Problem Set 10 Solutions

Problem 10.1 (Mod-2 lattices and trellis codes)

(a) Let $\mathcal{C}$ be an (n,k,d) binary linear block code. Show that

$$\Lambda_{\mathcal{C}} = \{\mathbf{x} \in \mathbb{Z}^n \mid \mathbf{x} \equiv \mathbf{c} \ mod\ 2 \ for\ some\ \mathbf{c} \in \mathcal{C}\}$$

is an n-dimensional sublattice of $\mathbb{Z}^n$ (called a "Construction A" or "mod-2" lattice).

$\Lambda_{\mathcal{C}}$ is evidently a subset of $\mathbb{Z}^n$. To show that it is a sublattice, we must prove that it has the group property. Suppose that $\mathbf{x}$ and $\mathbf{x}'$ are two elements of $\Lambda_{\mathcal{C}}$ that are congruent to codewords $\mathbf{c} \in \mathcal{C}$ and $\mathbf{c}' \in \mathcal{C}$, respectively. Then it is easy to see that $\mathbf{x}+\mathbf{x}'$ is congruent (mod 2) to $\mathbf{c}+\mathbf{c}'$, which must also be a codeword of $\mathcal{C}$ by the group property of a linear code $\mathcal{C}$. Finally, $\Lambda_{\mathcal{C}}$ is n-dimensional because it includes $2\mathbb{Z}^n = \{\mathbf{x} \in \mathbb{Z}^n \mid \mathbf{x} \equiv \mathbf{0} \bmod 2\}$, which is n-dimensional.

(b) Show that if $\mathcal{C}$ has N_d weight-d words, then the mod-2 lattice $\Lambda_{\mathcal{C}}$ has the following geometrical parameters:

$$\begin{aligned} d^2_{\min}(\Lambda_{\mathcal{C}}) &= \min\{d, 4\}; \\ K_{\min}(\Lambda_{\mathcal{C}}) &= \begin{cases} 2^d N_d, & \text{if } d < 4; \\ 2n, & \text{if } d > 4; \\ 2^d N_d + 2n, & \text{if } d = 4; \end{cases} \\ V(\Lambda_{\mathcal{C}}) &= 2^{n-k}; \\ \gamma_{\mathrm{c}}(\Lambda_{\mathcal{C}}) &= \frac{d^2_{\min}(\Lambda_{\mathcal{C}})}{2^{\eta(\mathcal{C})}}, \end{aligned}$$

where $\eta(\mathcal{C}) = 2(n-k)/n$ is the redundancy of $\mathcal{C}$ in bits per two dimensions.

By definition, $\Lambda_{\mathcal{C}}$ is the union of the 2^k cosets $\{2\mathbb{Z}^n + \mathbf{c} \mid \mathbf{c} \in \mathcal{C}\}$ of its sublattice $2\mathbb{Z}^n$.

Within any coset $2\mathbb{Z}^n + \mathbf{c}$, as within $2\mathbb{Z}^4$, the minimum squared distance is 4, and every element $\boldsymbol{\lambda}$ has $2n$ nearest neighbors at this distance of the type $\boldsymbol{\lambda} \pm (2, 0, 0, \ldots, 0)$.

The minimum squared distance between cosets is the minimum distance d of $\mathcal{C}$, because two elements of $2\mathbb{Z}^n + \mathbf{c}$ and $2\mathbb{Z}^n + \mathbf{c}'$ must differ by at least ± 1 wherever $\mathbf{c}$ and $\mathbf{c}'$ differ. For every codeword $\mathbf{c} \in \mathcal{C}$ of weight d, there are 2^d nearest neighbors of this type.

We conclude that if $d < 4$, then $d^2_{\min}(\Lambda_{\mathcal{C}}) = d$ and $K_{\min}(\Lambda_{\mathcal{C}}) = 2^d N_d$; if $d > 4$, then $d^2_{\min}(\Lambda_{\mathcal{C}}) = 4$ and $K_{\min}(\Lambda_{\mathcal{C}}) = 2n$; and if $d = 4$, then $d^2_{\min}(\Lambda_{\mathcal{C}}) = 4$ and $K_{\min}(\Lambda_{\mathcal{C}}) = 2^d N_d + 2n$.

Because $\Lambda_{\mathcal{C}}$ is the union of the 2^k cosets of $2\mathbb{Z}^n$, it is 2^k times as dense as $2\mathbb{Z}^n$. Since the volume of $2\mathbb{Z}^n$ per lattice point is $V(2\mathbb{Z}^n) = 2^n$, this implies that $V(\Lambda_{\mathcal{C}}) = 2^{n-k}$.

