Lattice Packings by Clusters of Cubes

in Coding Theory

Ulrich Tamm

Bielefeld

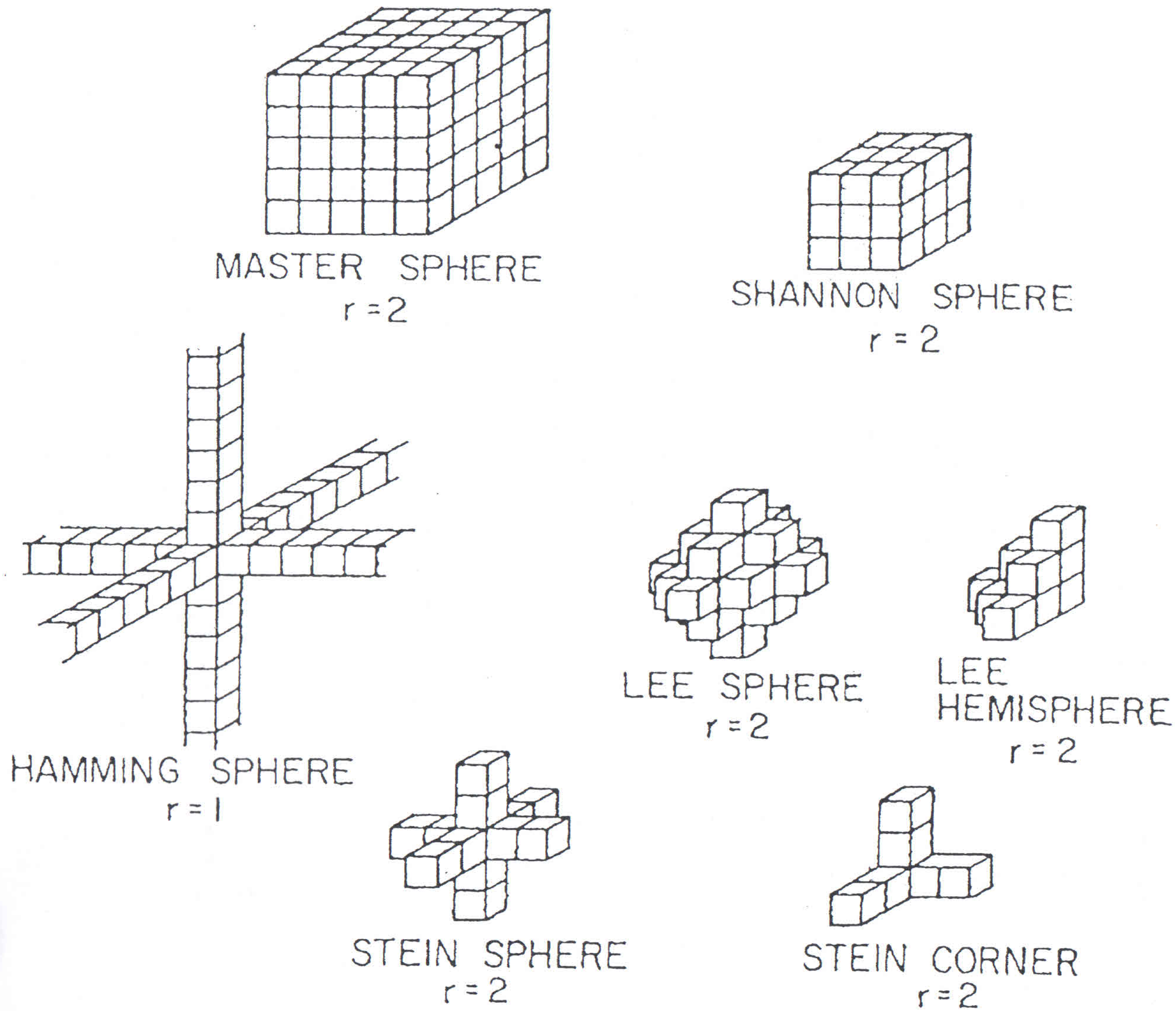


Fig. 1. Three-dimensional spheres of radius ≤ 2 in several different metrics.

Tiling and Packing

of:

1) n–space R^n

2) products of cycles or paths $\{0, 1, \ldots, m-1\}^n$

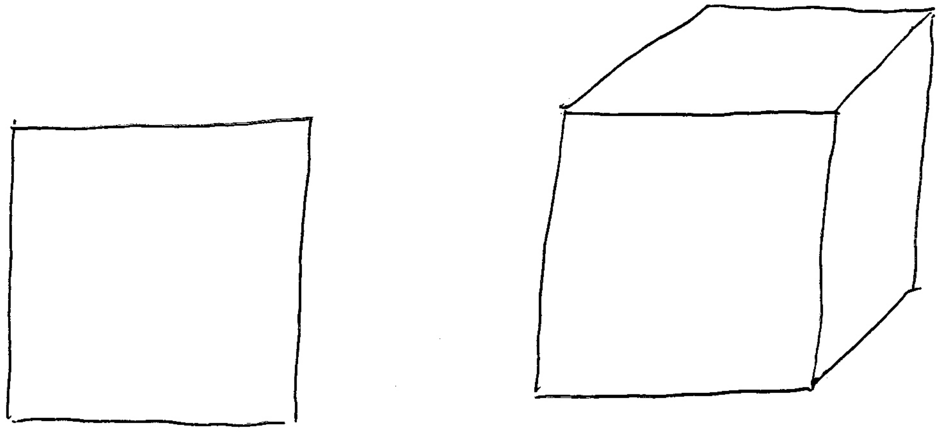
by clusters of unit cubes

a) unit cubes $\longrightarrow$ Number Theory

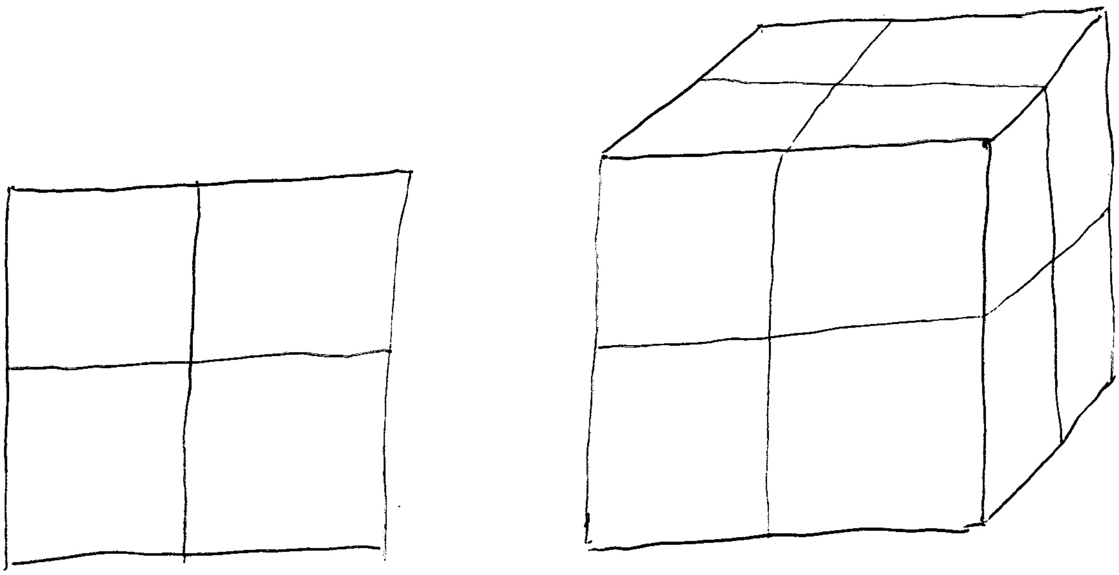
b) cubes of side length 2 $\longrightarrow$ Graph Theory

c) cross and semicross $\longrightarrow$ Coding Theory

Clusters of Cubes (unit)



