occupied by an a all the way to cell $3a + 1$. Since none of the three symbols $0, a, 2a + 1$ can occur in more than a consecutive cells, the interval occupied by a's has at most a cells, and these are among the cells at $2a + 2, 2a + 3, \ldots, 3a + 1$.

If, for $1 \leqq i \leqq 2a + 1$, there is a 0 at cell i, then there is an a at cell $i + a$, hence $i \geqq a + 2$. So, for $1 \leqq i \leqq \mathrm{a} + 1$, cell i can contain neither 0 nor a; it must contain $2a + 1$, contradicting the fact that a given symbol cannot appear in $a + 1$ consecutive cells. This concludes the proof.

Weinstein [57] investigated the packing density of a set of k integers for large k. On the one hand, he showed constructively that the packing constant for any set of k integers is at least $2/k$. To obtain sets with small packing constants, he considered a set A that is a "basis for subtraction" of the set $\{0, 1, \ldots, n\}$. The set A of nonnegative integers is a basis for subtraction for $\{0, 1, \ldots, n\}$ if $A - A \supseteq \{0, 1, \ldots, n\}$. If A has k elements, then the packing density of A is clearly at most $k/(n + 1)$, since no two translating vectors of a packing family can differ by an element in $A - A$. With the aid of this tool, he constructed, for large k, sets of k integers whose packing density is at most $8/(3k)$.

In [12] Gilpin and Shelton considered the density of admissible sets for a finite set D.

QUESTION I–9. What can be said about the packing constant for any set of four integers?

II. The cross and semicross. The rest of this survey is devoted to questions raised by two particular clusters, the cross and the semicross. For convenience we will assume that the arms of the semicross correspond to the positive axes. Occasionally we will consider arms of non-integral length (when the cross or semicross is not a cluster), but generally the arm length k will be assumed to be an integer. Because of their connection with coding theory, the fact that they are star bodies, and their amenability to algebraic and combinatorial analysis, they have received a good deal of attention. This section discusses their geometry, while §III concerns their algebra.

A. *The cross.* The $(k, 1)$-cross, being an interval of length $2k + 1$, lattice tiles the line, $\mathbf{R}^1$. However, even the $(k, 2)$-cross raises interesting problems.

For integral k the $(k, 2)$-cross tiles the plane only when $k = 0$ or 1. (If we allow non-integral k, we find that the $(1/2, 2)$-cross also tiles $\mathbf{R}^2$.) Everett and Hickerson **[8]** showed that, for every real number $k \geqq 1$, the packing constant of the $(k, 2)$-cross is $(4k + 1)/(k^2 + 2k + 2)$ and a best packing is provided by the lattice with basis vectors $(k + 1, 1)$ and $(-1, k + 1)$. For $0 < k < 1/2$ and $1/2 < k < 1$, the packing constant of the $(k, 2)$-cross is not known.

The covering constant of the $(k, 2)$-cross is far more difficult to determine. In **[8]** it is conjectured that, for positive integral k, it is $(4k + 1)/(3k + 2)$. This bound is suggested by the fact that the cluster formed of the union of the $(k, 2)$-crosses with center squares at $(0, 0), (1, 1), (2, 2), \ldots, (k - 1, k - 1)$ has area $k(3k + 2)$ and tiles the plane. (For $k > 1$ this is a periodic but not lattice covering.) Loomis **[8]** verified this conjecture for the $(2, 2)$-cross, whose covering constant is $9/8$. The proof begins by using the shift theorem to make the problem discrete, and then develops an extensive combinatorial argument that depends on a weighting of the ways squares covered by more than one cross are contributed by the crosses. Rooney **[40]** has shown that the lattice covering constant of the $(2, 2)$-cross is $9/7$.

The covering constant of the $(k, 2)$-cross has also been examined for non-integer values of k. Hickerson has shown that it is $21/20$ for the $(1/3, 2)$-cross, and conjectures that the covering constant of the $(k, 2)$-cross, for $0 \leqq k \leqq 2$, is given by these formulas:

$$\frac{4k + 1}{(k + 1)(2k + 1)}, \qquad 0 \leqq k \leqq 1/2$$

$$\frac{4k + 1}{2(k + 1)}, \qquad 1/2 \leqq k \leqq (\sqrt{5} - 1)/2$$

$$\begin{array}{ll} \dfrac{4k+1}{k^2+3k+1}, & (\sqrt{5}-1)/2 \leqq k \leqq 1. \\[2ex] \dfrac{4k+1}{2k+3}, & 1 \leqq k \leqq \dfrac{\sqrt{17}-1}{2} \\[2ex] \dfrac{2(4k+1)}{k^2+5k+2}, & \dfrac{\sqrt{17}-1}{2} \leqq k \leqq 2 \end{array}$$

QUESTION II-1. What is the covering constant of the $(k, 2)$-cross?

Stein [43] showed for integer k that if the (k, n)-cross tiles $\mathbf{R}^n$, then the $(k, 2n)$-semicross tiles $\mathbf{R}^{2n}$.

Using finite fields, Stein [44] constructed a tiling of $\mathbf{R}^{10}$ by the $(4, 10)$-cross (with notches and bumps added) and showed that there is no lattice tiling by this set. This is the first example of a star body that tiles, but not as a lattice. Using a slightly different algebraic approach, Szabó [51] proved that the notched $(3/2, 5)$-cross has the same property. In both cases, the notches are added to force the crosses to fit together along complete facets of the individual cubes. It is not clear that the notches are necessary. It may be that, for integer values of k, if a (k, n)-cross lattice tiles, then it $\mathbf{Z}$-lattice tiles. In any case, by Hajós's theorem in §I-B, if a cross (or any cluster) lattice tiles, it $\mathbf{Q}$-lattice tiles.

Szabó [52], [53] explored $\mathbf{Q}$-lattice tilings by crosses, proving the following theorem.

THEOREM II-1. *If k is an integer and the (k, n)-cross $\mathbf{Z}$-lattice tiles R^n, and if $2kn + 1$ is composite and each of its prime divisors is larger than k, then:*

(a) *there is a $\mathbf{Q}$-lattice tiling of $\mathbf{R}^n$ by the (k, n)-cross, which is not a $\mathbf{Z}$-tiling; and*

(b) *there is a $\mathbf{Z}$-tiling by the (k, n)-cross that is not a lattice tiling.*

The proof of (b) in [52] and [53], which is independent of that of (a), makes use of Hajós's fundamental theorem on the factorization of abelian groups by sets that are "front ends" of cyclic subgroups. However, (b) follows from (a) by applying the shift theorem, described in §I-B, to the lattice Λ produced in (a). Because of the special form of Λ it can be shown that the shift of Λ is not a lattice.

The question, "For which k and n does the (k, n)-cross tile $\mathbf{R}^n$?", is far from being answered. We might suspect that, for $n \geqq 2$, the (k, n)-cross cannot tile $\mathbf{R}^n$ when k is too large. Confirming this suspicion, Stein [43] showed that, for $n > 2$, if the (k, n)-cross tiles $\mathbf{R}^n$, then $k \leqq 2(n-1)$. This bound is probably not the strongest possible. For $n = 2$ the actual bound is 1 and for $n = 3$ the bound is 2. No example is known for which k exceeds $n - 1$. For an odd prime p, the $((p-1)/2, p+1)$-cross tiles R^{p+1}, as was shown in [19]. This suggests that perhaps, for all $n \geqq 4$, if a (k, n)-cross tiles $\mathbf{R}^n$, then $k < n/2$.

QUESTION II-2. For a given $n \geqq 2$, if the (k, n)-cross tiles $\mathbf{R}^n$, how large can k be?

QUESTION II-3. For which k and n does the (k, n)-cross tile $\mathbf{R}^n$? $\mathbf{Z}$-lattice tile $\mathbf{R}^n$? $\mathbf{Q}$-lattice tile $\mathbf{R}^n$?

Algebraic methods for constructing $\mathbf{Z}$-lattice tilings of $\mathbf{R}^n$ by the (k, n)-cross will be discussed in §V.

While almost nothing is known about the covering constant of the cross for dimensions $n \geqq 3$, its packing constant has been determined, at least asymptotically for large k. Stein **[47]** obtained the following theorem.

THEOREM II-2. *Let $\delta\ (k, n)$ be the packing constant and $\delta_\Lambda(k, n)$ be the lattice-packing constant of the (k, n)-cross. Then, for $n \geqq 2$,*

$$\lim_{k\to\infty} k^2\delta(k, n) = 1 \quad \textit{and} \quad \lim_{k\to\infty} k^2\, \delta_\Lambda(k, n) = 1.$$

The algebraic argument behind the second limit is discussed in §V.

QUESTION II-4. What can be said about the $\mathbf{Z}$-lattice, $\mathbf{Q}$-lattice, and arbitrary packing constants of the (k, n)-cross for $n \geqq 3$?

QUESTION II-5. What are the $\mathbf{Z}$-lattice and lattice-covering constants of the (k, n)-cross, $n \geqq 2$? What is the covering constant?

B. *The semicross.* The semicross is fundamentally different from the cross in several respects. First, because of the greater symmetry of a cross, C, tiling by translates of C is the same as tiling by congruent copies of C. Second, the $(k, 2)$-semicross tiles $\mathbf{R}^2$ for all real k, but only for $k = 0, 1/2$, and 1 does the $(k, 2)$-cross tile $\mathbf{R}^2$. A more dramatic contrast is found in the way the semicross and cross pack $\mathbf{R}^3$. Stein **[47]** showed that the lattice-packing constant of the $(k, 3)$-semicross is at most $8(3k + 1)/k^{3/2}$, while its packing constant is at least $(3k + 1)/k^{1.484}$ for large k. These two facts show that

$$\lim_{k\to\infty} \frac{\delta^*_\Lambda(k, 3)}{\delta^*(k, 3)} = 0,$$

where $\delta^*_\Lambda\ (k, n)$ is the lattice-packing constant and $\delta^*(k, n)$ is the packing constant of the (k, n)-semicross. By Theorem II-2, the corresponding limit for $(k, 3)$-crosses is 1.

The problem of determining the packing density of the $(k, 3)$-semicross was first considered by Hamaker and Stein in **[20]**. It is intimately connected with the following combinatorial design.

Consider a square array of k^2 cells. Place in some of these cells one of the integers $1, 2, \ldots, k$ in such a way that the following three conditions are satisfied:

(a) For two filled-in cells in a row, the one further right has a larger entry;

(b) For two filled-in cells in a column, the higher one has a larger entry; and

(c) For two filled-in cells with the same entry, the cell further right is higher (the "positive slope" condition).

Such an array is called a monotonic matrix of order k.

A monotonic matrix of order k records the locations of corners of a set of disjoint translates of a (k, 3)-semicross. The entry z at the cell where column x meets row y records the presence of the corner (x, y, z). The more entries there are in a monotonic matrix of order k, the more disjoint translates of the (k, 3)-semicross can be placed with their corners in a cube of width k.

Let $m(k)$ be the largest number of filled-in cells in all k by k monotonic matrices. It is not hard to show that $m(1) = 1$, $m(2) = 2$, $m(3) = 5$, and $m(4) = 8$. Computer searches by Ken Joy and by Peter Constantinidis showed that $m(5) = 11$ and suggest that $m(6) = 14$. (There were many cases of 14 found, and none of 15.) Table II-1 lists $m(k)$ for small values of k; numbers in parentheses are lower bounds.

k	1	2	3	4	5	6	7	8	9	10
$m(k)$	1	2	5	8	11	(14)	(19)	(22)	(28)	(32)

TABLE II-1

The only monotonic matrices of order 3 with 5 entries are the one shown in Figure II-1

$$\begin{array}{|ccc|}
\hline
2 & & 3 \\
 & & 1 \\
1 & 3 & \\
\hline
\end{array}$$

FIGURE II-1

and its transpose. When k is a square, it is easy to construct a monotonic matrix with $k^{3/2}$ entries, as illustrated in Figure II-2 in the case $k = 9$.

$$\begin{array}{|ccc|ccc|ccc|}
\hline
 & & 3 & & & 6 & & & 9 \\
 & 3 & & & 6 & & & 9 & \\
3 & & & 6 & & & 9 & & \\
\hline
 & & 2 & & & 5 & & & 8 \\
 & 2 & & & 5 & & & 8 & \\
2 & & & 5 & & & 8 & & \\
\hline
 & & 1 & & & 4 & & & 7 \\
 & 1 & & & 4 & & & 7 & \\
1 & & & 4 & & & 7 & & \\
\hline
\end{array}$$

FIGURE II-2

With the aid of the following lemma, which rests on the existence of the monotonic matrix of Figure II-1, we can construct monotonic matrices of order k for which $m(k) > k^{3/2}$.

