Lattices and Quadratic Forms (Summer 2024) - Solutions to Problem Set 8

1. Let $C \leq \mathbb{F}_2^n$ be of length n and dimension k and consider the associated code lattice $A_1^n \leq \Gamma_C \leq (A_1^\sharp)^n$. Our first goal is to show that $\Gamma_{C^\perp}$ is a sublattice of $\Gamma_C^\sharp$. So let x be an arbitrary element of $\Gamma_{C^\perp}$ and y be an arbitrary element of Γ_C. Then we have (identifying A_1^n with $\sqrt{2}\mathbb{Z}^n$)

$$x = \sqrt{2}\left(z + \frac{b}{2}\right) \quad \text{and} \quad y = \sqrt{2}\left(z' + \frac{c}{2}\right),$$

where $z, z' \in \mathbb{Z}^n$ and $b, c \in \{0,1\}^n$ reducing modulo 2 to a codeword in $C^\perp$ and C, respectively. Then we have

$$x \cdot y = 2z \cdot z' + z \cdot c + z' \cdot b + \frac{1}{2} b \cdot c.$$

The first three terms are trivially integers. For the last term, we note that $b \cdot c \equiv 0 \pmod 2$ because the corresponding codewords are orthogonal in $\mathbb{F}_2^n$. So we have $x \cdot y \in \mathbb{Z}$ and because the vectors here are arbitrary $\Gamma_{C^\perp} \leq \Gamma_C^\sharp$.

To prove the equality, we will show that the discriminants of $\Gamma_{C^\perp}$ and $\Gamma_C^\sharp$ are equal (recall that if $L' \leq L$ then $\det(L') = |L/L'|^2 \det(L)$). Since A_1^n is a sublattice of Γ_C, we have $\det(A_1^n) = |\Gamma_C/A_1^n|^2 \det(\Gamma_C)$. Noting that $\det(A_1^n) = 2^n$ and $|\Gamma_C/A_1^n| = |C| = 2^k$, we find

$$\det(\Gamma_C) = 2^{n-2k}.$$

Since the dual code $C^\perp$ has dimension $n-k$, the same computation shows that

$$\det(\Gamma_{C^\perp}) = 2^{n-2(n-k)} = 2^{2k-n}.$$

We also have

$$\det(\Gamma_C^\sharp) = \frac{1}{\det(\Gamma_C)} = 2^{2k-n}.$$

So we indeed have $\det(\Gamma_{C^\perp}) = \det(\Gamma_C^\sharp)$ and hence the two lattices are equal to each other: $\Gamma_{C^\perp} = \Gamma_C^\sharp$.

2. Let C be a binary $[n,k,d]$ code with

$$n = 2^r - 1, \quad k = 2^r - 1 - r, \quad \text{and} \quad d = 3$$

and let $P \in \mathbb{F}_2^{(n-k)\times n}$ be a parity check matrix for C. Recall that codewords of C correspond to linear dependencies between the columns of P. Since $d = 3$, we have a minimum of three columns from P to form a linear dependency. In particular, the columns of P should all be nonzero (otherwise we would have $d = 1$) and furthermore any two of these nonzero columns $v_i, v_j \in \mathbb{F}_2^{n-k}$ with $i \neq j$ should not be linearly dependent (otherwise we would have $d = 2$) and hence we have $v_i \neq v_j$. Now note that $\mathbb{F}_2^{n-k} = \mathbb{F}_2^r$ has $2^r - 1$ pairwise different nonzero vectors. Since $n = 2^r - 1$, the columns of P exactly consist of these $2^r - 1$ nonzero vectors in $\mathbb{F}_2^r$. This is nothing but the parity check matrix for the Hamming code $H(\mathbb{F}_2, r)$. Note that the ordering of the columns of P was left ambiguous in our definition of $H(\mathbb{F}_2, r)$ as well, since any such ordering choice produces equivalent codes (permuting the underlying bits).

3. Let $C \leq \mathbb{F}_q^n$ be a linear code of dimension k with generator matrix $G = [I_k|Q]$ where $Q \in \mathbb{F}_q^{k\times(n-k)}$.
   - Let us first assume that C is a self-dual code ($C = C^\perp$). Then the dimension k of C and $n-k$ of $C^\perp$ are equal to each other and hence Q is a square matrix. Moreover, the columns of G^T (forming a basis for C) are orthogonal to each other by this assumption and hence $GG^T = 0 \in \mathbb{F}_q^{k\times k}$. Inserting $G = [I_k|Q]$ into this equation yields $I_k + QQ^T = 0$ as we wanted to show.
   - Conversely, let us first assume that the matrix $Q \in \mathbb{F}_q^{k\times(n-k)}$ defining the generator matrix G in the standard form as above satisfy $QQ^T = -I_k$. This is then equivalent to $GG^T = 0 \in \mathbb{F}_q^{k\times k}$, i.e. the