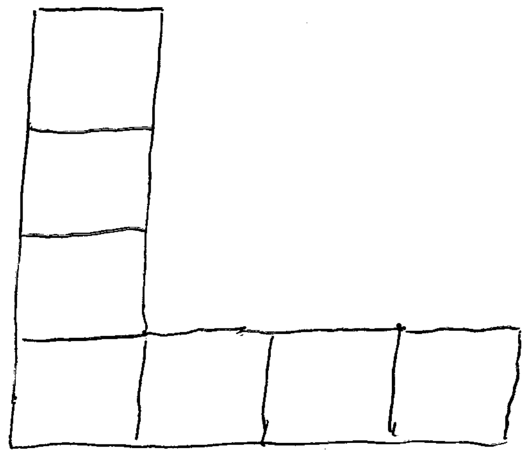
single cube



2^n unit cubes

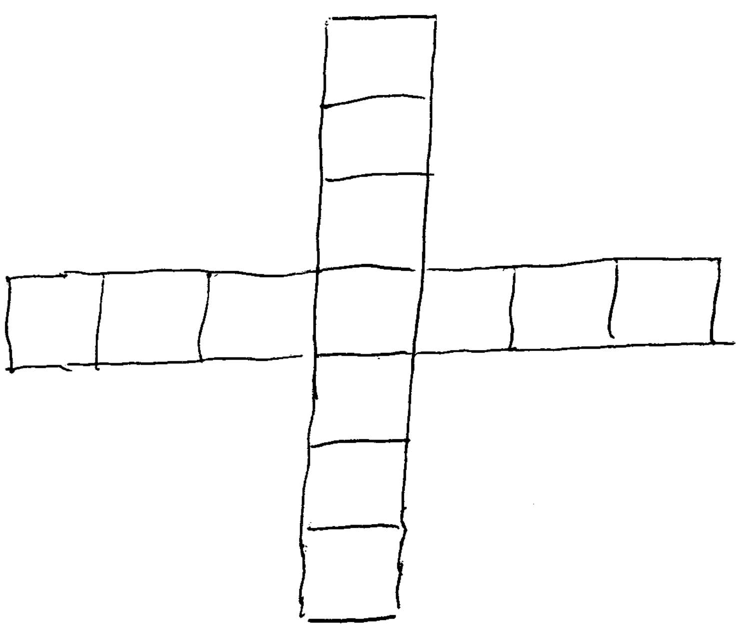
→ cube of side length 2

(k, n) - semicross



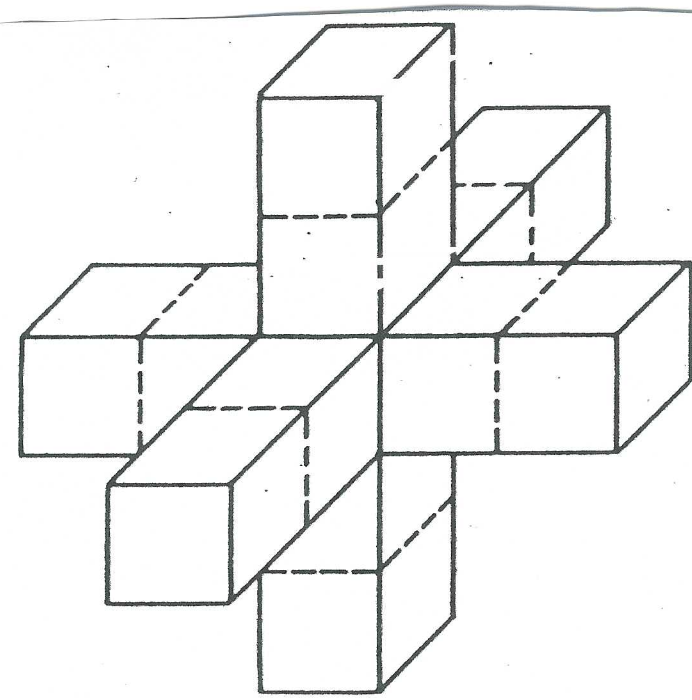
$k = 3$, $n = 2$

(k, n) - cross



$k = 3$, $n = 2$

n - dimension k - # cubes attached in each direction



(2,3)-cross

Minkowski's Conjecture

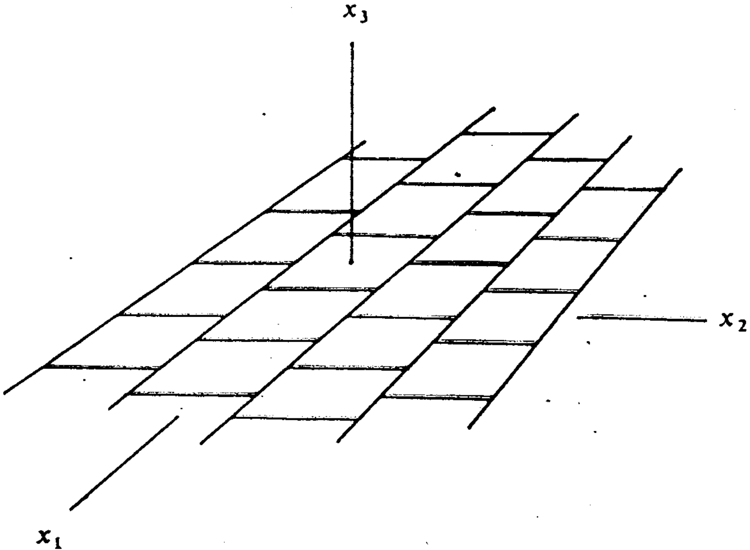
Conjecture (Minkowski 1896, 1907): In a lattice tiling of the n-space R^n by unit cubes some pair of cubes share a complete $(n-1)$–dimensional face.

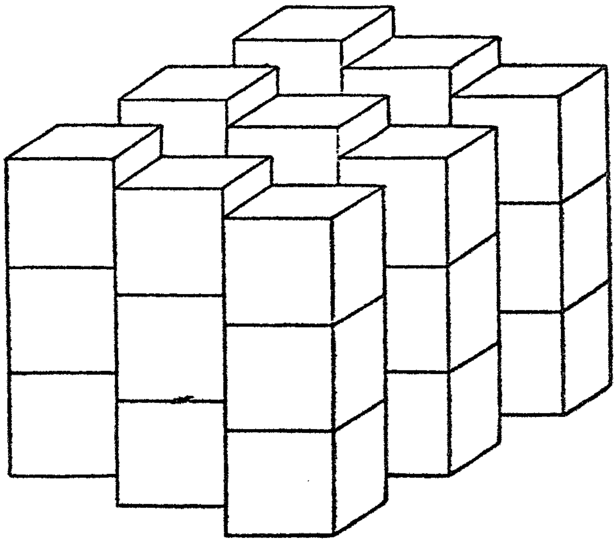
- motivated by diophantine approximation
- easy for small $n = 2, 3$
- gives insight into structure of lattice tilings (see diagram)
- solved by Hajos in 1941 by algebraic methods
- not correct for arbitrary tilings in high dimensions (Lagarias, Shor 1992)

Theorem (Hajos, 1941): Let G be a finite abelian group. If $a_1, a_2, \ldots, a_r$ are elements of G and $r_1, r_2, \ldots, r_n$ are positive integers such that each element of G is uniquley expressible in the form

$$a_1^{x_1} \cdots a_r^{x_r}, \qquad 0 \leq x_1 \leq r_1 - 1, \ldots, 0 \leq x_n \leq r_n - 1$$

then $a_i^{r_i} = e$ for some i.


x_3
x_2
x_1



Structure

Problem in *Geometry*

Solution via *Algebra*

Motivation from *Number Theory*

Applications in

Coding Theory

Graph Theory

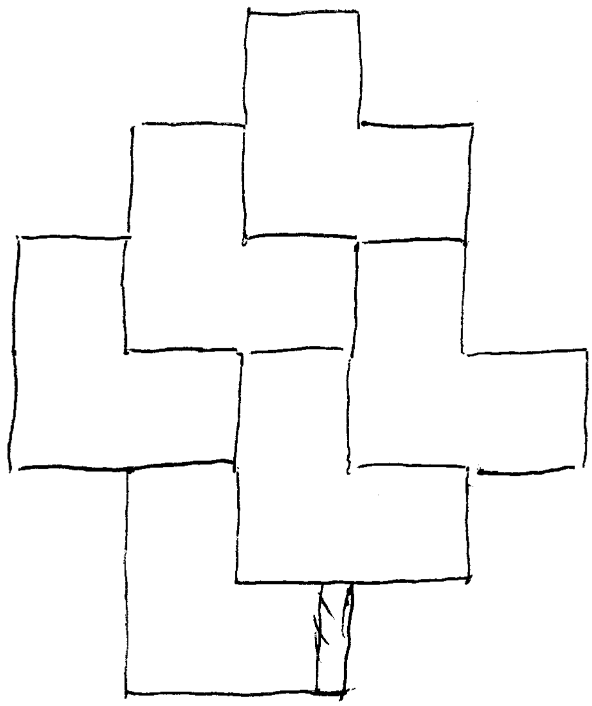
Cryptography

Links to *Linear Algebra*, etc.

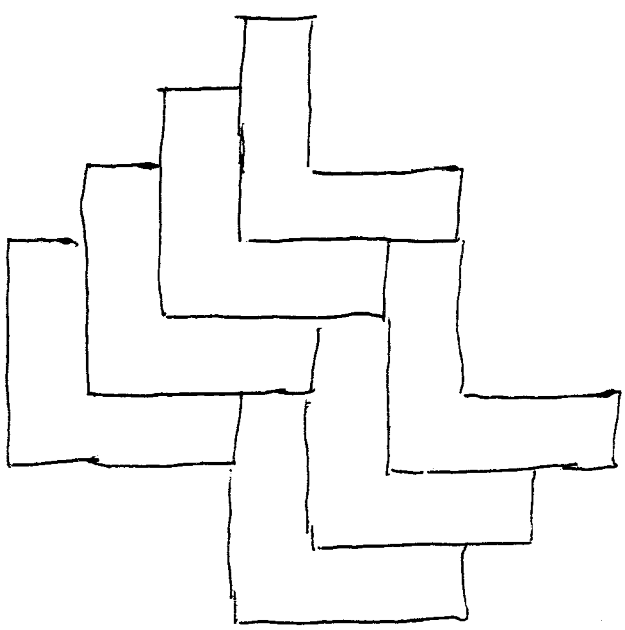
Lattice Tiling $\equiv$ Group Factorization