LEMMA II-1. *For each positive integer k, $m(2k + 1) \geqq 2m(k) + 3k$.*

PROOF. Partition a $2k + 1$ by $2k + 1$ array into nine regions by two vertical lines and two horizontal lines, resulting in four corner k by k squares, four 1 by k rectangles and a 1 by 1 square in the center, as shown in Figure II-3.

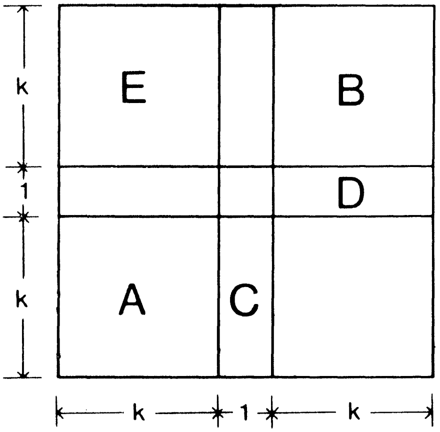


FIGURE II-3

Label five of those nine regions A, B, C, D, and E, as shown in Ficure II-3. In square A, form a monotonic matrix of order k with $m(k)$ entries, using the numbers $1, 2, \ldots, k$. In square B, using the numbers $k + 2, k + 3, \ldots, 2k + 1$, form a monotonic matrix of order k with $m(k)$ entries. In the main diagonal of E place the number $k + 1$, k times. In C place the numbers $k + 2, k + 3, \ldots, 2k + 1$ and in D, the numbers $1, 2, \ldots, k$. The resulting matrix is monotonic, and shows that $m(2k + 1) \geqq 2m(k) + 3k$.

		4		6		7
	4					5
4				5	7	
				1	2	3
2		3	7			
		1	6			
1	3		5			

			5				8	9
		5					6	7
	5				8	9		
5					6	7		
					1	2	3	4
		3	4	9				
		1	2	8				
3	4			7				
1	2			6				

FIGURE II-4

The matrices of orders 7 and 9 shown in Figure II-4 are constructed with the aid of the lemma. Thus $m(7) \geqq 19 \doteq 7^{1.513}$ and $m(9) \geqq 28 \doteq 9^{1.517}$.

QUESTION II-6. Is $m(8) \geqq 23$, as table II-1 may suggest?

The function m has the following properties: (i) $m(k) \leqq k^2$, (ii) $m(k+1) > m(k)$; and (iii) $m(k_1k_2) \geqq m(k_1)\, m(k_2)$. The first two are immediate, while the third is established in **[20]**. It follows from these three properties that if $m(k)$ is written as $k^{e(k)}$, then $\lim_{k\to\infty} e(k)$ exists and is at most 2. This limit equals sup $\{e(k)\}$ and lies in the interval $[\log_9 28, 2]$. (Hickerson has shown that $m(255) \geqq 4639$, so $\lim_{k\to\infty} e(k) \geqq 1.523$.)

QUESTION II-7. What is $\lim_{k\to\infty} e(k)$?

If it turns out that $\lim_{k\to\infty} e(k) < 2$, then $\lim_{k\to\infty} m(k)/k^2 = 0$. As shown in **[20]**, this equation is equivalent to the assertion that the density of packings of $\mathbf{R}^3$ by the $(k, 3)$-semicross approaches 0 as k approaches infinity. However, not even the following question has been answered.

QUESTION II-8. Is $\lim_{k\to\infty} m(k)/k^2 = 0$?

We are tempted to conjecture on the basis of admittedly skimpy data that

$$m(k) \sim \frac{k^2}{\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{k}}, \tag{II-2}$$

or, equivalently, $m(k) \sim k^2/\log k$. Table II-2 compares $m(k)$ and, to two decimals, $k^2/(1/1 + 1/2 + \cdots + 1/k)$, for $k = 1, 2, \ldots, 9$.

k	m(k)	$k^2/\left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{k}\right)$
1	1	1
2	2	2.67
3	5	4.91
4	8	7.68
5	11	10.95
6	$\geqq$ 14	14.69
7	$\geqq$ 19	18.90
8	$\geqq$ 22 (23?)	23.55
9	$\geqq$ 28	28.63
10	$\geqq$ 32	34.14

TABLE III-2

If it turns out that $m(k) \sim k^2/\log k$, then it follows that $\lim_{k\to\infty} e(k) = 2$ and $\lim_{k\to\infty} m(k)/k^2 = 0$.

QUESTION II-9. Is formula (II-2) correct?

III. Multiplier sets. Figure III-1 shows that the (1, 2)-cross **Z**-lattice tiles $\mathbf{R}^2$ by means of the translating vectors $\{(x, y) | x + 2y \equiv 0 (\text{mod } 5)\}$.

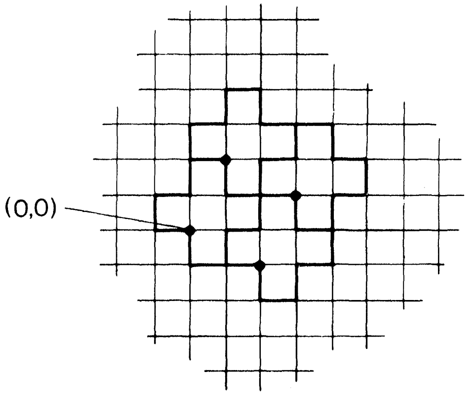


FIGURE III-1

The reflection of this tiling in the line $y = x$ produces the only other tiling of the plane by the (1, 2)-cross up to translation. Similarly, the (1, 3)-cross tiles $\mathbf{R}^3$ with $\{(x, y, z) | x + 2y + 3x \equiv 0 (\text{mod } 7)\}$ as translation vectors, and the (2, 3)-cross tiles $\mathbf{R}^3$ by means of $\{(x, y, z) | x + 3y + 4z \equiv 0 (\text{mod } 13)\}$. These **Z**-lattice tilings depend on certain properties of the cyclic groups $C(5)$, $C(7)$, and $C(13)$, respectively. The first reduces to the fact that the four numbers $1, -1, 2, -2$, constitute the nonzero elements of $C(5)$. The second corresponds to the fact that $1, -1, 2, -2, 3, -3$ are the six nonzero elements of $C(7)$ and the third to the fact that each nonzero element of $C(13)$ can be expressed uniquely in the form ab, where $a \in \{\pm 1, \pm 2\}$ and $b \in \{1, 3, 4\}$. These examples illustrate the following algebraic means of producing **Z**-lattice tilings.

Let G be a finite abelian group of order m. Let k and n be positive integers such that $2kn + 1 = m$. Assume that there are n elements in G, $\{g_1, g_2, \ldots, g_n\}$, such that the $2kn$ elements $\pm ig_j$, $1 \leqq i \leqq k$, $1 \leqq j \leqq n$, are distinct from each other and distinct from $0 \in G$. In other words, each nonzero element in G is uniquely expressible in the form $\pm ig_j$, $1 \leqq i \leqq k$, $1 \leqq j \leqq n$. Then the (k, n)-cross **Z**-lattice tiles $\mathbf{R}^n$. As the set of translating vectors, A, use the set of all integer points $(x_1, x_2, \ldots, x_n)$ such that

$$x_1g_1 + x_2g_2 + \cdots + x_ng_n = 0,$$

the identity element of G. Note that the quotient group $\mathbf{Z}^n/A$ is isomorphic to G.

The converse also holds. Starting from a $\mathbf{Z}$-lattice tiling of $\mathbf{R}^n$ by translates of the (k, n)-cross by vectors in a lattice A, we may construct a finite abelian group G, namely $\mathbf{Z}^n/A$, and the set $\{g_1, g_2, \ldots, g_n\} \subseteq G$ as the images of the n unit vectors $(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, \ldots, 0, 1)$ under the natural homomorphism from $\mathbf{Z}^n$ to $\mathbf{Z}^n/A$. (See **[18]** or **[45]**.)

A similar result holds for the (k, n)-semicross. In this case the group G has order $kn + 1$ and the kn elements ig_j, $1 \leqq i \leqq k$, $1 \leqq j \leqq n$, are distinct from each other and from 0. This is equivalent to the assertion that the (k, n)-semicross $\mathbf{Z}$-lattice tiles $\mathbf{R}^n$. These two basic facts motivate the rest of this survey.

First we make some general definitions.

Let M be a finite set of nonzero integers, called a multiplier set, and let G be a finite abelian group. Assume that there is a set S in G such that each nonzero element in G has a unique representation in the form ms, $m \in M$, $s \in S$, and that 0 has no such representation. Then we say that M splits G and that S is a splitting set.

If $(m, |G|) = 1$ for each $m \in M$, the splitting is called nonsingular. Otherwise it is called singular. If each prime that divides $|G|$ divides at least one $m \in M$, then the splitting is called purely singular.

If G is the cyclic group $C(n)$, split by M with splitting set S, then we may identify M with a subset of $C(n)$. Each element of $C(n) - \{0\}$ is uniquely expressible as a product ms, $m \in M$, $s \in S$, where the product is taken in the multiplicative structure of the ring $\mathbf{Z}_n$. In particular, when n is a prime, $C(n) - \{0\}$ is a cyclic group of order $n - 1$, denoted $C(n)^*$. The splitting of $C(n)$ is then equivalent to a factoring of the group $C(n)^*$ (A factoring of a group G consists of two subsets A and B such that each element of G is uniquely expressible in the form ab, $a \in A$, $b \in B$. Such a factoring is denoted $G = A \circ B$. More generally, if X, A, and B are subsets of G such that each element of $X \subseteq G$ is uniquely representable in the form ab, $a \in A$, $b \in B$, and each product ab is in X, then we write $X = A \circ B$.) For a survey of the work of Sands and deBruijn on factoring groups, see **[45]**.

A. Splittings of finite abelian groups. Splitting behaves nicely with respect to exact sequences, as the following theorems show.

Theorem III-1. **[23]**. *Let H be a subgroup of the finite abelian group G. Then if M splits G and G/H, it splits H.*

The proof shows that if S is a splitting set of G, then $S \cap H$ is a splitting set of H. Actually, Hickerson proved this in the case of a normal subgroup of the not necessarily abelian group G, after extending the definition of splitting to nonabelian groups in the expected way. The assumption that G is finite is essential, as this example of Hickerson's shows.

Let G be the additive group of rational numbers modulo 1 and let H be the subgroup consisting of the elements 0 and 1/2. Let $M = \{2\}$. Then M splits G by the splitting set $S = \{g | g \in G,\ 0 < g < 1/2\}$, hence splits G/H, which is isomorphic to G, but does not split H since 1/2 is not of the form $2x$, $x \in H$.

COROLLARY III-1. ([*GSt*]) *Let H be a subgroup of the finite abelian group G. Then if M splits G and H, it splits G/H.*

This follows from Theorem III-1 by use of the functor Hom(, $Q/[1]$), where $Q/[1]$ is the additive group of Q modulo 1. From the exact sequence of finite abelian groups,

$$0 \to H \to G \to G/H \to 0,$$

we obtain the exact sequence

$$0 \leftarrow \mathrm{Hom}(H, Q/[1]) \leftarrow \mathrm{Hom}(G, Q/[1]) \leftarrow \mathrm{Hom}(G/H, Q/[1]) \leftarrow 0.$$

Since Hom(A, $Q/[1]$) is isomorphic to A for any finite abelian group A, the corollary follows. However, this argument does not show how to construct the splitting set in G/H.

