Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 313–318*

Lattice Packings by Clusters of Cubes in Coding Theory

Ulrich Tamm tamm@ieee.org
University of Applied Sciences, Bielefeld, Germany

Abstract. Packings of the integer lattice Z^n by the cross or the semicross are intimately related to integer codes. Less known is that packings by $2 \times 2 \times \cdots \times 2$ cubes correspond to zero–error codes in the sense of Shannon and Lovász. We shall discuss single-error correcting codes building a bridge between these two seemingly unrelated code concepts.

1 Introduction

Clusters of unit cubes are often called polyominoes generalizing the notion domino for the most simple one - the cluster of two adjacent 2-dimensional cubes. Tiling and packing of mostly finite structures like boxes are discussed, for instance, in [7]. More interesting for coding theory are packings of tori or lattices.

Lattice packings, tilings, and coverings of the n–dimensional space R^n by clusters of units cubes are often a useful tool in coding theory and also related areas like memories [2]. The clusters correspond to the error spheres around a codeword, which is represented by a unit cube with the corresponding coordinates in its center (or in one of the corners). When the code is over a finite ring Z_q^n the coordinates are finally reduced modulo q, of course.

Golomb [6] systematically analyzed the error spheres arising from several metrics. The Hamming sphere consists of a whole dimension, hence of infinitely many cubes and the Lee sphere has a very complicated structure. However, for Lee distance 1 the Lee sphere coincides with the Stein sphere, in which the possible distortions are of limited size in each direction of just one coordinate. This error sphere and also the Stein corner (corresponding to "asymmetric" errors in one coordinate) are very suitable for an analysis via lattice packings. The tilings of R^n by the corresponding Lee sphere led Golomb and Welch [8] to the complete characterization of perfect Lee codes of distance 1. Further results on packings by the more general Stein sphere will briefly be discussed in Section 2.

Golomb [6] points out that the Hamming sphere corresponds to the L_0–metric and the Lee sphere to the L_1–metric. The error spheres corresponding to the L_∞–metric he denotes as the Shannon spheres, "since they generalize a coding problem considered by Shannon". This is the famous zero-error capacity problem for odd cycles [15], which can equivalently be formulated as the problem of packing an $a \times a \times \cdots \times a$–torus by $2 \times 2 \times \cdots \times 2$–cubes in n dimensions. Of course, the problem is only interesting for odd a, since for even a, trivially, a tiling exists. We shall discuss packings by the Shannon sphere in Section 3.

2 Stein Sphere and Stein Corner

The Stein sphere or (k, n) - cross arises when at one central unit cube a file of k unit cubes is attached in each direction of the n dimensions. For the Stein corner or (k, n)–semicross the files of k unit cubes are only attached to one direction of each dimension. Thus, the Stein corner and the Stein sphere are the error sphere for asymmetric and symmetric errors, respectively, arising from distortions of a single of the n components by at most k.

Lattice packings and tilings of the n-space are inimately related with checksums of the form

$$\sum_{i=1}^{n} w_i \cdot c_i = 0 \bmod m,$$

where $(w_1, \ldots, w_n) \in Z$ is a fixed sequence of weights and n is the length of the code. Vinck and Morita [23] denoted as integer codes the set of words $(c_1, \ldots, c_n)$ fulfilling such an equation.

Most notably is the choice $(w_1, \ldots, w_n) = (1, 2, \ldots, n)$. Choosing as modulus $m = 2n + 1$ for these weights the code words fulfilling the checksum placed as the centers of the crosses yield a tiling of the R^n by $(1, n)$–crosses.

Further, Varshamov and Tenengolts [22] and Levenshtein [11], used these weights for binary codewords and $m = n + 1$ in order to correct single asymmetric errors and deletions, respectively.

Tilings and packings by the (k, n)-semicross and the (k, n)–cross for $k \geq 1$ had been mostly studied by Stein and his coauthors, cf. [17, 18]. Basically, the analysis for these error spheres is possible since the geometric packing and tiling problems (actually, tilings are easier to analyze) can equivalently be formulated algebraically as problems concerning group factorizations. The existence conditions for perfect codes (corresponding to tilings by the error spheres), however, then are usually not efficiently verifiable. Via checking number theoretic conditions in [19] the cases $k = 3, 4$ could algorithmically be handled. The most efficient conditions for general error spheres we found in [20], where also a survey of several applications in graph theory, cryptology, computer science, etc. was provided.