Defining $\eta(\mathcal{C}) = 2(n-k)/n$, the nominal coding gain of $\Lambda_{\mathcal{C}}$ is then

$$\gamma_{\mathrm{c}}(\Lambda_{\mathcal{C}}) = \frac{d^2_{\min}(\Lambda_{\mathcal{C}})}{V(\Lambda_{\mathcal{C}})^{2/n}} = \frac{d^2_{\min}(\Lambda_{\mathcal{C}})}{2^{2(n-k)/n}} = \frac{d^2_{\min}(\Lambda_{\mathcal{C}})}{2^{\eta(\mathcal{C})}}.$$

(c) Show that the mod-2 lattices corresponding to the $(4,3,2)$ *and* $(4,1,4)$ *binary linear block codes have coding gain* $2^{1/2}$ *(1.51 dB) (these lattices are in fact versions of* D_4*). Show that the mod-2 lattice corresponding to the* $(8,4,4)$ *binary linear block code has coding gain* 2 *(3.01 dB) (this lattice is in fact a version of* E_8*). Show that no mod-2 lattice has a nominal coding gain more than* 4 *(6.02 dB).*

From the above expressions, we have $d^2_{\min}(\Lambda_{(4,3,2)}) = 2$ and $\eta(4,3,2) = \frac{1}{2}$, so $\gamma_c(\Lambda_{(4,3,2)}) = 2 \cdot 2^{-1/2} = 2^{1/2}$. Also, we have $d^2_{\min}(\Lambda_{(4,1,4)}) = 4$ and $\eta(4,1,4) = \frac{3}{2}$, so $\gamma_c(\Lambda_{(4,1,4)}) = 4 \cdot 2^{-3/2} = 2^{1/2}$. (Note also that $K_{\min}(\Lambda_{(4,3,2)}) = 4{\cdot}6 = 24$ and $K_{\min}(\Lambda_{(4,1,4)}) = 16{\cdot}1{+}8 = 24$.)

Finally, we have $d^2_{\min}(\Lambda_{(8,4,4)}) = 4$ and $\eta(8,4,4) = 1$, so $\gamma_c(\Lambda_{(8,4,4)}) = 4 \cdot 2^{-1} = 2$. (Note also that $K_{\min}(\Lambda_{(8,4,4)}) = 16 \cdot 14 + 16 = 240$.)

Every mod-2 lattice has $d^2_{\min}(\Lambda_{\mathcal{C}}) \le 4$ and $\eta(\mathcal{C}) \ge 0$, so $\gamma_c(\Lambda_{\mathcal{C}}) = d^2_{\min}(\Lambda_{\mathcal{C}})2^{-\eta(\mathcal{C})} \le 4$.

(d) Let $\mathcal{C}$ *be a rate-*k/n *binary linear convolutional code with free distance* d *and* N_d *minimum-weight code sequences per* n *dimensions. Define the corresponding mod-2 trellis code* $\Lambda_{\mathcal{C}}$ *to be the set of all integer sequences* $\mathbf{x}$ *with* D*-transform* $x(D)$ *such that* $x(D) \equiv c(D)$ *mod 2 for some code sequence* $c(D) \in \mathcal{C}$*.*

(i) Show that an encoder as in Figure 5 of Chapter 14 based on the convolutional code $\mathcal{C}$ *and the lattice partition* $\mathbb{Z}^n/2\mathbb{Z}^n$ *is an encoder for this mod-2 trellis code.*

The rate-k/n convolutional encoder puts out a sequence of binary n-tuples $\mathbf{c}_k$. Let each binary n-tuple $\mathbf{c}_k$ select a coset $2\mathbb{Z}^n + \mathbf{c}_k$ of $2\mathbb{Z}^n$ in $\mathbb{Z}^n$. Thus the n-tuple sequence $\{\dots, \mathbf{c}_k, \mathbf{c}_{k+1}, \dots\}$ selects the coset sequence $\{\dots, 2\mathbb{Z}^n + \mathbf{c}_k, 2\mathbb{Z}^n + \mathbf{c}_{k+1}, \dots\}$, which is precisely the set of all integer sequences that are congruent mod 2 to $\{\dots, \mathbf{c}_k, \mathbf{c}_{k+1}, \dots\}$.

(ii) Show that $\Lambda_{\mathcal{C}}$ *has the group property.*

Suppose that $x(D)$ and $x'(D)$ are two elements of $\Lambda_{\mathcal{C}}$ that are congruent to codewords $c(D) \in \mathcal{C}$ and $c'(D) \in \mathcal{C}$, respectively. Then it is easy to see that $x(D)+x'(D)$ is congruent (mod 2) to $c(D) + c'(D)$, which must also be a codeword of $\mathcal{C}$ by the group property of a linear code $\mathcal{C}$.

(iii) Show that $\Lambda_{\mathcal{C}}$ *has the following parameters:*

$$\begin{aligned} d^2_{\min}(\Lambda_{\mathcal{C}}) &= \min\{d, 4\}; \\ K_{\min}(\Lambda_{\mathcal{C}}) &= \begin{cases} 2^d N_d, & \text{if } d < 4; \\ 2n, & \text{if } d > 4; \\ 2^d N_d + 2n, & \text{if } d = 4; \end{cases} \\ \gamma_c(\Lambda_{\mathcal{C}}) &= d^2_{\min}(\Lambda_{\mathcal{C}})2^{-\eta(\mathcal{C})}, \end{aligned}$$

where $\eta(\mathcal{C}) = 2(n-k)/n$ *is the redundancy of* $\mathcal{C}$ *in bits per two dimensions.*

The proof is precisely as for part (b), above, except that by using the expression (14.18) for $\gamma_c(\Lambda_{\mathcal{C}})$, we avoid having to define the volume of a trellis code.