The next few theorems enable us to construct splittings of a group from splittings of smaller groups.

THEOREM III-2. [**19**] *Let G be a finite abelian group and*

$$0 \to A \xrightarrow{\alpha} G \xrightarrow{\beta} B \to 0$$

an exact sequence. If M splits the groups A and B, with the splitting of A nonsingular, then M splits G.

The proof is constructive. Let $a_1, a_2, \ldots, a_r$ be a splitting set in A and $b_1, b_2, \ldots, b_s$ be a splitting set in B. Select $g_1, g_2, \ldots, g_s$ in G such that $\beta(g_i) = b_i$, $1 \leqq i \leqq s$. Then it can be checked that the set

$$\{\alpha(a_1), \alpha(a_2), \ldots, \alpha(a_r)\} \cup (\alpha(A) + \{g_1, g_2, \ldots, g_s\})$$

is a splitting set for G. (For subsets X and Y in an abelian group, $X + Y$ denotes the set $\{x + y \mid x \in X,\ y \in Y\}$.) It follows from Theorem III-2 that if p is a prime and M splits $C(p)$, then M splits any abelian group of order p^n. In the next theorem, which is obtained from Theorem III-2 by use of Hom(, $Q/[1]$), the splitting set whose existence is asserted is not constructed.

THEOREM III-3. [19] *Let G be a finite abelian group and*

$$0 \to A \xrightarrow{\alpha} G \xrightarrow{\beta} B \to 0$$

an exact sequence. If M splits A and B, with the splitting of B nonsingular, then M splits G.

The restriction "nonsingular" in these two theorems cannot be removed. For instance, $M = \{1, 2, 3\}$ splits $C(4)$ but not $C(16)$, and there is an exact sequence, $0 \to C(4) \to C(16) \to C(4) \to 0$.

Next, consider the case when M splits G.

THEOREM III-4. [(19] *Let G be a finite abelian group and*

$$0 \to A \xrightarrow{\alpha} G \xrightarrow{\beta} B \to 0$$

an exact sequence. If M splits G and if $(m, |B|) = 1$, *for each* $m \in M$, *then M splits A (hence B). If M splits G and if* $(m, |A|) = 1$, *for each* $m \in M$, *then M splits B (hence A).*

The first part is proved constructively by showing that the subset of the splitting set for G that lies in A is a splitting set for A. The second part is then obtained by duality.

The assumption that $(m, |B|) = 1$ is necessary, as the example $M = \{1, 2, 3\}$, $G = C(4)$ and $A = B = C(2)$ shows.

With the aid of these theorems we can determine, for instance, all finite abelian groups G that are split by $M = \{1, 2\}$. First, write G as the direct product of its Sylow subgroups,

$$G = Sy(p_1) \times Sy(p_2) \times \cdots \times Sy(p_r),$$

where $p_1, p_2, \ldots, p_r$ are the prime divisors of $|G|$. Since $|G|$ is odd, each element of M is relatively prime to the orders of these Sylow subgroups. By the preceding theorems, M splits G if and only if M splits each $Sy(p_i)$. Next, write each $Sy(p_i)$ as the direct product of cyclic subgroups. The theorems show that M splits $Sy(p_i)$ if and only if M splits each of these cyclic subgroups. But the existence of the exact sequence $0 \to C(p) \to C(p^n) \to C(p^{n-1}) \to 0$, for any prime p, together with the theorems, shows that M splits $C(p^n)$ if and only if M splits $C(p)$. It is then an easy matter to show that M splits $C(p)$ if and only if the order of 2 modulo p is even. So the question "Which finite abelian groups does $M = \{1, 2\}$ split?" is equivalent to the question "For which odd primes p is the order of 2 modulo p even?" The order is even when $p \equiv 3$ or $5 (\text{mod } 8)$, odd when $p \equiv 7 (\text{mod } 8)$, but either odd or even when $p \equiv 1 (\text{mod } 8)$.

The case $M = \{1, 2\}$ was simplified by the fact that all splittings by M are nonsingular. For $M = \{1, 2, 3\}$ the result is more complicated, since there are singular splittings, such as the splitting of $C(4)$. In [10] it is shown that $M = \{1, 2, 3\}$ splits the finite abelian group if and only if (a) the 2-sylow subgroup of G is either $\{1\}$ or $C(4)$ and (b) M splits $C(p)$ for each odd prime divisor p of $|G|$. The argument uses the following result of Hickerson **[23]**, which generalizes a theorem in **[10]**.

THEOREM III-5. *Let p be a prime. If M splits the finite abelian p-group G singularly, then G is cyclic.*

The case $M = \{1, 2, 3, 4\}$ was also settled in **[10]**: $M = \{1, 2, 3, 4\}$ splits the finite abelian group G if and only if (a) the 3-sylow subgroup of G is either $C(1)$ or $C(9)$, and (b) M splits $C(p)$ for each prime divisor p of $|G|$ other than 3.

In **[23]** this was generalized to any set M with four elements and an incomplete result for any set M of five elements was obtained. $Sy(2) \times Sy(3)$ must be of the form $C(2^a) \times C(2^b) \times C(3^c)$, where $c \equiv a + b (\text{mod } 4)$. For the particular case when M is $\{1, 2, 3, 4, 5\}$ it was shown that M splits the finite abelian group G if and only if $Sy(2) \times Sy(3)$ is $C(6)$ or $C(1)$ and M splits $C(p)$, for all prime divisors p of $|G|$, $p \geqq 7$.

The next theorem treats the case $M = \{1, 2, 3, 4, 5, 6\}$.

THEOREM III-6. *$M = \{1, 2, 3, 4, 5, 6\}$ splits the finite abelian group G if and only if $|G|$ is not a multiple of 5 and M splits $C(p)$ for each prime divisor p of $|G|$.*

PROOF. Since $|G| \equiv 1 (\text{mod } 6)$, all elements of M other than 5 are relatively prime to $|G|$. Write G as the product of its Sylow subgroups,

$$G = Sy(5) \times Sy(p_1) \times \cdots \times Sy(p_r),$$

where the p_i are the primes that divide $|G|$ but no element of M. By the preceding theorems, M splits G if and only if M splits each of these Sylow subgroups. M splits $Sy(p_i)$ if and only if it splits $C(p_i)$.

Consider the form of $Sy(5)$, which, for the moment, we will assume has more than one element. Since the splitting of $Sy(5)$ is singular, $Sy(5)$ is cyclic, of the form $C(5^n)$. Furthermore, since $5^n \equiv 1 (\text{mod } 6)$, n is even. We shall determine which cyclic groups of the form $C(5^n)$, n even, are split by M.

Consider $C(5^n)$ to be comprised of the integers $0, 1, 2, \ldots, 5^n - 1$. Assume that $n \geqq 4$. Let d_i, $i = 0$ or 1, be the number of elements in $C(5^n)$ divisible by 5^i but not by 5^{i+1}. Note that $d_i = 5^{n-i} - 5^{n-i-1}$. Let s_i, $i = 0$ or 1, be the number of elements in the alleged splitting set that are divisible by 5^i but not by 5^{i+1}. Then $d_0 = 5s_0$ and $d_1 = s_0 + 5s_1$. Thus $5^n - 5^{n-1} = 5s_0$ and $5^{n-1} - 5^{n-2} = s_0 + 5s_1$. Hence $s_0 = 5^{n-1} - 5^{n-2}$ and $s_1 = 0$. Thus the number of elements in the splitting set that are multiples of 5^2 is $(5^n - 1)/6 - (5^{n-1} - 5^{n-2})$, which equals $(5^{n-2} - 1)/6$. Let T be this subset of the splitting set. Since $|T| = (5^{n-2} - 1)/6$, M splits the subgroup of $C(5^n)$ that consists of the multiples of 25; consequently it splits $C(5^{n-2})$. By descent, M splits $C(25)$. But, as some short calculations show, M does not split $C(25)$. Thus $Sy(5)$ is the group of order 1. This proves the theorem and incidentally shows that each splitting of a finite abelian group by $M = \{1, 2, 3, 4, 5, 6\}$ is nonsingular.

As these arguments illustrate, if the finite abelian group G is split by the multiplier set M, then G can be expressed as a direct product $A \times B$, where $|B|$ is relatively prime to each $m \in M$ and each prime that divides $|A|$ divides at least one $m \in M$. Moreover, M splits B nonsingularly and splits A purely singularly. Nonsingular splittings are determined by the prime divisors p of $|B|$ for which M splits $C(p)$. Purely singular splittings do not have such a reduction. The first results on purely singular splittings appeared in **[10]** and concerned finite abelian p groups and $C(p^n)$ in particular.

The following theorem appears in **[23]**.

THEOREM III-7. *Let M split the finite abelian group G in a purely singular manner. Then* (a) $|M| \geqq 3$; (b) *If* $|M| = 3$, *then* $G = C(4^r)$ *for some* $r \geqq 0$; *and* (c) *If* $|M| = 4$, *then* $G = C(9)$.

As shown in **[10]** and **[23]**, $C(4^r)$ has a splitting with $M = \{1, -1, 2\}$ and $S = \{n \mid 0 < n < 4^r/2$, 2 appears an even number of times in the prime factorization of $n\}$.

QUESTION III-1. What are the purely singular splittings of $C(2^n)$? Of $C(p^n)$ for odd primes p?

For other results in this direction see **[10]**, **[23]**, and **[54]**.

A set of integers M may split no finite abelian group. Such a set must have at least three elements, as shown in **[18]**. Furthermore, Hamaker showed that $M = \{1, 3, 27\}$ splits no finite abelian group. On the other hand, as shown by Hickerson in **[23]**, it does split an infinite abelian group, namely the group of rationals with denominators a power of 3 under addition modulo 1. Hamaker's result was generalized in **[10]**: For any integer $c \geqq 2$, the set $\{1, c, c^3\}$ does not split any finite abelian group. This is a special case of the following theorem.

THEOREM III-8. *$M = \{1, a, b\}$ splits some finite abelian group other than $C(1)$ if and only if one of these two conditions holds*:

(1) *a and b are not both integral powers of an integer c.*

(2) *a and b are both integral powers of an integer c, $a = c^s$, $b = c^t$ and $s't' \equiv 2 (\mathrm{mod}\ 3)$, where $s = ds'$, $t = dt'$ and $d = (s, t)$.*

QUESTION III-2. Which multiplier sets split some finite abelian group of order greater than 1? Some infinite abelian group? Which M split infinitely many finite abelian groups purely singularly?

In reference to the last question, $M = \{1, -1, 2\}$ does, but sets of cardinality 1, 2, or 4 do not. Neither does $\{1, 2, 3\}$, $\{1, 2, 3, 4, 5\}$, nor $\{1, 2, 3, 4, 5, 6\}$, as already shown. Hickerson has shown that $\{1, 2, 3, 4, 5, 6, 7, 8\}$ does not as well; this is a consequence of the fact that $\{1, 2, 3, 4, 5, 6, 7, 8\}$ splits a finite abelian group G if and only if $Sy(3)$ is $C(1)$ or $C(9)$, $Sy(5) = C(1)$, $Sy(7) = C(1)$, and $\{1, 2, 3, 4, 5, 6, 7, 8\}$ splits $C(p)$ for each prime divisor p of $|G|$, $p \geqq 11$. He has obtained similar results for many other such multiplier sets.

B. *Splittings of infinite abelian groups.* The question, "Which finite sets of positive integers, M, split Z?", was considered in **[11]**, where a complete solution was obtained. The key lies in this lemma.