Tiling by semicross

$k=1$



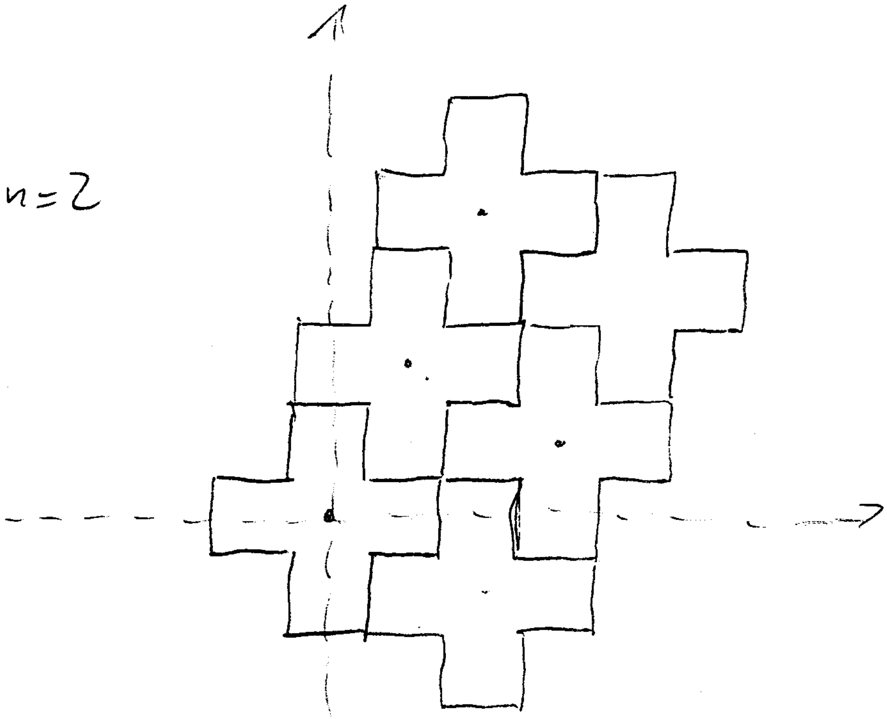
$k=2$



- possible for all k, $n=2$

Tiling by cross

$k = 1,\ n = 2$



centers in $(0,0)$, $(1,2)$, $(2,4)$, $(3,1)$, $(4,2)$ etc.

$$\{(i,j) : i + 2j \equiv 0 \mod 5\}$$

$k=1,\ n \geq 2$: centers in

$$\{(i_1, i_2, \ldots, i_n) : i_1 + 2i_2 + 3i_3 + \ldots + n \cdot i_n \equiv 0 \mod (2n+1)\}$$

$k=2,\ n=2$ not possible

Integer Codes

An integer code consists of all words $(c_1, \ldots, c_n) \in Z_m^n$ fulfilling

$$\sum_{i=1}^{n} w_i \cdot c_i = d \bmod m,$$

$(w_1, \ldots, w_n) \in Z_m^n$ fixed sequence of weights

d is an element of Z_m

n is the length of the code

m is the size of the code alphabet.

Applications

Coding Theory

Single–error correcting codes
in various settings: substitution, deletion, insertion, permutation, RLL, symmetric, asymmetric, erasure, etc. – appropriate choice of the weight sequence

Perfect codes

Computer Science

Packet loss in internet communication (Sloane 2002)

Deletions in genome sequences

Efficient placement of resources in distributed computations

Flash Memories

Graph Theory

Codes in graphs (Biggs 1973)
graphs often related to error–correcting codes

Domination

Cryptography

Cryptosystems via Factorization of groups

steganography

The syndrome

The effect of a single error is reflected in the behaviour of the syndrome, which should be changed to a value different from d

Example: substitution of the letter c_i by $c_i \pm j$

$$w_1c_1 + \ldots w_{i-1}c_{i-1} + w_i(c_i \pm j) + w_{i+1}c_{i+1} + \ldots w_nc_n$$
$$= d \pm w_i \cdot j,$$

Example: permutation of letters c_i and c_{i+1}

$$w_1c_1 + \ldots w_{i-1}c_{i-1} + w_ic_{i+1} + w_{i+1}c_i + w_{i+2}c_{i+2} + \ldots w_nc_n =$$
$$d + (w_i - w_{i+1})(c_{i+1} - c_i).$$

Example: peak shifts in RLL codes (Levenshtein, Vinck 1993)

$$w_1c_1 + \ldots + w_{i-1}c_{i-1} + w_i(c_i \pm j) + w_{i+1}(c_{i+1} \mp j)$$
$$+w_{i+2}c_{i+2} + \ldots + w_nc_n = d \pm (w_i - w_{i+1})j.$$

In order to be able to correct one single error, the syndromes of an integer code have to be pairwisely different. So if the possible distortions are from an error set $\mathcal{E}$ and the linear combinations of the weights are from a set $\mathcal{H}$, then we have to assure that

$$e \cdot h \neq e' \cdot h' \text{ for all } e, e' \in \mathcal{E} \text{ and } h, h' \in \mathcal{H}.$$

$\mathcal{H}$ syndrome code, shift code for $\mathcal{E} = \{1, \ldots, k\}$ (Levenshtein, Vinck 1993)

If all possible values occur as a syndrome, then the code is perfect.