Problem 10.2 (Invariance of nominal coding gain)

Show that $\gamma_c(\Lambda)$ is invariant to scaling, orthogonal transformations, and Cartesian products; i.e., $\gamma_c(\alpha U \Lambda^m) = \gamma_c(\Lambda)$, where $\alpha > 0$ is any scale factor, U is any orthogonal matrix, and $m \geq 1$ is any positive integer. Show that $\gamma_c(\alpha U \mathbb{Z}^n) = 1$ for any version $\alpha U \mathbb{Z}^n$ of any integer lattice $\mathbb{Z}^n$.

The minimum squared distance of a scaled n-dimensional lattice $\alpha\Lambda$ is $d^2_{\min}(\alpha\Lambda) = \alpha^2 d^2_{\min}(\Lambda)$, and its volume is $V(\alpha\Lambda) = \alpha^n V(\Lambda)$, so $\gamma_c(\Lambda)$ is invariant to scaling:

$$\gamma_c(\alpha\Lambda) = \frac{d^2_{\min}(\alpha\Lambda)}{V(\alpha\Lambda)^{2/n}} = \frac{\alpha^2 d^2_{\min}(\Lambda)}{\alpha^2 V(\Lambda)^{2/n}} = \gamma_c(\Lambda).$$

An orthogonal transformation preserves distances and volumes, so $\gamma_c(\Lambda)$ is invariant under orthogonal transformations.

The minimum squared distance of a Cartesian-product lattice Λ^m is the same as that of Λ, because two elements of Λ^m may differ in any one of its m components by any element of Λ. The dimension of Λ^m is mn. The volume of Λ^m is $V(\Lambda^m) = (V(\Lambda))^m$, because its generator matrix consists of m diagonal copies of G. Thus $\gamma_c(\Lambda)$ is invariant under Cartesian products:

$$\gamma_c(\Lambda^m) = \frac{d^2_{\min}(\Lambda^m)}{V(\Lambda^m)^{2/mn}} = \frac{d^2_{\min}(\Lambda)}{V(\Lambda)^{2/n}} = \gamma_c(\Lambda).$$

Since $\gamma_c(\mathbb{Z}) = 1$, we have $\gamma_c(\alpha U \mathbb{Z}^m) = 1$ for any version $\alpha U \mathbb{Z}^m$ of any integer lattice $\mathbb{Z}^m$.

Problem 10.3 (Invariance of normalized second moment)

Show that $G(\mathcal{R})$ is invariant to scaling, orthogonal transformations, and Cartesian products; i.e., $G(\alpha U \mathcal{R}^m) = G(\mathcal{R})$, where $\alpha > 0$ is any scale factor, U is any orthogonal matrix, and $m \geq 1$ is any positive integer. Show that $G(\alpha U[-1,1)^n) = 1/12$ for any version $\alpha U[-1,1)^n$ of any n-cube $[-1,1)^n$ centered at the origin.

A scaled n-dimensional region $\alpha\mathcal{R}$ has average energy $P(\alpha\mathcal{R}) = \alpha^2 P(\mathcal{R})$ and volume $V(\alpha\mathcal{R}) = \alpha^n V(\Lambda)$, so $G(\mathcal{R})$ is invariant to scaling:

$$G(\alpha\mathcal{R}) = \frac{P(\alpha\mathcal{R})}{V(\alpha\mathcal{R})^{2/n}} = \frac{\alpha^2 P(\mathcal{R})}{\alpha^2 V(\mathcal{R})^{2/n}} = G(\mathcal{R}).$$

An orthogonal transformation preserves energy and volume, so $G(\Lambda)$ is invariant under orthogonal transformations.

The average energy per dimension of a Cartesian-product region $\mathcal{R}^m$ is the same as that of $\mathcal{R}$, because average energy scales with dimension. The dimension of $\mathcal{R}^m$ is mn. The volume of $\mathcal{R}^m$ is $V(\mathcal{R}^m) = (V(\mathcal{R}))^m$. Thus $G(\mathcal{R})$ is invariant under Cartesian products:

$$G(\mathcal{R}^m) = \frac{P(\mathcal{R}^m)}{V(\mathcal{R}^m)^{2/mn}} = \frac{P(\mathcal{R})}{V(\mathcal{R})^{2/n}} = G(\mathcal{R}).$$

Since $P([-1,1)) = 1/3$, $V([-1,1)) = 2$, we have $G([-1,1)) = 1/12$. Thus $G(\alpha U[-1,1)^m) = 1/12$ for any version $\alpha U[-1,1)^m$ of any m-cube $[-1,1)^m$ centered at the origin.