LEMMA III-1. *Let M be a finite set of positive integers that splits $\mathbf{Z}$. Let x be the smallest element of M that is larger than* 1. *Let $y \in M$ not be relatively prime to x. Then x divides y.*

They then characterize all such M with this theorem.

THEOREM III-9. *A set M of positive integers split $\mathbf{Z}$ if and only if there are subsets $M_1, M_2, \ldots, M_r$ of M such that*

(i) $M = M_1 \circ M_2 \circ \cdots \circ M_r$;

(ii) $|M_i| = p_i$ *is prime,*

and

(iii) $M_i = \{1, x_i, x_i^2, \ldots, x_i^{p_i-1}\}$, *where x_i is an integer greater than* 1 *and, for* $2 \leqq i \leqq r$,

$$x_i = z_i \prod_{j=1}^{i-1} x_j^{a_{ij}p_j},$$

with a_{ij}, $z_i \in Z$, $a_{ij} \geqq 0$, $z_i \geqq 1$, $\gcd(z_i, \prod_{j=1}^{i-1} x_j) = 1$, *and* $a_{ij} = 0$ *if x_j divides x_k, for some k, $j < k < r$.*

In addition, it was shown in **[11]** that if M splits $\mathbf{Z}$, then it splits any torsion-free infinite abelian group.

Splittings of the additive group of rationals, $\mathbf{Q}$, by a finite set of positive integers, M, were also considered in **[11]**. Observe that M may be considered a subset of $\mathbf{Q}$ and that M factors $\mathbf{Q}^*$, the multiplicative group of positive rational numbers.

Let G be the subgroup of $\mathbf{Q}^*$ generated by the positive primes that divide at least one element of M. Letting $p_1, p_2, \ldots, p_n$ be these primes, we see that G is the free abelian group generated multiplicatively by $\{p_1, p_2, \ldots, p_n\}$. Let $\varphi\colon \mathbf{Z}^n \to G$ be the isomorphism given by

$$\varphi(z_1, \ldots, z_n) = p_1^{z_1} \cdots p_n^{z_n}.$$

Then $M = \{m_1, m_2, \ldots, m_k\}$ factors $\mathbf{Q}^*$ if and only if the cluster corresponding to $\varphi^{-1}(m_1), \varphi^{-1}(m_2), \ldots, \varphi^{-1}(m_k)$ tiles $\mathbf{Z}^n$. Thus, the three questions: "Which finite sets of positive integers split the additive group Q?"; "Which finite sets of positive integers factor the multiplicative group Q^*?"; and "Which clusters tile Euclidean space?" are equivalent. The particular primes that appear in the prime factorization of the elements of M are irrelevant. In particular, for any distinct primes p and p', $M = \{1, p, p'\}$ splits $\mathbf{Q}$ but not $\mathbf{Z}$.

If M does not split $\mathbf{Z}$, we then may ask how densely does it pack $\mathbf{Z}$ and how sparsely does it cover $\mathbf{Z}$.

QUESTION III-3. Let a and b be distinct positive integers greater than 1. Let $M = \{1, a, b\}$. How dense a packing set $S \subseteq Z$ can always be found?

QUESTION III-4. To what extent do results on splitting finite abelian groups generalize to infinite abelian groups? To non-abelian groups?

QUESTION III-5. If a multiplier set splits some finite abelian group does it split some cyclic group? Some group of prime order? An infinite number of groups of prime order?

IV. The multiplier set $\{1, 2, \ldots, k\}$. Because of their close connection with tilings by the semicross and cross, the particular sets $\{1, 2, \ldots, k\}$ and $\{\pm 1, \pm 2, \ldots, \pm k\}$ have been the multiplier sets most thoroughly studied. Let $S(k) = \{1, 2, \ldots, k\}$ ("S" for "Semicross") and let $F(k) = \{\pm 1, \pm 2, \ldots, \pm k\}$ ("F" for "Full cross"). Trivially, $S(k)$ splits $C(k + 1)$ and $C(2k + 1)$ and $F(k)$ splits $C(2k + 1)$. It is not known whether for every k, they split some other group, though the evidence gathered so far indicates that they do. We first consider $S(k)$.

A. *Splittings by* $S(k) = \{1, 2, \ldots, k\}$. In §III we already examined which groups are split by $S(k)$ for $k = 2, 3, 4, 5, 6, 8$. If $k + 1$ is prime, $k + 1 = p$, then $S(k)$ splits any finite p-group since it splits $C(p)$. Similarly, if $2k + 1$ is prime, $2k + 1 = p$, then $S(k)$ splits any finite p-group. For instance, $S(6)$ splits $C(7)$ and $C(13)$ and therefore any finite abelian group of order $7^a 13^b$. Similar reasoning shows that $S(k)$, $k = 8, 9, 10, 11$, and 12, splits a group of prime order, hence an infinite number of groups.

QUESTION IV-1. We showed earlier that, for $k = 2, 3, 4, 6$, and 8, if $S(k)$ splits $C(r) \times G$ for a finite abelian group G, then $S(k)$ splits $C(r)$. Is this true for any other values of k?

QUESTION IV-2. If $S(k)$ splits $C(r) \times G$, where G is an abelian group, must k and r be relatively prime? (If G is finite, the answer is yes since k divides $r|G| - 1$.) The same question may be asked for any multiplier set with k elements.

In the first work on splittings **[43]**, Stein considered only splittings of cyclic groups. Though it was not known at the time, cyclic groups are in a sense the easiest groups to split, as the following theorem of Hickerson [**23**] shows. It provides an affirmative answer to a question of Raphael Robinson.

THEOREM IV-1. *If $S(k)$ or $F(k)$ splits the finite abelian group G, then it splits the cyclic group of the same order as G, $C(|G|)$.*

This theorem is not true for all multiplier sets. For example, as shown in [**23**], $\{\pm 1, \pm 2, \pm 3, \pm 5, 7\}$ splits $C(2) \times C(2) \times C(7)$ but not $C(28)$. Theorem IV-1 is a consequence of this more general result in [**23**].

THEOREM IV-2. *Let M be a finite set of nonzero integers such that, for all primes p, the number of elements in M divisible by p is either 0 or at least $|M|/p^2$. Then if M splits the finite abelian group G, it splits $C(|G|)$.*

QUESTION IV-3. Which multiplier sets M have the property that if they split the finite abelian group G they split $C(|G|)$?

Since $S(p-1)$ splits any p-group when p is a prime, it is natural to consider a related question for $S(n-1)$ for any positive integer n. After all, $S(n-1)$ splits $C(n)$. It turns out that for composite n analogous splittings are quite rare, as the following theorem, proved in [**10**], shows.

THEOREM IV-3. *Let $G = C(n^{a_1}) \times \cdots \times C(n^{a_r})$, where $r \geqq 2$ and $a_i \geqq 1$ or else $r = 1$ and $a_1 \geqq 2$. If $S(n-1)$ splits G, then n is prime.*

In other words, if n is not prime and $S(n-1)$ splits a group G of the form described in the theorem, then $G = C(n)$.

Hamaker [**18**] showed that if $S(k)$ splits an abelian group of order $m > 2k + 1$, then $k^2 \leqq 2(m-1)$. This is equivalent to the assertion that in a **Z**-lattice tiling of $\mathbf{R}^n$ by the (k, n)-semicross, $n \geqq 3$, we have $k \leqq 2n$. Recently, Stein [**48**] reduced $2n$ to $n - 2$, which is best possible.

For a prime p, $S(p-1)$ splits $C(p^2)$ with a splitting set of $p + 1$ elements. This means that the $(p-1, p+1)$-semicross **Z**-lattice tiles R^{p+1}. These algebraic results and a related result from coding theory suggest the following geometric question.

QUESTION IV-4. If the (k, n)-semicross tiles $\mathbf{R}^n$, $n \geqq 3$, is $k \leqq n - 2$?

As we saw earlier, the determination of nonsingular splittings by $S(k)$ depends on which cyclic groups of prime order, $C(p)$, are split by $S(k)$. In such a splitting we may assume without loss of generality that $S(k)$ is a subset of $C(p)$ and that the splitting set contains 1. We have a factoring of $C(p)^*$,

$$C(p)^* = \{1, 2, \ldots, k\} \circ S.$$

Recall that $C(p)^*$ is a cyclic group of order $p - 1$. We might hope that S

is a subgroup of $C(p)^*$ and that the elements $1, 2, \ldots, k$ are its coset representatives. This need not be. For instance, $S(2)$ splits $C(17)$ with splitting set $\{1, 4, 4^2, 4^3\} \circ \{1, 3\}$ but not by the set $\{1, 9, 9^2, \ldots, 9^7\}$, which is the only subgroup of order 8. However, in certain circumstances we can assume that the splitting set is a group, as the following theorem of Sands [**41**] shows.

THEOREM IV-4. *Let G be a finite abelian group of order qm where q is a prime power and $(q, m) = 1$. Then if A has q elements and factors G, there is a subgroup $B \subseteqq G$ such that $A \circ B = G$.*

For instance, if $S(4)$ splits $C(p)$, where $p \equiv 5 (\mathrm{mod}\ 8)$ is prime, the hypotheses are satisfied: 4 is a prime power and G has order of the form $8x + 4 = 4(2x + 1)$; and $(4, 2x + 1) = 1$. As another example, if $S(5)$ splits $C(p)$, where $p \equiv 6, 11, 16$, or $21 (\mathrm{mod}\ 25)$ is prime, the condition is met. This covers four out of five cases since if $S(5)$ splits $C(p)$, we already have $p \equiv 1 (\mathrm{mod}\ 5)$; hence, $p \equiv 1, 6, 11, 16$, or $21 (\mathrm{mod}\ 25)$. Only the case $p \equiv 1 (\mathrm{mod}\ 25)$ is not covered. In this case, since p is odd, we have $p \equiv 1 (\mathrm{mod}\ 50)$. In any event Theorem IV-4 indicates that we may not lose much by restricting our search for splittings to the case where the splitting set is a subgroup of the multiplicative group $C(p)^*$.

QUESTION IV-5. For the multiplier set $S(5)$, what do the splittings of $C(p)$ for $p \equiv 1 (\mathrm{mod}\ 50)$ look like?

Assume that $S(k)$ splits $C(p)$ with the splitting set B, a subgroup of $C(p)^*$. Then there is an onto homomorphism

$$h: C(p)^* \to C(k) \quad (\cong C(p)^*/B),$$

and this homomorphism, when restricted to $S(k)$, is a bijection from $S(k)$ to $C(k)$. (Think of $C(p)^*$ as being written multiplicatively and $C(k)$ additively.) Conversely, if there is a homomorphism h: $C(p)^* \to C(k)$ which is one-to-one on $S(k)$, then $S(k)$ splits $C(p)$,

$$C(p)^* = S(k) \circ \text{kernel } h.$$

It turns out, as described in [**43**] and [**10**], that a theorem of Kummer and Mills from analytic number theory enables us to construct such homomorphisms if we can construct a function resembling a logarithm, from $S(k)$ to $C(k)$. This type of function is described in the following definition.

DEFINITION. Let k be a positive integer. A one-to-one function f: $S(k) \to C(k)$ is a k-logarithm if, for $1 \leqq x, y, xy \leqq k, f(xy) = f(x) + f(y)$.

Observe that a k-logarithm is determined by its values on the primes in the interval $[1, k]$. A computer search by Hickerson showed that, for $k \leqq 172$, there is a k-logarithm. In addition, for any k such that $k + 1$ is prime, there is a k-logarithm, namely the ordinary index. Also as shown in **[10]**, if $2k + 1$ is prime, then there is a k-logarithm.

QUESTION IV-6. Is there always a k-logarithm for each positive integer k?

The ability to extend a k-logarithm to a homomorphism $h\colon C(p)^* \to C(k)$ for some prime p depends on the following result, proved in **[31]**.