columns $v_1, \ldots, v_k$ of G^T, which form a basis for C, satisfy $v_i \cdot v_j = 0$ for all i, j. Consequently, if $\alpha = a_1 v_1 + \ldots + a_k v_k$ and $\beta = b_1 v_1 + \ldots + b_k v_k$ are any two arbitrary codewords in C, then we have

$$\alpha \cdot \beta = \sum_{i,j} a_i b_j v_i \cdot v_j = 0$$

So the condition $QQ^T = -I_k$ implies that C is self-orthogonal ($C \leq C^\perp$).
If we further have that Q is a square matrix, then $k = n - k$ and hence C and $C^\perp$ have equal dimensions. The inclusion relation $C \leq C^\perp$ then requires that these vector spaces should in fact be equal $C = C^\perp$, i.e. C is self-dual.

4. Let $C \leq \mathbb{F}_2^n$ be a binary linear code that is self-orthogonal (i.e. $C \leq C^\perp$). In particular, self-orthogonality requires that any codeword $c \in C$ satisfies $c \cdot c = 0$ (where for $x, y \in \mathbb{F}_2^n$, $x \cdot y$ is the non-degenerate symmetric bilinear form $x_1 y_1 + \ldots + x_n y_n \in \mathbb{F}_2$). For binary codes, the weight $w(c)$ is equal to $c \cdot c$ modulo 2, and hence for self-orthogonal binary linear codes we have $2 \mid w(c)$ for any $c \in C$.
Now let us further assume that C has a generator matrix G where the columns $v_1, \ldots, v_k \in \mathbb{F}_2^n$ of G^T (which form a basis for C) all have weights divisible by 4. Then any given codeword $c \in C$ can be uniquely written as

$$c = \alpha_1 v_1 + \ldots + \alpha_k v_k \quad \text{ where } \alpha_1, \ldots, \alpha_k \in \mathbb{F}_2.$$

Now let us determine vectors $\widetilde{c}, \widetilde{v}_1, \ldots, \widetilde{v}_k$ in $\{0,1\}^n \subset \mathbb{Z}^n$ and $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_k \in \{0,1\} \subset \mathbb{Z}$ that are equal to $c, v_1, \ldots, v_k$ and $\alpha_1, \ldots, \alpha_k$ modulo 2. Then we have

$$\widetilde{c} \equiv \widetilde{\alpha}_1 \widetilde{v}_1 + \ldots + \widetilde{\alpha}_k \widetilde{v}_k \pmod 2.$$

Since a number modulo 2 determines its square modulo 4, we have

$$\widetilde{c}^2 \equiv (\widetilde{\alpha}_1 \widetilde{v}_1 + \ldots + \widetilde{\alpha}_k \widetilde{v}_k)^2 \pmod 4$$

with squares denoting the usual Euclidean norm in $\mathbb{Z}^n$. Since $w(c) \equiv \widetilde{c}^2 \pmod 4$, we will focus on the right hand side

$$(\widetilde{\alpha}_1 \widetilde{v}_1 + \ldots + \widetilde{\alpha}_k \widetilde{v}_k)^2 = \widetilde{\alpha}_1^2 \widetilde{v}_1^2 + \ldots + \widetilde{\alpha}_k^2 \widetilde{v}_k^2 + 2 \sum_{i<j} \widetilde{\alpha}_i \widetilde{\alpha}_j \widetilde{v}_i \cdot \widetilde{v}_j.$$

Now note that $\widetilde{v}_j^2 \equiv 0 \pmod 4$ for all j because we are assuming v_j's have weights divisible by 4. Moreover, we have $2 \mid \widetilde{v}_i \cdot \widetilde{v}_j$ for all i, j because C is self-orthogonal and hence we have $v_i \cdot v_j = 0$ in $\mathbb{F}_2$. Therefore, every term on the right hand side of our expression above for $(\widetilde{\alpha}_1 \widetilde{v}_1 + \ldots + \widetilde{\alpha}_k \widetilde{v}_k)^2$ is divisible by four and therefore

$$(\widetilde{\alpha}_1 \widetilde{v}_1 + \ldots + \widetilde{\alpha}_k \widetilde{v}_k)^2 \equiv 0 \pmod 4.$$

So $4 \mid w(c)$ for any codeword $c \in C$ and C is doubly-even.