$(\mathcal{E}, \mathcal{H})$ factorization of group Z_p^*

General Construction

Z_p – p prime number, $\qquad Z_p^* = (Z_p \setminus \{0\}, \cdot)$

g generator of Z_p^*, i.e.,
$Z_p^* = \{g^j : j = 0, \ldots, p-1\}$

$\mathcal{E} = \{a_0, a_1, \ldots, a_k\}$

Criterion (T. 2005): Let $a_i = g^{\mu_i}$ for $i = 0, \ldots, k-1$. A perfect integer code exists, if

$$\{\mu_0 \bmod k, \ldots, \mu_{k-1} \bmod k\} = \{0, \ldots, k-1\}.$$

Similar construction for $\mathcal{E} = \{\pm a_0, \pm a_1, \ldots, \pm a_k\}$
by replacing Z_p^* by $Z_p^*/\{1, -1\}$.

Examples $\mathcal{E} = \{\pm 1, \pm 3, \pm 5, \pm 7\}$:
$\mathcal{H} = \{1, 4, 6, 9, 16, 22, 24, 33, 35, 36, 43, 47\}$ in Z_{97}

5 is a generator of $Z_{97}/\{1, -1\}$

$5^0 = 1, \qquad 5^1 = 5, \qquad 5^{22} = 3, \qquad 5^{31} = 7.$

$0 \equiv 0 \bmod 4, \quad 1 \equiv 1 \bmod 4, \quad 22 \equiv 2 \bmod 4, \quad 31 \equiv 3 \bmod 4,$

Several Error Sets

1. The error set $\mathcal{E} = \{\pm 1, \pm a\}$ (Morita, Geyser, van Wijngaarden 2003):

The element a^2 has an even order modulo p

2. The error set $\mathcal{E} = \{\pm 1, \pm a, \pm b\}$ (T. 1997):

1 The orders of a and b are both divisible by 3.

2 Whenever $b^{l_1} = a^{l_2}$ for some integers l_1, l_2, then $l_1 + l_2 \equiv 0 \mod 3$.

$\mathcal{H} = \{a^i \cdot b^j, i - j \equiv 0 \mod 3\}$ is generated by the elements a^3, b^3 and $a \cdot b$.

3. The error set $\mathcal{E} = \{\pm 1, \pm a, \pm b, \pm c\}$ (T. 2005):

1 In $Z_p * / \{1, -1\}$ the orders of a and b are divisible by 4 and the order of c is divisible by 2,

2 whenever $a^i \cdot b^j \in \mathcal{G}$ then $i + j \equiv 0 \mod 4$,

3 whenever $a^i \cdot c^j \in \mathcal{G}$ then $2i + j \equiv 0 \mod 4$,

4 whenever $b^i \cdot c^j \in \mathcal{G}$ then $2i + j \equiv 0 \mod 4$.

$\mathcal{H}$ is generated by the elements $a^4, b^4, a \cdot b, c^2, c \cdot a^2$.

The error set $\{\pm 1, \pm 2, \ldots, \pm k\}$

by far most important case

- tilings of R^n by the cross (Stein 1967)
- group splitting
- peak shift correction in RLL codes (Levenshtein, Vinck 1993)
- codes in the Stein sphere (Golomb 1969), Lee metric as special case

Constructions from previous slide for small k

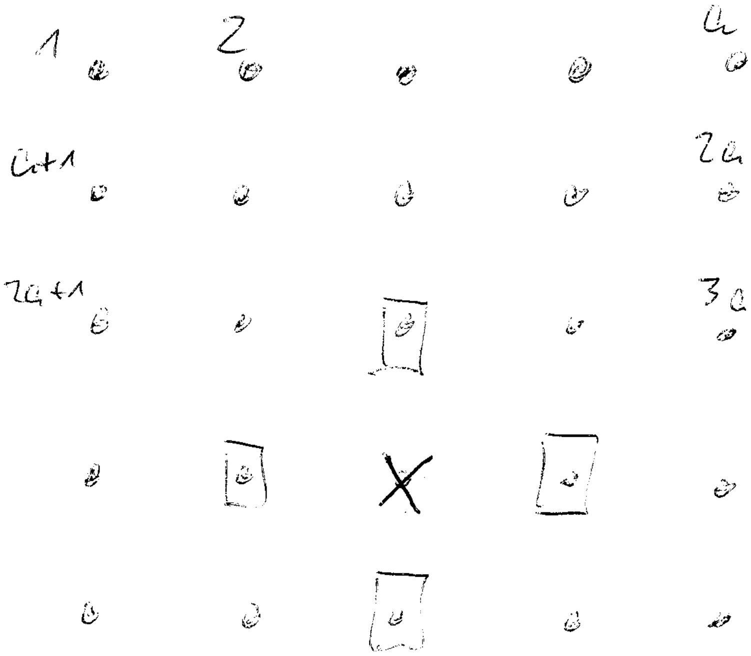
$\{\pm 1, \pm 2\}$, $\{\pm 1, \pm 2, \pm 3\}$,

$\{\pm 1, \pm 2, \pm 3, \pm 4\} = \{\pm 1, \pm 2, \pm 2^2, \pm 3\}$

$\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5\} = \{\pm 1, \pm 2, \pm 2^2, \pm 3, \pm 5\}$

Codes on Lattices

$a \times a$ grid



single error : $x \mapsto x \pm 1, \; x \pm a$

Cubes of Side length 2

Tiling of R^n obvious

Tiling of $(R \bmod l)^n$?

1) $l = 2m$ even: tiling exists

2) $l = 2m + 1$ odd: tiling does not exist

How good can a packing be?