THEOREM IV-5. (KUMMER (k prime) and MILLS (k composite), PRESCRIBING HOMOMORPHISMS.) *Let $p_1, p_2, \ldots, p_r$ be distinct prime positive integers. Let $b_1, b_2, \ldots, b_r$ be elements of $C(k)$, the additive group of integers modulo k. Then there are an infinite number of primes p and onto homomorphisms*

$$h\colon C(p)^* \to C(k)$$

such that $h(p_i) = b_i$, $i = 1, 2, \ldots, r$ if and only if one of the following cases holds:

(1) *k is odd*;

(2) *$k = 2m$, m odd, for each $p_i \equiv 1$ (4) where $p_i | m$, b_i is even, and for all $p_i \equiv 3$ (4) such that $p_i | m$, all the b_i's have the same parity.*

(3) *$k = 4m$, and for each p_i that divides m, b_i is even.*

Moreover, if there is one such prime p, there is an infinite number of such primes.

This theorem directs our attention to a special type of k-logarithm.

DEFINITION. Let k be a positive integer. A k-logarithm that meets the hypotheses of Theorem IV-5 for all the primes in the interval $[1, k]$ is a KM-k-logarithm, or KM-logarithm for short.

For odd k, a KM-logarithm is just a k-logarithm.

Take $k = 32$ as an example which fits into case (3) of the Kummer-Mills theorem. We will show that there are an infinite number of primes p such that $S(32)$ splits $C(p)$. First we construct a KM-logarithm for $k = 32$. Keeping in mind that it is determined by its values at the primes $\leqq 32$, we obtain the following table. Note that $f(2)$ is even, as condition (3) requires. (There is a slight error in this example as given in **[10]**.) Assign f at the primes as shown here.

2	3	5	7	11	13	17	19	23	29	31
2	9	12	26	5	17	31	22	25	29	1

This determines f on $S(32)$ as shown below.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	2	9	4	12	11	26	6	18	14	5	13	17	28	21	8	31	20	22	16	3	7	25	15	24	19	27	30	29	23	1	10

(Note that since the primes 17, 19, 23, 29, 31 do not occur as products xy nor as factors of $xy \leqq 32$, the values of f at these numbers are free to be assigned after defining f at the primes $\leqq 16$, which is half of 32. That there are primes between $k/2$ and k encourages us to think that there are k-logarithms. These primes are like jokers in a game of cards and introduce some leeway in defining f.)

By the Kummer-Mills theorem there are an infinite number of primes $p \equiv 1(\text{mod } 32)$ and homomorphisms $h{:}C(p)^* \to C(32)$ that extend the above assignment. Since such an h is necessarily one-to-one on $S(32)$, $S(32)$ splits $C(p)$.

The Kummer-Mills theorem, together with the fact that $S(k)$ splits $C(k+1)$ with splitting set $\{1\}$ and splits $C(2k+1)$ with splitting set $\{1, -1\}$, show that if $k+1$ or $2k+1$ is prime, then $S(k)$ splits an infinite number of groups of prime orders.

Information about splittings by $S(k)$ can in turn provide information about the Kummer-Mills theorem.

THEOREM IV-6. *Assume that, for the integer k, there is a KM-logarithm. Then the smallest prime $p > 2k + 1$ for which there is a homomorphism $h{:}C(p)^* \to C(k)$ that extends that logarithm is greater than* $(k+1)^2$.

PROOF. Let p be a prime greater than $2k + 1$ for which there is such an extension h. By **[48]** the splitting set has at least $k + 2$ elements. Thus $p - 1 \geqq k(k+2)$, and the theorem follows.

B. *Packings by $S(k)$*. The problem of finding **Z**-lattice tilings of $\mathbf{R}^n$ by the (k, n)-semicross led us to consider splittings of finite abelian groups by the multiplier set $S(k)$. Finding **Z**-lattice packings of $\mathbf{R}^n$ by the (k, n)-semicross is equivalent to finding n elements, $g_1, g_2, \ldots, g_n$, in some finite abelian group G such that the kn elements ig_j, $1 \leqq i \leqq k$, $1 \leqq j \leqq n$, are distinct from each other and distinct from 0. We say that the elements $g_1, g_2, \ldots, g_n$ form a packing set for $S(k)$ in G and that $S(k)$ has an n-packing in G. As with tilings, the corresponding **Z**-lattice packing of $\mathbf{R}^n$ is formed by using as translation vectors the integer vectors $(x_1, x_2, \ldots, x_n)$ such that

$$x_1g_1 + x_2g_2 + \cdots + x_ng_n = 0 \in G.$$

The density of this packing is $(kn + 1)/a$, where a is the order of the subgroup of G generated by the set $\{g_1, g_2, \ldots, g_n\}$. Since we are looking for dense packings, we will assume that G is generated by $\{g_1, g_2, \ldots, g_n\}$. The density of the packing is therefore

$$\frac{kn + 1}{|G|}.$$

The problem of finding dense $\mathbf{Z}$-lattice packings of $\mathbf{R}^n$ by the (k, n)-semicross reduces to finding, for given positive integers k and n, the smallest abelian group G in which there is an n-packing of $S(k)$. Call that minimal order $g(k, n)$. Trivially, $g(k, 1) = k + 1$ and $g(k, 2) = 2k + 1$. The exact value of $g(k, n)$, $n \geqq 3$, is not known, though the asymptotic behavior of $g(k, n)$ for fixed $n \geqq 3$ and k large is known and will be described below. Affirmative answers to the next two questions would simplify the search for dense packings of $S(k)$ in groups.

QUESTION IV-7. If $S(k)$ n-packs a finite abelian group G does it n-pack $C(|G|)$?

As mentioned earlier, the answer is yes if the packing is a splitting.

QUESTION IV-8. If $S(k)$ n-packs a cyclic group $C(m)$ is there an n-packing of $C(m)$ in which the packing set contains 1? This may be asked for any multiplier set.

(The notion of packing extends in the obvious way to any multiplier set.)

The first work on packings appears in **[47]**, which is concerned with the multiplier sets $F(k)$ and $S(k)$. We will discuss packings by $S(k)$ first and packings by $F(k)$ in the next section.

By the remarks on p.298, for a prime p, $S(p - 1)$ $(p + 1)$-packs $C(p^2)$. Thus, for any prime p, $S(p - 1)$ 3-packs $C(p^2)$. Since the ratio between consecutive primes p_{n+1}/p_n, approaches 1 as $n \to \infty$, we conclude that, for any $\varepsilon > 0$, $S(k)$ 3-packs a group $C(m)$ where $m < (1 + \varepsilon)k^2$. The same conclusion holds for n-packings, $n = 4, 5, 6, \ldots$. However, a much stronger result holds, as will now be described.

For $n = 3$, which corresponds to packing semicrosses in $\mathbf{R}^3$, the following theorem was obtained in **[47]**.

THEOREM IV-7. *For* $n = 3$,

$$\lim_{k \to \infty} \frac{g(k, n)}{k^{3/2}} = 1.$$

The proof consists of two parts. First it is shown that if $S(k)$ 3-packs a finite abelian group G, then $|G| \geqq (k + 1)^3$. The argument uses the pigeon-hole principle and can yield the slightly stronger result, $k^3 + 3k^2 + k \leqq (|G| - 1)^2$. Second, it is shown that, for any positive integer b, $S(b^2 - b)$ 3-packs $C(b^3 + 1)$.

The packing set constructed for the 3-packing just mentioned is $\{1, -b, (-b)^2\}$. Since $(-b)^3 = 1$ in $C(b^3 + 1)$, the packing set is a subgroup of the multiplicative structure of the ring $Z(b^3 + 1)$.

This particular method of construction also gives some information in the case of 4-packings and 6-packings. It can be shown that, for a positive odd integer b, $S((b^2 - 1)/2)$ 4-packs $C((b + 1)\ (b^2 + 1)/2)$. From this it follows that

$$\overline{\lim_{k\to\infty}} \frac{g^2(k, 4)}{k^3} \leqq 2.$$

The packing set is the subgroup $\{1, -b, (-b)^2, (-b)^3\}$, with $(-b)^4 = 1$ since $(b + 1)\ (b^2 + 1)/2$ divides $b^4 - 1$. Similarly, we can show that, for $b \equiv 1 (\text{mod } 6)$, $S((b^2 + b - 2)/3)$ 6-packs $C((b^2 + b + 1)(b + 1)/3)$ with packing set $\{1, -b, (-b)^2, (-b)^3, (-b)^4, (-b)^5\}$. Hence,

$$\overline{\lim_{k\to\infty}} \frac{g^2(k, 6)}{k^3} \leqq 3.$$

In this approach, a packing set in the form of a subgroup is formed. The method rests on the fact that the polynomials $x^3 - 1$, $x^4 - 1$, and $x^6 - 1$ have cubic factors with certain properties. Both k and the order of the group, m, are expressible as polynomials in b with rational coefficients, m as a cubic and k as a quadratic. The limit of m^2/k^3 for $n = 3$, 4, and 6 is 1, 2, and 3 respectively. This approach does not generalize to other orders, and for good reason. It turns out, as shown in [23], that

$$\lim_{k\to\infty} \frac{g^2(k, n)}{k^3} = 4 \cos^2 \frac{\pi}{n},$$

which is rational only when $n = 3$, 4, or 6. For example, when $n = 5$, the limit is $(3 + \sqrt{5})/2$.

Nevertheless, this technique can be used to construct specific very tight packings. For instance, we will show that $S(5)$ 6-packs $C(35)$ with packing set $\{1, -4, (-4)^2, (-4)^3, (-4)^4, (-4)^5\}$. To begin, note that

$$4^6 - 1 = \underbrace{(4 - 1)}_{3}\ \underbrace{(4^2 + 4 + 1)}_{3\cdot 7}\ \underbrace{(4 + 1)}_{5}\ \underbrace{(4^2 - 4 + 1)}_{13}.$$

Thus $(-4)^6 \equiv 1 (\text{mod } 35)$. Next, we show that none of the congruences (i) $-4i \equiv j (\text{mod } 35)$, (ii) $(-4)^2 i \equiv j (\text{mod } 35)$, and (iii) $(-4)^3 i \equiv j (\text{mod } 35)$ have solutions where $1 \leqq i, j \leqq 5$.

Since $4i + j < 35$ for $1 \leqq i, j \leqq 5$, (i) has no such solution.

Assume next that $16i \equiv j (\text{mod } 35)$. Then $i \equiv j (\text{mod } 5)$, so $i = j$ and we have $16i \equiv i(\text{mod } 7)$; thus $2i \equiv i(\text{mod } 7)$ and, finally, $i \equiv 0(\text{mod } 7)$. Thus (ii) has no solution in the given range.

If (iii) holds, we have $-64i \equiv j(\text{mod } 5)$ or $i \equiv j(\text{mod } 5)$, hence $i = j$ and $-64i \equiv i(\text{mod } 7)$. Thus $65i \equiv 0(\text{mod } 7)$ and $i \equiv 0(\text{mod } 7)$, which is impossible for $1 \leqq i \leqq 5$.

From the fact that (i), (ii), and (iii) have no solutions in $S(5)$ and the fact that $(-4)^6 \equiv 1(\text{mod } 35)$, it follows that $\{(-4)^i | 0 \leqq i \leqq 5\}$ is a packing set.

Incidentally, this packing shows that there is a **Z**-lattice packing of $\mathbf{R}^6$ by the (5, 6)-semicross with density 31/35.

QUESTION IV-9. Let $r \geqq 3$ and $k \geqq 1$. Is $g(k, r)/(k+1)^{3/2} \geqq 2\cos(\pi/r)$?

QUESTION IV-10. What is the exact value of $g(k, r)$?

Even for $r = 3$ the answer is not clear. The following theorem, whose proof is similar to that in **[47]** for the special case $b = d$, is of some aid in examining $g(k, 3)$ for small values of k.