Theorem 1. *Let $\mathcal{E} = \{1, a_1, \ldots, a_{k-1}\}$ be the error sphere of an integer code, let g be a generator of Z_p^* and let $a_i = g^{\nu_i}$ in Z_p^* for $i = 1, \ldots, k - 1$. Then a perfect integer code with error sphere $\mathcal{E}$ exists in Z_p, exactly if for some divisor* *l of* $\frac{p-1}{k}$ *the powers* ν_i *are such that* $\nu_i = l\mu_i$ *for* $i = 0, \ldots, k-1$*, where the* μ_i*'s fall into the different congruence classes modulo k, i. e.,*

$$\{\mu_1 \ mod \ k, \ldots, \mu_{k-1} \ mod \ k\} = \{1, \ldots, k-1\}.$$

3 The Shannon Sphere

The error sphere $\{1, a\}$ as in the above theorem was studied by Morita et al. [14] with an application in the construction of single-error correcting codes on the $a \times a$–grid, where the errors are imposed by the $(1,2)$-cross or $(1,2)$–semicross. In this context they asked what would happen if also the direct diagonal neighbours would be included into the error spheres.

The answer is, that in this case the $(1,2)$–semicross would be extended to a 2×2 – cube and the $(1,2)$-cross would be extended to a 3×3 – cube. A single-error correcting code then would correspond to a packing of the $a \times a$ – torus by 2×2 – cubes for asymmetric errors (the semicross) and by 3×3 – cubes for symmetric errors (the cross). The generalization to higher dimensions is obvious.

Such problems had been studied before in a different context, namely, in the analysis of Shannon's zero–error capacity of odd cycles of length a. This geometric approach was used in several papers ([1, 9, 16]) before Lovász [12] determined the zero-error capacity of the C_5 via algebraic graph theory.

The connection to error spheres is implicit already in [6] as pointed out in the introduction although there a bijection to the construction of zero–error codes is not given. Actually, the example provided, namely the $3 \times 3 \times 3$ cube is even a little misleading.

For instance, in two dimensions, the corners of the unit cubes forming the 2×2 cube are the vertices in the graph – here corresponding to the strong product of a path of length 2 – with the central node of the path representing a vertex on the odd cycle and the final nodes of the path representing the neighbours with which the vertex can be confused. A 3×3–cube, however, would correspond to a strong product of a path of length 3 which consists of 4 vertices. From such a path the confusability condition for the zero-error problem is not so easily constructed, simply, since there is no central node in the path.

Due to its importance for the zero–error capacity in literature mostly packings of tori by $2 \times 2 \times \cdots \times 2$–cubes have been considered. In [5] coverings of tori by $k \times k$– cubes for $k > 2$ are constructed. It is pointed out that in Hales' PhD thesis [9] also such packings are considered, however, in the resulting paper [10] they are seemingly not included. So, we provide a simple algebraic construction for two dimensions.

Theorem 2. *An optimal packing of a* $(k^2+1) \times (k^2+1)$ *– torus by* $k \times k$ *– cubes is obtained as follows: Place the lower left corners of the cubes in the* *positions* (i, j) *with* $i + kj \equiv 0$ *mod* $k^2 + 1$.

Proof. This construction is obtained by greedily placing the lower left corners in the positions $(i, ki \bmod k^2+1)$ for $i = 0, \ldots, k^2$. It obviously yields a packing with just one unit cube in each row and each column not covered by any $k \times k$–cube, namely, in the positions $(i, k(i+1) \bmod k^2+1)$. On the other hand, no row and no column can completely be covered by the $k \times k$–cubes, because k does not divide $k^2 + 1$. $\square$

For $k = 2$ this just yields the packing given by Shannon [15] whose direct product was finally shown to achieve the capacity by Lovász [12]. It would be interesting to check $k = 3$, which yields a code for correcting single symmetric errors with distortion at most 1 in two components, for optimality in higher dimensions when simply the direct product of the above 2-dimensional construction is applied. However, Lovász' bound is not directly applicable, since the incidence structure of the above-mentioned bijection does not correspond to an undirected graph.

Further constructions for packings by 2×2–cubes from [1] can be generalized to $k \times k$–cubes, for instance, the optimal packing for the 9×9 torus in [1] can easily be extended to $k > 2$.

4 Concluding Remarks

The extension of the spheres of certain single error–correcting codes to the diagonals of the central cube has been analyzed motivated by [14] and [21]. Actually, the aproach is implicit already in Golomb's paper [6] who denoted the arising error sphere as Shannon sphere and related the corresponding single–error correcting codes to Shannon's famous zero-error capacity. However, a closer look at the underlying bijection shows that the zero-error capacity of odd cycles would correspond to a tiling of an $a \times a \times \cdots \times a$–torus by $2 \times 2 \times \cdots \times 2$–boxes, which are the error spheres of a single asymmetric error correcting code.