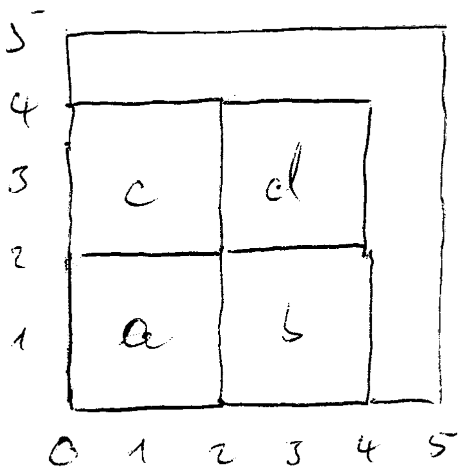
number of cubes in such a packing: $P(2m + 1, n)$

Obviously: $m^n \leq P(2m + 1, n) \leq (\frac{2m+1}{2})^n$

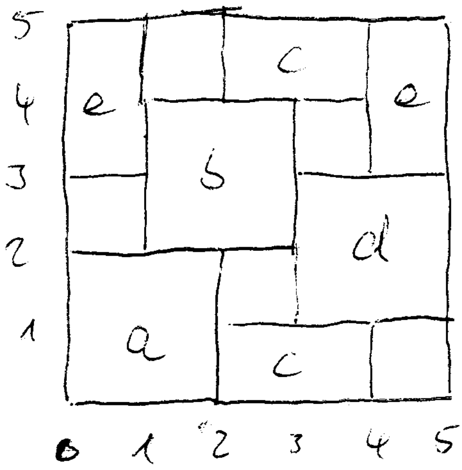
with: $\Theta(2m + 1) = \lim_{n\to\infty} P(m, n)^{1/n}$

$$m \leq \Theta(2m + 1) \leq m + \frac{1}{2}$$

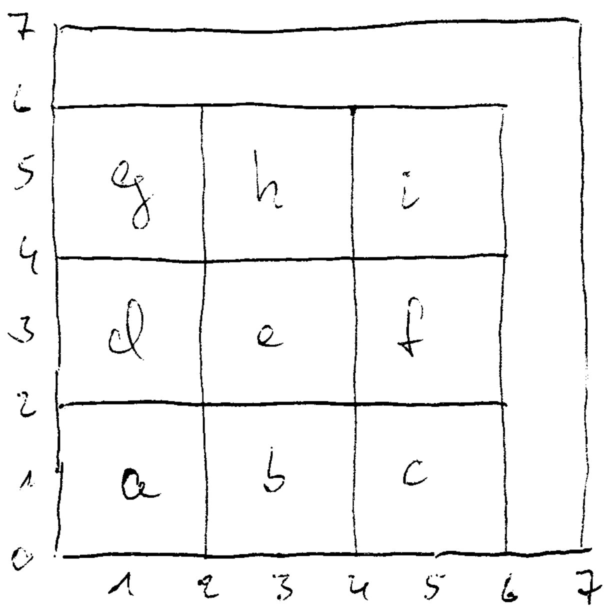
Problem equivalent to determination of the **Shannon Capacity** of C_{2m+1}.
(not so widely known)



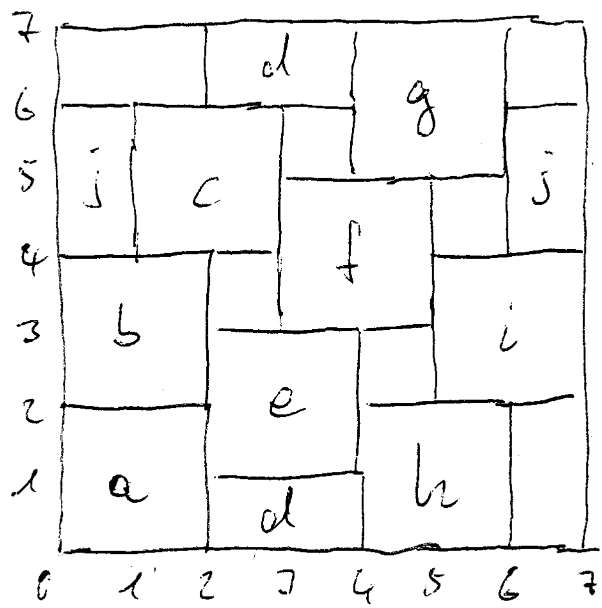
4 cubes



5 cubes



9 cubes



10 cubes

Shannon Capacity of Odd Cycles

Shannon, 1957:
Problem stated as "zero-error capacity" for graphs
C_5 smallest graph he could not solve

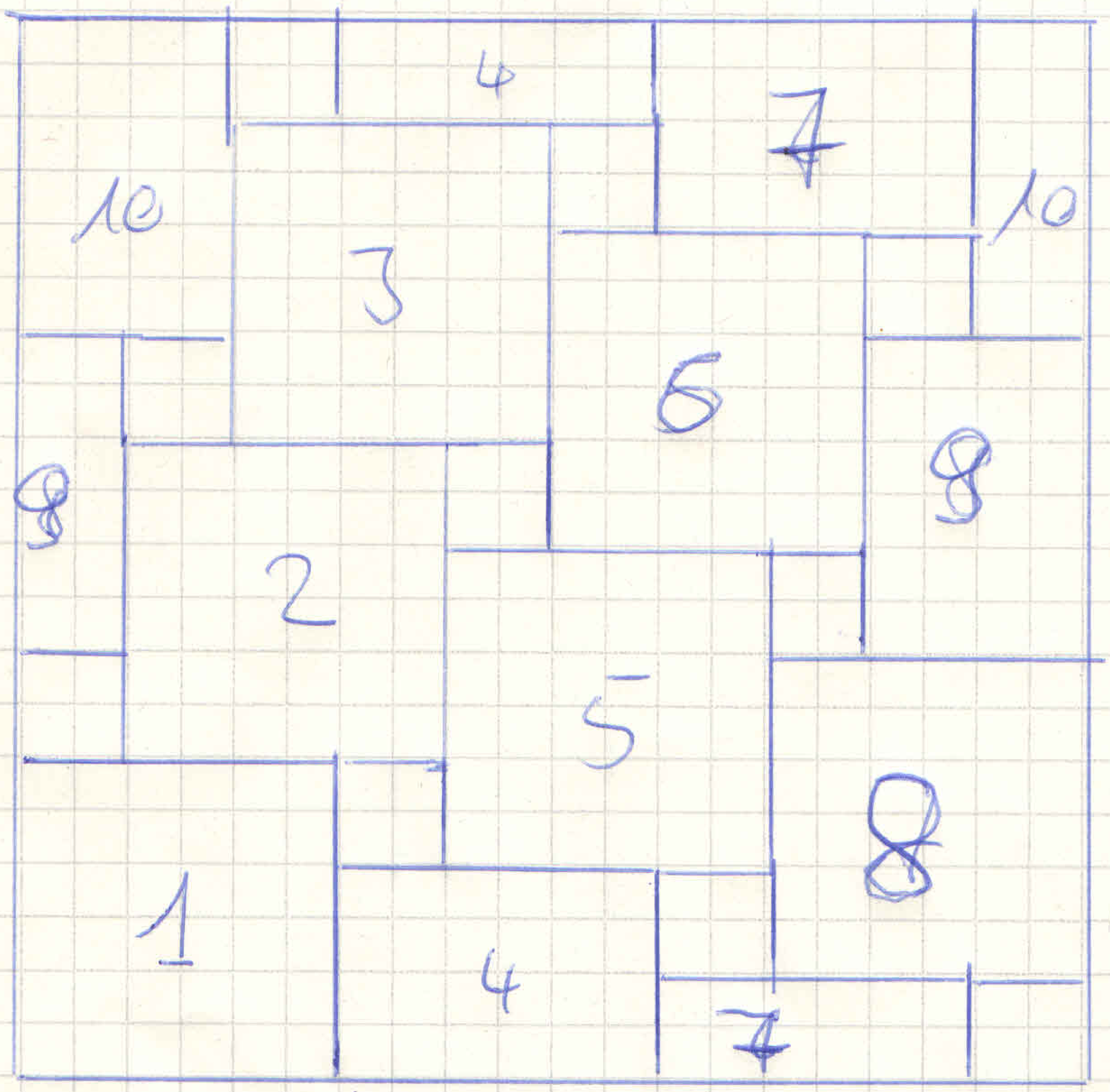
(...)