THEOREM IV-8. *Let b, k, d, and m be positive integers such that m divides $db^2 + 1$, and k is less than the minimum of $m/(b+1)$ and $m/(d+1)$. Then $S(k)$ 3-packs $C(m)$ with packing set $\{1, -b, bd\}$.*

For instance, the case $b = 4$, $d = 5$ shows that $S(13)$ 3-packs $C(81)$ with packing set $\{1, -4, 20\}$. The case $b = d = 5$ shows that $S(10)$ 3-packs $C(63)$. Theorem IV-8, together with some computations, provides the basis for Table IV-1, which lists some 3-packings.

The entry m in the second column corresponding to k in the first column records the fact that $S(k)$ 3-packs $C(m)$. For $1 \leqq k \leqq 6$, this was checked to equal $g(k, 3)$. For $7 \leqq k \leqq 9$, it was checked that m is the smallest order of a cyclic group that $S(k)$ 3-packs. The packing of $S(5)$ in $C(26)$ does not seem to fit into a pattern.

The final column records the density of the corresponding **Z**-lattice packing of $\mathbf{R}^3$ by the $(k, 3)$-semicross. The contrast of $k = 5$ and $k = 6$ shows that the **Z**-lattice packing density is not a monotonic function of k.

A word is in order concerning the geometry of these **Z**-lattices, in particular, their symmetry and bases.

Corresponding to the packing set $\{(-b)^i | 0 \leqq i \leqq n-1\}$, where $(-b)^n = 1$ is the **Z**-lattice in $\mathbf{R}^n$,

$$\text{(IV-1)} \quad L = \{(x_0, x_1, \ldots, x_{n-1}) | x_i \in \mathbf{Z}, \sum_{i=0}^{n-1}(-b)^i x_i \equiv 0(\text{mod } m)\}.$$

If $(x_0, x_1, \ldots, x_{n-1}) \in L$, we have

$$x_0 - bx_1 + b^2x_2 - \cdots + (-b)^{n-1} x_{n-1} \equiv 0(\text{mod } m),$$

k	m	Remark	**Z**-lattice packing density
1	4	Splitting	$4/4 \doteq 1.000$
2	9	$b = d = 2$ Smallest group	$7/9 \doteq 0.778$
3	13	$b = 2$, $d = 3$ Smallest group	$10/13 \doteq 0.769$
4	19	$b = 3$, $d = 2$ Smallest group	$13/19 \doteq 0.684$
5	26	Packing set $\{1, 12, 23\}$ Smallest group	$16/26 \doteq 0.615$
6	28	$b = d = 3$ Smallest group	$19/28 \doteq 0.679$
7	37	$b = 3$, $d = 4$ Smallest cyclic group	$22/37 \doteq 0.595$
8	49	See $k = 9$ Smallest cyclic group	$25/49 \doteq 0.510$
9	49	$b = 4$, $d = 3$, Smallest cyclic group	$28/49 \doteq 0.571$
10	63	$b = d = 5$	$31/63 \doteq 0.492$
11	65	See $k = 12$	$34/65 \doteq 0.523$
12	65	$b = d = 4$	$37/65 \doteq 0.569$
13	81	$b = 4$, $d = 5$	$40/81 \doteq 0.494$
16	101	$b = 5$, $d = 4$	$49/101 \doteq 0.485$
20	126	$b = d = 5$	$61/126 \doteq 0.484$
21	151	$b = 5$, $d = 6$	$64/151 \doteq 0.424$
25	181	$b = 6$, $d = 5$	$76/181 \doteq 0.420$
30	217	$b = d = 6$	$91/217 \doteq 0.419$
42	344	$b = d = 7$	$127/344 \doteq 0.369$

TABLE IV-1

hence, on multiplication by $-b$,

$$-bx_0 + b^2x_1 - b^3x_2 + \cdots + x_{n-1} \equiv 0 (\text{mod } m).$$

Thus, the point $(x_{n-1}, x_0, x_1, \ldots, x_{n-2})$ is also in L. The lattice is highly symmetric, being carried into itself by the cyclic group generated by the isometry T, where

$$T(x_0, x_1, \ldots, x_{n-1}) = (x_{n-1}, x_0, x_1, \ldots, x_{n-2}).$$

If $m = b^n - (-1)^n$, the lattice has a basis obtained from one vector v by the operation of T and its powers, namely the basis consisting of the n vectors

$$\begin{gathered}(b, 1, 0, \ldots, 0)\\ (0, b, 1, \ldots, 0)\\ \cdots\cdots\cdots\\ (0, \ldots, 0, b, 1)\\ (1, 0, \ldots, 0, b)\end{gathered}$$

(The determinant of the matrix formed by these n vectors equals $b^n - (-1)^n$, as can be seen by expanding it along the first column.) However, if m is less than $b^n - (-1)^n$, the lattice, though carried into itself by T, may not have a basis of the form $v, T(v), \ldots, T^{n-1}(v)$, which we will call a cyclic basis.

For instance, consider $n = 3$, $b = 5$, and $m = 21$, which divides $5^3 - (-1)^3 = 126$. The lattice $L = \{(x, y, z) \mid x - 5y + 25z \equiv 0 (\mathrm{mod}\ 21)\}$ has determinant 21. Assume that there is a vector $v = (x_0, y_0, z_0)$ such that $v, T(v), T^2(v)$ is a basis for L. We would then have $x_0 = 5y_0 - 25z_0 + 21q$, $q \in \mathbf{Z}$, and

$$\begin{vmatrix} x_0 & y_0 & z_0 \\ z_0 & x_0 & y_0 \\ y_0 & z_0 & x_0 \end{vmatrix} = \pm 21,$$

that is

$$x_0^3 + y_0^3 + z_0^3 - 3x_0y_0z_0 = \pm 21. \qquad \text{(IV-2)}$$

We claim (IV-2) has no integer solutions with $x_0 = 5y_0 - 25z_0 + 21q$.

First of all, $x_0 = 5y_0 - 4z_0 + 21t$, $t \in \mathbf{Z}$, so that $x_0 \equiv 5(y_0 + z_0) + 3t$ (mod 9). Then

$$\begin{aligned} & x_0^3 + y_0^3 + z_0^3 - 3x_0y_0z_0 \\ &\quad \equiv (5(y_0 + z_0) + 3t)^3 + y_0^3 + z_0^3 - 3(5(y_0 + z_0) + 3t)y_0z_0 (\mathrm{mod}\ 9) \\ &\quad \equiv 125(y_0 + z_0)^3 + y_0^3 + z_0^3 - 15(y_0 + z_0)y_0z_0 (\mathrm{mod}\ 9) \\ &\quad \equiv -(y_0 + z_0)^3 + y_0^3 + z_0^3 + 3(y_0 + z_0)y_0z_0 (\mathrm{mod}\ 9) \\ &\quad \equiv 0 (\mathrm{mod}\ 9) \end{aligned}$$

Since 9 does not divide 21, (IV-2) cannot hold.

However, the case $n = 3$, $b = 5$, and $m = 63$, another divisor of 126, is quite different. The corresponding lattice does have a cyclic basis, v, $T(v)$, $T^2(v)$, where $v = (3, -2, 2)$. So is the case $n = 3$, $b = 5$, and $m = 9$, where $v = (1, 2, 0)$ works.

Question IV-11. When does a $\mathbf{Z}$-lattice in $\mathbf{R}^n$ that is invariant with respect to the cyclic permutation T, $T(x_1, x_2, \ldots, x_n) = (x_n, x_1, \ldots, x_{n-1})$ have a cyclic basis?

Even for lattices L in $\mathbf{R}^3$ whose quotient group $\mathbf{Z}^3/L$ is not cyclic the question is of interest. Consider, for instance, a positive integer n and let $L = \{(x, y, z) \mid x \equiv y \equiv z (\mathrm{mod}\ n)\}$. In this case, $\mathbf{Z}^3/L \approx C(n) \times C(n)$, since the homomorphism from $\mathbf{Z}^3$ to $C(n) \times C(n)$ given by $(x, y, z) \to (x - y, y - z)$ is onto and has L as its kernel. L is symmetric with respect to T. The following theorem tells when a cyclic base can be found for L.

THEOREM IV-9. *For the positive integer n, the lattice $L = \{(x, y, z) | x \equiv y \equiv z (\mathrm{mod}\ n)\}$ has a cyclic basis if and only if n is not a multiple of* 3.

PROOF. If $n \not\equiv 0(\mathrm{mod}\ 3)$, consider the vector $v = (x + n, x, x) \in L$ for which the determinant of the matrix formed of v, $T(v)$, $T^2(v)$ equals $n^2(n + 3x)$. If $n \equiv 1(\mathrm{mod}\ 3)$, there is an integer x such that $n + 3x = 1$ and the determinant then equals n^2. If $n \equiv -1(\mathrm{mod}\ 3)$, x can be chosen so the determinant equals $-n^2$.

If $n \equiv 0(\mathrm{mod}\ 3)$, consider the arbitrary vector $v \in L$, which has the form $(x, x + nb, x + nc)$ for some integers x, b, and c. The determinant,

$$\begin{vmatrix} x & x + nb & x + nc \\ x + nc & x & x + nb \\ x + nb & x + nc & x \end{vmatrix}$$

equals

$$3n^2xc^2 - 3n^2xbc + 3n^2xb^2 + n^3b^3 + n^3c^3,$$

which, being divisible by $3n^2$, cannot equal n^2. This concludes the proof.

In the reverse direction, assume that the lattice

$$\text{(IV-3)} \quad L = \{(x_0, x_1, \ldots, x_{n-1}) | x_0 + a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1} \equiv 0(\mathrm{mod}\ m)\}$$

is invariant under the isometry T given earlier. Then, for all choices of the integers $x_1, x_2, \ldots, x_{n-1}$, the point $(x_{n-1}, x_0, x_1, \ldots, x_{n-2})$ lies in L if $(x_0, x_1, \ldots, x_{n-1})$ does. Thus

$$\text{(IV-4)} \quad x_{n-1} + a_1(-a_1x_1 - a_2x_2 - \cdots - a_{n-1}x_{n-1}) + a_2x_1 + a_3x_2 + \cdots + a_{n-1}x_{n-2} \equiv 0(\mathrm{mod}\ m).$$

for all choices of $x_1, x_2, \ldots, x_{n-1}$ in $\mathbf{Z}$. Comparison of coefficients in (IV-4) shows that

$$-a_1^2 + a_2 \equiv 0(\mathrm{mod}\ m), \ -a_1a_2 + a_3 \equiv 0(\mathrm{mod}\ m) \cdots$$
$$- a_1a_{n-2} + a_{n-1} \equiv 0(\mathrm{mod}\ m) \text{ and } 1 - a_1a_{n-1} \equiv 0(\mathrm{mod}\ m).$$

Hence $a_2 \equiv a_1^2$, $a_3 \equiv a_1a_2 \equiv a_1^3, \ldots, a_{n-1} \equiv a_1^{n-1}$, and $a_1^n \equiv 1$. Thus the congruence in (IV-3) has the form (IV-1), with $a_1 = -b$.

Incidentally, in case $n + 1 = p$, a prime, the $(1, n)$-semicross $\mathbf{Z}$-lattice tiles $\mathbf{R}^n$ by a lattice that is invariant with respect to T. In a suitable indexing of the coordinates, the lattice is described by the congruence

$$x_1 + 2x_2 + \cdots + nx_n \equiv 0(\mathrm{mod}\ p = n + 1).$$

Since $C(p)^*$ is cyclic, with generator g, say, after reindexing the coordinates, the preceding congruence takes the form

$$x_1 + gx_2 + g^2x_3 + \cdots + g^{n-1}x_n \equiv 0(\text{mod } p),$$

with $g^n \equiv 1(\text{mod } p)$. This shows that the lattice is invariant with respect to T.

