Lattices from Codes

Construction of D_n from codes. The lattice D_n is by definition

$$D_n = \{(x_1, \ldots, x_n),\ \sum_{i=1}^{n} x_i \text{ is even}\}.$$

It is sometimes called the checkerboard lattice (drawing it in two dimensions explains why).

(a) Recall the definition of the binary single parity check code and write its systematic generator matrix.

(b) Construct a generator matrix for the lattice $\Lambda_C = \rho^{-1}(C)$ via Construction A.

(c) Show this is a generator matrix of D_n.

Construction of E_8 from codes. A Gram matrix for E_8 is

$$\begin{bmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 2 \end{bmatrix}.$$

The goal of this exercise is to build the lattice E_8 using a (scaled) Construction A. For this exercise, while it is possible to do these computations by hand, using SAGE (or any other suitable software) helps with repeated computations.

(a) Recall a parity check matrix H of the binary Hamming code (denoted by $\mathcal{H}_3$) of length 7.

(b) List the codewords of $\mathcal{H}_3$ and compute their weight.

(c) Extend $\mathcal{H}_3$ into $\tilde{\mathcal{H}_3} = \{(\mathbf{x}, x_8),\ \mathbf{x} \in \mathcal{H}_3,\ \sum_{i=1}^{8} x_i = 0\}$. Show that we have now 14 codewords of weight 4, 7 with $x_8 = 0$ and 7 with $x_8 = 1$. Compute the minimum Hamming distance of $\tilde{\mathcal{H}_3}$.

(d) Compute the minimum norm of $\Lambda_C = \rho^{-1}(C)$ and the number of vectors with this norm in Λ_C.

(e) Show that $w_H(\mathbf{x} + \mathbf{y}) = w_H(\mathbf{x}) + w_H(\mathbf{y}) - 2\langle \mathbf{x}, \mathbf{y} \rangle$ for $\mathbf{x}, \mathbf{y}$ binary vectors.

(f) Set

$$\mathbf{f}_i = \frac{1}{\sqrt{2}}\mathbf{u}_i,\ i = 1\ldots,7$$

where $\mathbf{u}_i,\ i = 1\ldots,7$ are the 7 vectors of $\tilde{\mathcal{H}}_3$ of weight 4, with $x_8 = 1$. Compute $\langle \mathbf{f}_j, \mathbf{f}_i \rangle$.

(g) Set

$$\begin{aligned} \mathbf{b}_1 &= \mathbf{f}_1 \\ \mathbf{b}_2 &= \mathbf{f}_2 - \mathbf{f}_1 \\ &\vdots \\ \mathbf{b}_7 &= \mathbf{f}_7 - \mathbf{f}_6. \end{aligned}$$

Compute $\langle \mathbf{b}_j, \mathbf{b}_i \rangle$ and compare with the Gram matrix of E_8. Find the missing vector $\mathbf{b}_8$.

Finding constructions of lattices from codes is still fairly open. For example, `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/` lists interesting lattices, and and how they can be constructed can be reported.