Lovasz, 1979:
$\Theta(5) = \sqrt{5}$
upper bound via Lovasz theta – function

$$\Theta(2m+1) \leq \theta(2m+1) = \frac{(2m+1)\cos(\pi/(2m+1))}{1+\cos(\pi/(2m+1))} = n + \frac{1}{2} - O(1/n)$$

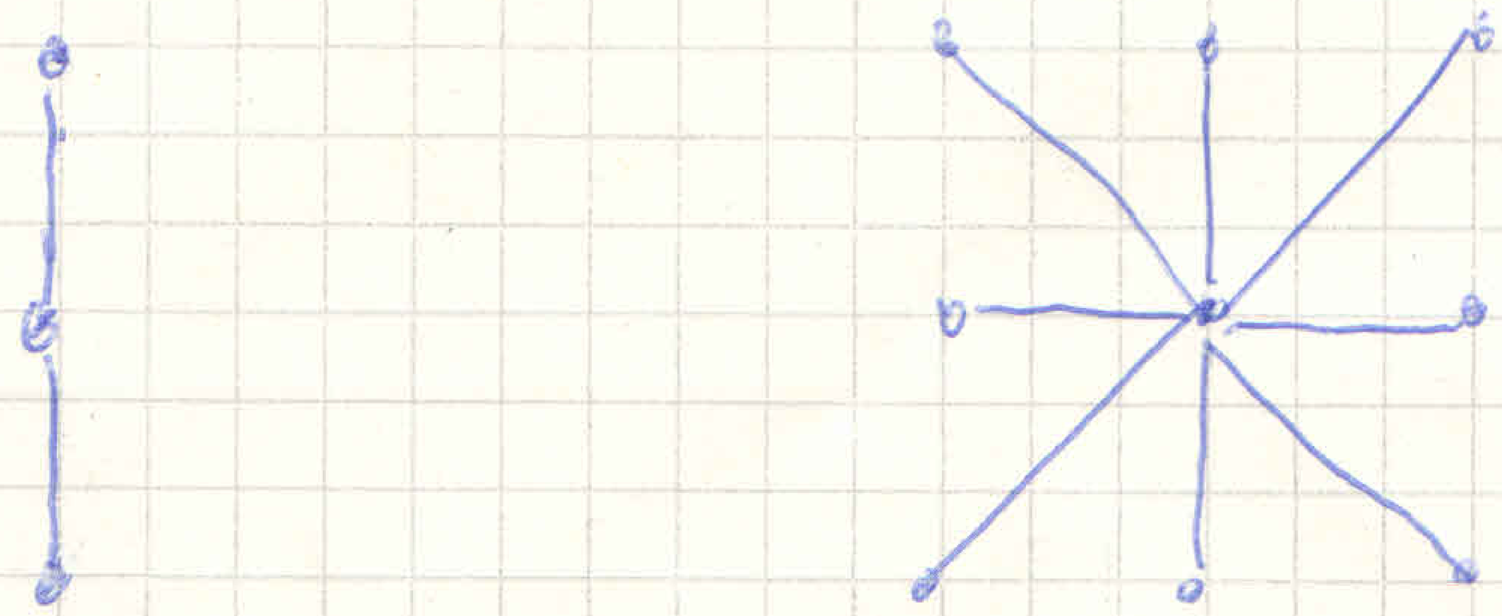
- Bohman, 2003+2005: $\lim_{m\to\infty}(m + \frac{1}{2} - \Theta(2m+1)) = 0$
- for large m asymptotic is $\Theta(2m+1] \approx m + \frac{1}{2}$
- for small m very difficult, especially $\Theta(7) =?$
- (...): Baumert et al. 1971, (Hales 1973), Stein 1977, etc. use approach via cubes, improve some lower bounds
- very fundamental for Graph Theory: strong perfect graph conjecture (Berge)