In this section we considered **Z**-lattice tilings and packings by the (k, n)-semicross. **Z**-lattice coverings have scarcely been examined. In $\mathbf{R}^1$ and $\mathbf{R}^2$ every semicross tiles and in $\mathbf{R}^3$ the $(1, 3)$-semicross does. So the first interesting case is the covering density of the $(2, 3)$-semicross. If we consider only **Z**-lattice coverings, the problem becomes: What is the largest order of an abelian group G for which there are three elements g_1, g_2, g_3 in G such that each nonzero element of G is of the form ig_j, $i = 1, 2, j = 1, 2, 3$? Call such a set a covering set in G. The answer is 6. In $C(6)$ there is the covering set $\{1, 3, 5\}$ for $S(2)$. Thus there is a lattice covering of $\mathbf{R}^3$ by the $(2, 3)$-semicross with density $7/6$.

QUESTION IV-12. Let k and n be positive integers. What is the order of the largest abelian group G such that there are n elements in G, $g_1, g_2, \ldots, g_n$, with the property that each nonzero element of G is of the form ig_j, $1 \leqq i \leqq k$, $1 \leqq j \leqq n$?

V. $\mathbf{M = F(k) = \{\pm 1, \pm 2, \ldots, \pm k\}}$. This section, motivated by the full cross, parallels the preceding section, which concerned the algebra of tilings and packings by the semicross.

A. *Splittings by* $F(k) = \{\pm 1, \pm 2, \ldots, \pm k\}$. If $2k + 1$ is a prime, p, then $F(k)$ splits $C(p)$, hence any finite abelian p-group. Furthermore, by Theorem IV-1, if $F(k)$ splits the finite abelian group G, then it splits the cyclic group $C(|G|)$. It is easy to see that $F(1)$ splits any abelian group of odd order. It is not known whether $F(k)$ always splits an abelian group of order greater than $2k + 1$. It is an easy consequence of the pigeonhole principle that the order of such a group would have to be at least $(k + 1)^2$. (See [43] or [47].) This is equivalent to the assertion that if $F(k)$ splits a finite abelian group of order greater than $2k + 1$, then the splitting set has at least

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

elements. For odd k, therefore, the splitting set has at least $(k + 3)/2$ elements and the group has order at least $(2k)\ (k + 3)/2 + 1 = k^2 + 3k + 1$.

These are probably far from the best lower bounds. If $2k + 1$ is prime, then $F(k)$ splits $C((2k + 1)^2)$, which is a group of order $4k^2 + 4k + 1$; the splitting set has $2k + 2$ elements. Letting $r(k)$ be the order of the smallest group of order greater than $2k + 1$ that $F(k)$ splits (assuming that there is such a group), we have

$$r(k) \geqq (k + 1)^2$$

and, when $2k + 1$ is prime,

$$r(k) \leqq (2k + 1)^2.$$

QUESTION V-1: How does $r(k)$ behave for large k?

There is a complication in using the Kummer-Mills theorem to produce splittings by $F(k)$. Consider for instance splittings by $F(6)$. Let f be the KM-logarithm

$$f \Big\downarrow \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 3 & 2 & 5 & 4 \end{array}.$$

There is an infinite number of primes $p \equiv 1 (\text{mod } 6)$ and homomorphisms h: $C(p)^* \rightarrow C(6)$ that extend f. If $p \equiv 1(\text{mod } 12)$, then the kernel of h has an even number of elements and therefore contains the subgroup $\{1, -1\}$. The kernel is therefore factorable in the form $\{1, -1\} \circ A$, and we have the factorization of $C(p)^*$,

$$\{1, 2, 3, 4, 5, 6\} \circ \{1, -1\} \circ A = C(p)^*$$

or

$$F(6) \circ A = C(p)^*.$$

However, the Kummer-Mills theorem does not guarantee the existence of $p \equiv 1(\text{mod } 12)$ for which f extends to a homomorphism from $C(p)^*$ to $C(6)$.

As Mills pointed out in correspondence, a slight variation in the construction will give $p \equiv 1(\text{mod } 12)$. Instead of working with $C(6)$, work with $C(12)$. Define f: $\{1, 6\} \rightarrow C(12)$ by the table below.

$$\mathrm{f} \Big\downarrow \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 2 & 3 & 5 \end{array}.$$

Since $f(3)$ is even, condition (3) of the Kummer-Mills theorem is satisfied. There are therefore an infinite number of primes $p \equiv 1(\text{mod } 12)$ and corresponding homomorphisms h: $C(p)^* \rightarrow C(12)$ extending f. Let g: $C(12) \rightarrow C(12)/\{0, 6\}$ be the natural homomorphism. Then $g \circ h$ is a homomorphism from $C(p)^*$ to $C(6)$ that induce a $1 - 1$ correspondence between $\{1, 2, 3, 4, 5, 6\}$ and $C(6)$.

B. *Packings by $F(k)$*. Let $h(k, n)$ be the smallest order of a finite abelian group that $F(k)$ n-packs. This function was investigated in **[47]** after 3-packings by $S(k)$.

Trivially, $h(k, 1) = 2k + 1$. It was shown geometrically in **[8]** that

$h(k, 2) = k^2 + 2k + 2$, hence that $h(k, n) \geqq k^2 + 2k + 2$ for $n \geqq 3$. The following theorem obtained in [**47**] contrasts with the corresponding result on packings by $S(k)$ in two respects, i.e., n does not influence the limit and the exponent is 2 instead of 3/2.

THEOREM V-1. *For* $n \geqq 2$,

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

The proof consists of constructing packing sets in the form of an arithmetic progression supplemented by 1 rather than a geometric progression, which was used to construct packings for $S(k)$. The examples in Table V-1 can be justified by the technique used in [**47**]

n = size of packing set	Packing set	Order of cyclic group packed	Condition
2	$1, k + 1$	$k^2 + 2k + 2 = (k + 1)^2 + 1$	k even
3	$1, k + 1, k + 2$	$k^2 + 3k + 3$	
4	$1, k + 1, k + 2, k + 3$	$k^2 + 4k + 5 = (k + 2)^2 + 1$	k even
5	$1, k + 1, k + 3, k + 5, k + 7$	$k^2 + 8k + 9$	k even, $k \not\equiv 2 (\mathrm{mod}\ 3)$
6	$1, k + 11, k + 13, k + 15, k + 17, k + 19$	$k^2 + 30k + 233$	$k \equiv 0 (\mathrm{mod}\ 6)$

TABLE V-1

These examples were found while searching for packing sets in the form of geometric progressions. (It was also expected that the lattice of a dense packing would have a good deal of symmetry.) In fact, consider the case $n = 3$. The powers of $k + 1$ in $C(k^2 + 3k + 3)$ are $(k + 1)^2 = -(k + 2)$ and $(k + 1)^3 = 1$. Thus, the given packing set equals $\{1, k + 1, -(k + 1)^2\}$ with $(k + 1)^3 = 1$. Hence the geometric progression $\{1, k + 1, (k + 1)^2\}$ is also a packing set, since changing the sign of an element in a packing set for $F(k)$ produces another packing set.

In the proof of Theorem V-1 a packing set of n elements for $F(k)$ was constructed in the cyclic group of order $k^2 + uk + v$, where the integers u and v depend on n but not on k. The number u is on the order of $(n^2/2)$ LCM$\{1, 2, \ldots, n\}$, which is probably much larger than necessary, as Table V-1 indicates. However, even Table V-1 may not give a good estimate of $h(k, n)$.

For $n = 2$, $h(k, n)$ is given by the formula $k^2 + 2k + 2$ in the table.

For $n = 3$ it was checked that, for $1 \leqq k \leqq 6$, the order of the smallest cyclic group that $F(k)$ 3-packs is given by the formula $k^2 + 3k + 3$. For 4-, 5-, and 6-packings the orders of the groups given in Table V-1 diverge rapidly from $h(k, n)$, as the Tables V-2, 3, 4 show.

Table V-2 lists the order of the smallest cyclic group that $F(k)$ 4-packs for $1 \leqq k \leqq 6$.

k	Order of group	Remark
1	9	Split by $\{1, 2, 3, 4\}$
2	17	Split by $\{1, 4\} \circ \{1, 3\}$
3	30	Packed by $\{1, 4, 5, 7\}$
4	37	Packed by $\{1, 5, 6, 7\}$
5	61	Packed by $\{1, 9, 11, 23\}$
6	65	Packed by $\{1, 7, 8, 9\}$

TABLE V-2 (4-packs)

Table V-3 lists some cyclic groups in which $F(k)$ has a 5-packing.

k	Order of group	Remark
1	11	Split by $\{1, 2, 3, 4, 5\}$
2	22	Packed by $\{1, 3, 5, 7, 9\}$, which is, up to sign, $\{1, 3, 3^2, 3^3, 3^4\}$, $3^5 = 1$
3	35	Packed by $\{1, 5, 6, 8, 13\}$, which is, up to sign, $\{5\} \cup \{1, 8, 8^2, 8^3\}$, $8^4 = 1$
4	45	Theorem V-2(b)
5	70	Packed by $\{1, 7, 8, 9, 11\}$
6	82	Packed by $\{1, 23, 23^2, 23^3, 23^4\}$, $23^5 = -1$

TABLE V-3 (5-packs)

Table V-4 lists some cyclic groups in which $F(k)$ has a 6-packing.

k	Order of group	Remark
1	13	Split by $\{1, 2, 3, 4, 5, 6\}$
2	25	Splitting, since $F(2)$ splits $C(5)$
3	43	Packing set $\{1, 5\} \circ \{1, 6, 6^2\}$, which is, up to sign, $\{1, 5, 6, 7, 8, 13\}$
4	50	Theorem V-2 (a)
5	77	Theorem V-2 (d)
6	85	Packed by $\{1, 7, 8, 11, 36, 38\}$

TABLE V-4 (6-packs)

Some of these packings are based on the following theorem.

THEOREM V-2. (a) *For any odd prime p, $F(p-1)$ $(p+1)$-packs $C(2p^2)$ and $C(p) \times C(2p)$.*

(b) *For any prime p, $F(p-1)$ p-packs $C(p) \times C(2p-1)$, which is $C(p(2p-1))$.*

(c) *For any prime p and integer $n \geqq 2p-1$, $F(p-1)$ p-packs $C(p) \times C(n)$.*

(d) *For r relatively prime to $k!$ and $s > 2k$, $F(k)$ r-packs $C(r) \times C(s)$.*

PROOF. (a) It is easy to check that

$$\{1, 2p \pm 1, 4p \pm 1, \ldots, 2\frac{p-1}{2}p \pm 1\} \cup \{p\}$$

and

$$\{(0,1), (1,1), \ldots, (p-1, 1)\} \cup \{(1, p)\}$$

are packing sets for $F(p-1)$ in the respective groups $C(2p^2)$ and $C(p) \times C(2p)$.

(b), (c), and (d) are successively more general. For (d) the packing set $\{(0,1), (1,1), \ldots, (r-1, 1)\}$ suffices.

The packings in Theorem V-2 (a) come very close to being splittings since $2(p-1)(p+1) = 2p^2 - 2$, only 2 less than the order of the group. (In the first case, p^2 is not covered, and in the second, $(0, p)$.) Thus, for odd primes p, the $(p-1, p+1)$-cross, expanded by one cube at the end of one arm, tiles $\mathbf{R}^{p+1}$ in at least two ways.

QUESTION V-2. For which primes p does $F(p-1)$ split $C(2p^2-1)$?

QUESTION V-3. If $F(n-1)$ $(n+1)$-packs $C(2n^2)$, must n be prime?

We may also examine how well $F(k)$ packs large groups when k is fixed. As the next theorem shows, in this case $F(k)$ comes near splitting the groups.

THEOREM V-3. *Let $F(k)$ split two groups of prime order, $C(p)$ and $C(q)$. Then*

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

PROOF. Since $F(k)$ splits $C(p)$ and $C(q)$, it splits all groups $C(p^i q^j)$ where i and j are nonnegative integers. Using the fact that $\log p$ and $\log q$ are linearly independent over $\mathbf{Q}$, it is easy to show that in the sequence of integers $p^i q^j$, arranged by increasing size, the ratio between successive terms approaches 1.