This problem has been studied in the 1970's but seems not to have been continued intensively after Lovász determined the zero-error capacity of the C_5 with different methods (actually, it was even not easy to trace the references). There has been recent interest, since Bohman [3] used a construction from [1]. Further, a related packing problem by not connected cubes comes into play for the zero-error capacity of triangular graphs [13].

For single symmetric error correcting codes the error sphere corresponds to a $3 \times 3 \times \cdots \times 3$–box. However, the resulting confusability graph is not undirected such that it does not immediately relate to Shannon's original problem.

References

[1] L. Baumert, R.J. McEliece, E. Rodemich, H.C. Rumsey jr., R. Stanley and H. Taylor, A combinatorial packing problem, *Proceedings SIAM-AMS Sympos. Appl. Math., New York, 1970, Computers in Algebra and Number Theory, G. Birkhoff and M. Hall jr. (eds.)*, AMS, 1971, 97-108.

[2] E.E. Belitskaja, V.R. Sidorenko, and P. Stenström, Testing of memory with defects of fixed configurations, *Proceedings of 2nd International Workshop on Algebraic and Combinatorial Coding Theory*, Leningrad, 1990, 24 – 28.

[3] T. Bohmann, A limit theorem for the Shannon capacities of odd cycles II, *Proceedings of the AMS*, **133**, 2005, 537-543.

[4] R.J. McEliece and E.C. Posner, Hide and seek, data storage and entropy, *Ann. Math. Statistics*, **42**, 1971, 1706–1716.

[5] R.J. McEliece and H. Taylor, Covering tori with squares, *J. Combin. Theory A*, **14** (1), 1973, 119–124.

[6] S.W. Golomb, A general formulation of error metrics, *IEEE Trans. Inform. Theory*, **15**, 1969, 425 – 42.

[7] S.W. Golomb, *Polyominoes*, Princeton University Press, 2nd ed., 1994.

[8] S.W. Golomb and L.R. Welch, Algebraic coding for the Lee metric, *Error Correcting Codes (H. B. Mann ed.)*, 1968, 175 – 194.

[9] R.S. Hales, *Numerical invariants and gamma products of graphs*, PhD. dissertation, Harvard, 1970.

[10] R.S. Hales, Numerical invariants and the strong product of graphs, *J. Combin. Theory B*, **15**, 1973, 146-155.

[11] V. I. Levenshtein, Binary codes with correction for deletions and insertions of the symbol 1, *Problemy Peredachi Informacii*, **1**, 1965, 12 – 25.

[12] L. Lovász, On the Shannon capacity of a graph, *IEEE Trans. Inform. Theory*, **25**, 1979, 1–7.

[13] K.A. Mathew, P.R.J. Östergard and A. Popa, On the Shannon capacity of triangular graphs, *Electronic J. Combin*, **20** (2), 2013, # P27.

[14] H. Morita, A. Geyser, and A. J. van Wijngaarden, On integer codes capable of correcting single errors in two – dimensional lattices, *Proceedings 2003 IEEE Int. Symp. Inform. Theory*, 2003, p. 16.

[15] C.E. Shannon, The zero-error capacity of a graph, *IRE Trans. Inform. Theory*, **IT-2**, 1956, 8–19.

[16] S. Stein, Modified linear dependence and the capacity of a cyclic graph, *Linear Algebra Appl.*, **17** (3), 1977, 191–195.

[17] S. Stein, Packing of R^n by certain error spheres, *IEEE Trans. Inform. Theory*, **30** (2), 1984, 356 – 363.

[18] S. Stein and S. Szabó, *Algebra and Tiling*, The Carus Mathematical Monographs 25, The Mathematical Association of America, 1994.

[19] U. Tamm, Splittings of cyclic groups and perfect shift codes, *IEEE Trans. Inform. Theory*, **61** (5), 1998, 2003 – 2009.

[20] U. Tamm, Reflections about a single checksum, *International Workshop on the Arithmetic of Finite Fields (WAIFI 2010)*, Springer Lecture Notes in Computer Science LNCS 6087, 2010, 238–249.

[21] U.Tamm, Some reflections about integer codes, *Proceedings 3rd International Workshop on Advances in Communications, Boppard, Germany, on the occasion of the 65th birthday of Professor Han Vinck*, 2014.

[22] R. R. Varshamov and G. M. Tenengolts, One asymmetric error correcting codes, *Avtomatika i Telemechanika*, **26** (2), 1965, 288 – 292.

[23] A.J.H. Vinck and H. Morita, Codes over the ring of integers modulo m, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E81–A** (10), 1998, 2013 – 2018.