10 3×3 rectangles in a 10×10 rectangle

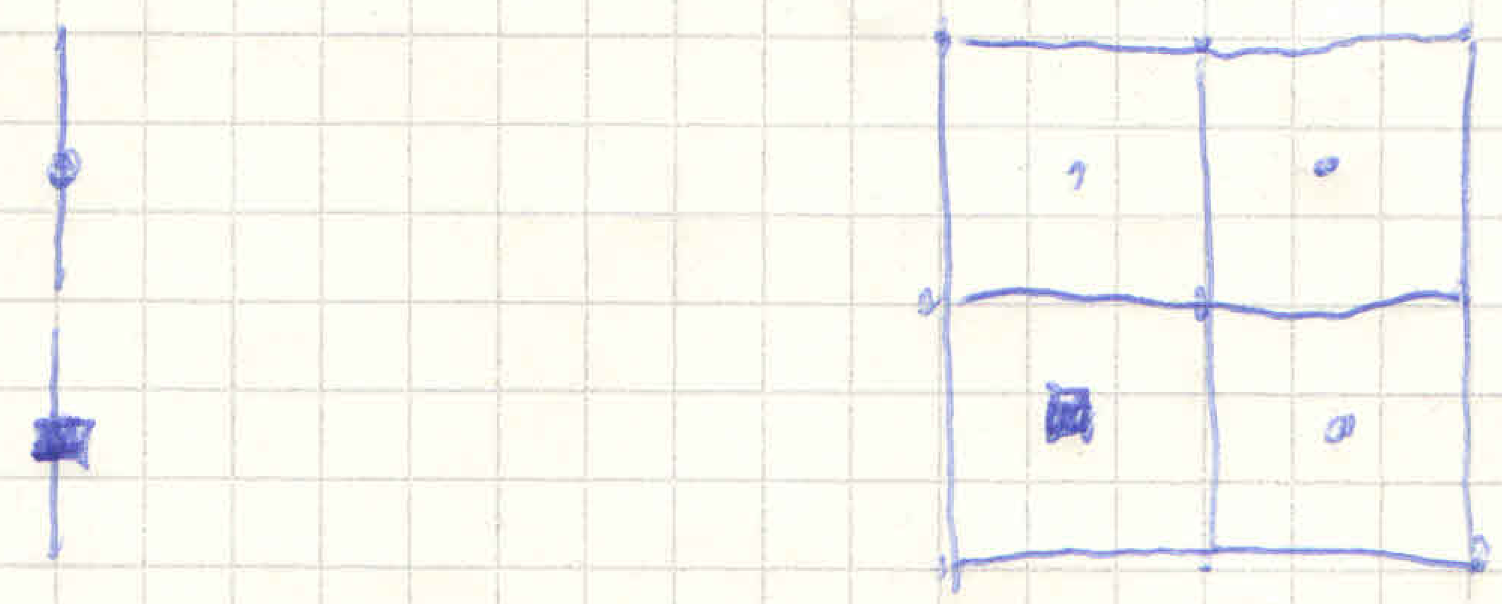


- generalizable to
k^2+1 $k\times k$ rectangles in a $(k^2+1)\times(k^2+1)$ rectangle
- lower left corners in points (i,j) with
$$i+k\cdot j \equiv 0 \mod (k^2+1)$$

equivalence 2×2

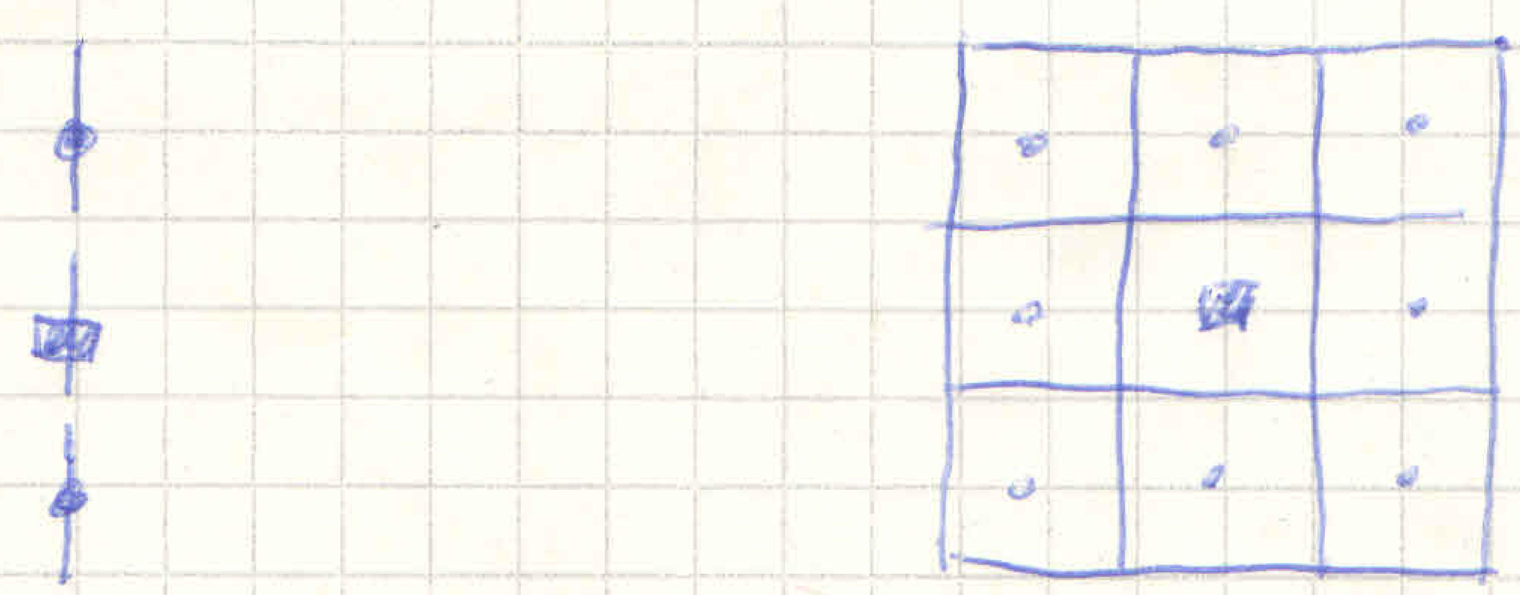


graph
strong product



code
(asymmetric)

equivalence 3×3 ?



code
(symmetric)

graph ?
(maybe undirected)

3×3 Shannon Sphere

Interpretation as symmetric single–error correcting code

(generalizing question by Morita et al.)

Problem: Graph theoretic equivalent?

(for 2×2 Shannon sphere this is the neighborhood of a cycle)

improvements of trivial construction possible

Upper bounds?

(might yield new insights into zero-error capacity)