If $2kn + 1$ is of the form $p^i q^j$, then $h(k, n) = 2kn + 1$. If $2kn + 1$ is not of that form, let m be the smallest integer of the form $p^i q^j$ that is larger than $2kn + 1$. Since $h(k, n) \leqq m$ and $m/(2kn + 1)$ is close to 1 when n is large, it follows that $\lim_{n\to\infty} h(k, n)/(2kn + 1) = 1$.

The hypothesis of Theorem V-3 holds if $2k + 1$ is prime, by the Kummer-Mills theorem. For instance, when n is large, the $(6, n)$-cross packs $\mathbf{R}^n$ with a density near 1 (and equals 1 for an infinite number of n). This means that crosses with arms that are short with respect to the dimension pack very well.

From the fact that for prime p, $F(p - 1)(p + 1)$-packs $C(2p^2)$, it follows that

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

This means that, for large dimension when the arm length of the cross equals the dimension of the space, the cross packs that space very densely.

VI. Origins. The general history of clusters is too long and varied to be covered here. However, the origins of the study of the cross and semicross are simple, though they can be traced back to several independent sources: Ulrich in 1957, Kárteszi in 1966, Stein in 1967, and Golomb and Welch in 1968.

Ulrich [**55**] constructed single-error correcting codes for alphabets of more than two symbols. His equation $X_1 + 2X_2 + 3X_3 + 4X_4 \equiv 0 (\mathrm{mod}\ 10)$ utilizes a packing of $\{1, -1\}$ in $C(10)$. (See [**55**, p.1349].). On p. 1351 he presents the equivalent of a splitting of $C(5) \times C(5)$ by $\{1, -1\}$. Later, pp. 1362–3, he shows essentially that $\{(1,4), (1, 3), (1,2), (1, 1), (1, 0), (0, 1)\}$ is a splitting set for $\{1, 2, 3, 4\}$ in $C(5) \times C(5)$ and remarks that "the number base must be prime". However, this paper did not lead to subsequent investigations of crosses or semicrosses in Euclidian space.

Kárteszi [**25**] asked whether the (1, 3)-cross tiles space. This was answered by Freller [**9**] in 1970; Korchmâros [**27**] about the same time treated $n > 3$. Molnar [**32**] in 1971 related the number of $\mathbf{Z}$-lattice tilings of $\mathbf{R}^n$ by the $(1, n)$-cross to the number of abelian groups of order $2n + 1$. Medyanik [**30**], apparently unaware of Molnar's work, showed in 1977 that the $(1, n)$-cross tiles $\mathbf{R}^n$.

Around 1963 I posed the following problem. Consider the standard lattice of unit squares that partition the plane. What is the smallest density of a set S of such squares with the property that every square from the lattice has at least one edge on the border of a square in S? That the answer is 1/5 follows immediately from the fact that the (1, 2)-cross tiles the plane. (Each cross must contain at least one member of S; hence, the density of S is at least 1/5. On the other hand, the set of center squares of the crosses in the tiling serves as a suitable family S.) This initiated my work in (k, n)-crosses and semicrosses, which first appeared in 1967 [**43**].

Golomb and Welch [**13**] showed that the $(1, n)$-cross tiles $\mathbf{R}^n$. They thought of the center of a cross as a code word and the other cubes of the cross as words that might be received if there were an error in one coordinate of the code word. A tiling then corresponds to a perfect code.

In 1978, Szabó [**49**], stimulated by Molnar's work, considered tilings by "lopsided" crosses, where at each facet of the central cube either no cube or one cube is attached. Around that time he read a Russian translation of [**45**] and became familiar with the papers of Hamaker and Stein; in 1981 he proved in [**51**] that if $2n + 1$ is not prime, then there is a nonlattice **Z**-tiling by the $(1, n)$-cross and a **Q**-lattice tiling that is not a **Z**-tiling.

References

1. A. Adler and F.C. Holroyd, *Some results on one-dimensional tilings*, Geom. Dedicata **10** (1981), 49–58.

2. R.P. Bambah, Math. Reviews **47** (1976), #7604.

3. ———, V.C. Dumir, and R.J. Hans-Gill, *Covering by star domains*, Indian J. Pure Appl. Math. **8** (1977), 344–350.

4. R. Bantegnie, *Elements Cristallographiques*, Acta Math. Acad. Sci. Hung. **30** (1977), 283–302.

5. F.W. Barnes, *Algebraic theory of brick packing*. I, Discrete Math. **42** (1982), 7–26.

6. F.W. Barnes, *Algebraic theory of brick packing* II, ibid., 129–144.

7. H. Davenport and C.A. Rogers, *On the critical determinant of cylinders*, Quart. J. Math Oxford (2), **1** (1950), 215–218.

8. H. Everett and D. Hickerson, *Packing and covering by translates of certain nonconvex bodies*, Proc. Amer. Math. Soc. **75** (1979), 87–91.

9. M. Freller, *Egy térkitöltési feladat*, *MTA* III, Osztaly Közlemenyei, **21** (1972), 71–72.

10. S. Galovich and S. Stein, *Splittings of abelian groups by integers*, Aequations Math. **22** (1981), 249–267.

11. S. Galovich, J. Goldfeather, S. Seltzer, and K. Smith, *Splittings of infinite abelian groups*, Aequations Math. (to appear).

12. M. Gilpin and R. Shelton, *Forced differences between terms of subsequences of integer sequences*, Proc. Amer. Math Soc. **88** (1983), 569–578.

13. S. Golomb and L. Welch, *Perfect codes in the Lee metric*, Univ. Southern California, USCEE report **249** (1968), 1–24.

14. B. Gordon, *Tilings of lattice points in Euclidean n-space*, Discrete Math. **29** (1980), 69–174.

15. H. Groemer, *Über gewisse dichteste Anordnungen von Punkten in der Ebene*, Archiv der Math. **15** (1964), 385–387.

16. P. Gruber, *Geometry of numbers*, *Contributions to Geometry*, Proc. Geometry Symposium in Siegen 1978, Ed. Jürgen Tölke and Jörg M. Wills.

17. G. Hajós, *Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Wurfelgitter*, Math. Z. **47** (1942), 427–467.

18. W. Hamaker, *Factoring groups and tiling space*, Aequationes Math. **9** (1973), 145–149.

19. ——— and S. Stein, *Splitting groups by integers*, Proc. Amer. Math. Soc. **46** (1974), 322–324.

20. ———, *Combinatorial packing of* $\mathbf{R}^3$ *by certain error spheres*, IEEE Transactions Inf. Theory **30** (1984), 364–368.

21. J.R. Henderson and R. Dean, *The* 1-*width of* (0, 1)-*matrices having constant row sum* 3, J. Comb. Th. (A) **16** (1974), 355–370.

22. ———, *A general upper bound for* 1-*widths*, J. Comb. Th. (A) **18** (1975), 236–238.

23. D. Hickerson, *Splittings of finite groups*, Pacific J. Math. **107** (1983), 141–171.

24. ——— and S. Stein, *Abelian groups and packing by semicrosses*, Pacific J. Math. (to appear).

25. F. Kárteszi, *Szemléletes geometric*, Gondolat, Budapest (1966).

26. M.S. Klamkin and A. Liu, *Polyominoes on the infinite checkerboard*, J. Comb. Th. (A) **29** (1980), 7–16.

27. G. Korchmáros, *Egy n-dimenzios mozaik*, Manuscript, Eötvös Loránd University, Budapest, (1971).

28. P. Loomis, *The covering constant of a certain symmetric star body*, Sitzungsberichte der osterreichischen Akadamie der Wissenschaften (1984), 295–308.

29. G.G. Lorentz, *On a problem in additive number theory*, Proc. Amer. Math. Soc. **5** (1954), 838–841.

30. A.I. Medyanik, *Razbienie* E^n *na prostranstvyenie kryesti*, Ukrainskii Geo. Sbornik **23** (1980), 84–90 (in Russian).

31. W.H. Mills, *Characters with preassigned values*, Canad. J. Math. **15** (1963), 169–171.

32. E. Molnar, *Sur mosaici dello spazio di dimensione n*, Accad. Naz. dei Lincei Rend., Ser. 8, **51** (1971), 177–185.

33. D.J. Newman, *Complements of finite sets of integers*, Mich. Math. J. **14** (1967), 481–486.

34. ———, *Tesselation of integers*, J. Number Theory **9** (1977), 107–111.

35. K.A. Post, *On the nonexistence of periodic tilings with cubistic cross-polytopes*, Technological University Eindhoven, Department of Mathematics, Report 79-WSK-07, November 1979, 1–15.

36. R.M. Robinson, *Undecidability and nonperiodicity for tilings of the plane*, Inventiones Math. **12** (1971), 177–209.

37. ———, *Multiple tilings of n-dimensional space by unit cubes*, Math. Z. **166** (1979), 225–264.

38. C.A. Rogers, *The closest packing of convex* 2-*dimensional domains*, Acta Math. **86** (1951), 309–321.

39. ———, *Packing and Covering*, Cambridge, 1964.

40. E.K. Rooney, Lattice coverings of the plane by a cross (ms).

41. A.D. Sands, *On a problem of L. Fuchs*, J. London Math. Soc. **37** (1962), 277–284.

42. ———, and S. Swierczkowski, *Decomposition of the line in isometric three-point sets*, Fund. Math. **48** (1960), 361–362.

43. S. Stein, *Factoring by subsets*, Pacific J. Math. **22** (1967), 523–541.

44. ———, *A symmetric star body that tiles but not as a lattice*, Proc. Amer. Math. Soc. **36** (1972), 543–548.

45. ———, *Algebraic tiling*, Amer. Math. Monthly **81** (1974), 445–462.

46. ———, *Two combinatorial covering theorems*, J. Comb. Theory **16** (1974), 391–397.

47. ———, *Packings of* $\mathbf{R}^n$ *by certain error spheres*, IEEE Transactions Inf. Theory-**30** (1984), 356–363.

48. ———, *Upper bound on arm length of a lattice-tiling semicross*, Studia Scien., Math. Hung. (to appear).

49. S. Szabó, *Veges abel-czoportok és n-dimenziós mazaikok*, Mat. Lapok **28** (1980), 305–318.

50. ———, *On decomposing finite abelian groups*, Acta Math. Acad. Scien. Hung **36** (1980), 105–114.

51. ———, *On mosaics consisting of multidimensional crosses*, Acta Math. Acad. Sci. Hung. **39** (1981), 191–203.

52. ———, *Rational tilings by n-dimensional crosses*, I, Proc. Amer. Math. Soc., to appear.

53. ———, *Rational tilings by n-dimensional crosses*, II.

54. P. Tong, *Splittings of* $C(2^n)$ (correspondence).

55. W. Ulrich, *Non-binary error correction codes*, The Bell System Technical Journal, November 1957, 1341–1388.

56. G. Weinstein, *Minimal complementary sets*, Trans. Amer. Math. Soc. **212** (1975), 131–137.

57. ———, *Some covering and packing results in number theory*, J. Number Theory, **8** (1976), 193–205.

58. M.R. von Wolff, *A star domain with densest admissible point set not a lattice*, Acta Math. **108** (1962), 53–60.

59. H. Zassenhaus, *Modern developments in the theory of numbers*, Bull. Amer. Math. Soc., **67** (1961), 426–439.

MATHEMATICS DEPARTMENT, UNIVERSITY OF CALIFORNIA AT DAVIS DAVIS, CA 95616

Added in Proof. S. Szabó, in *A bound for k for tiling by* (k, n) *crosses and semicrosses*, Acta Marth. Hung. **44** (1–2) (1984), 97–99, showed that if $n \geqq 2$ and the (k, n)-cross lattice tiles Z_n, then $k \leqq n - 1$. S. Stein, in *Splitting groups of prime order* (ms.) obtains criteria for splitting $C(P)$, p prime, incidentally obtaining sets of integers that split no group.