Lemma 2 Let \((\gamma, C)\) be an arbitrary coordinate coding on \(\mathbb{R}^{d_B}\). Given an \((L_h, L_G)\)-Lipschitz smooth generator \(G_u(h)\) and an \(L_\infty\)-Lipschitz discriminator \(D_v\), for all \(h \in \mathbb{R}^{d_B}\):

\[
\left| D_v(G_u(h)) - D_v\left(\sum_v \gamma_v(h) G_u(v)\right) \right| \leq L_x L_h \|h - r(h)\|_2 + L_x L_G \sum_{v \in C} |\gamma_v(h)| \|v - r(h)\|_2^2.
\]

Proof Given an \((L_h, L_G)\)-Lipschitz smooth generator \(G_u(h)\), an \(L_\infty\)-Lipschitz discriminator \(D_v\), and let \(\gamma_v = \gamma_v(h)\) and \(h' = r(h) = \sum_{v \in C} \gamma_v(v)\). We have

\[
\left| \tilde{D}_v(G_u(h)) - \tilde{D}_v\left(\sum_v \gamma_v(h) G_u(v)\right) \right| = \left| D_v(G_u(h)) - D_v\left(\sum_v \gamma_v(h) G_u(v)\right) \right|
\]

\[
= \left| D_v(G_u(h)) - D_v(G_u(h')) - \left(D_v\left(\sum_v \gamma_v(h) G_u(v)\right) - D_v(G_u(h'))\right) \right|
\]

\[
\leq \left| D_v(G_u(h)) - D_v(G_u(h'))\right| + \left| D_v\left(\sum_v \gamma_v(h) G_u(v)\right) - D_v(G_u(h'))\right|
\]

\[
\leq L_x \|G_u(h) - G_u(h')\|_2 + L_x \left| \sum_v \gamma_v(h) G_u(v) - G_u(h') \right|_2
\]

\[
\leq L_x \|G_u(h) - G_u(h')\|_2 + L_x \left| \sum_v \gamma_v(h) \left(G_u(v) - G_u(h') - \Delta G_u(h')^T(v - h')\right) \right|_2
\]

\[
\leq L_x \|G_u(h) - G_u(h')\|_2 + L_x \sum_{v \in C} |\gamma_v| \|G_u(v) - G_u(h') - \Delta G_u(h')^T(v - h')\|_2
\]

\[
\leq L_x \sum_{v \in C} |\gamma_v| \|v - h'\|_2^2 + L_x L_G \sum_{v \in C} |\gamma_v| \|v - r(h)\|_2^2
\]

\[
= L_x L_h \|h - h'\|_2 + L_x L_G \sum_{v \in C} |\gamma_v| \|v - r(h)\|_2^2,
\]

where \(\tilde{D}_v(\cdot) = 1 - D_v(\cdot)\). In the above derivation, the first inequality holds by the triangle inequality. The second inequality uses an assumption that \(D_v\) is Lipschitz smooth w.r.t. the input. The third inequality uses the facts that \(\sum_{v \in C} \gamma_v(x) = 1\) and \(h' = \sum_{v \in C} \gamma_v v\). The last inequality uses the \((L_h, L_G)\)-Lipschitz smooth generator \(G_u\), that is

\[
\|G_u(v) - G_u(h') - \Delta G_u(h')^T(v - h')\|_2 \leq L_G \|v - h'\|_2^2.
\]
8. Proof of Lemma 1

**Lemma 1 (Generator Approximation)** Let $(\gamma, C)$ be an arbitrary coordinate coding on $\mathbb{R}^{dB}$. Given a Lipschitz smooth generator $G_u(h)$, for all $h \in \mathbb{R}^{dB}$:

$$\left\| G_u \left( \sum_{v \in C} \gamma_v(h)v \right) - \sum_{v \in C} \gamma_v(h)G_u(v) \right\|_2 \leq 2L_h \| h - r(h) \|_2 + L_G \sum_{v \in C} |\gamma_v(h)||v - r(h)\|_2^2.$$  

**Proof** From Lemma 2, when the discriminator is identity function: $D_v(t) = t$, that is

$$\left| D_v(G_u(h)) - D_v \left( \sum_{v \in C} \gamma_v(h)G_u(v) \right) \right| = \left\| G_u(h) - \sum_{v} \gamma_v(h)G_u(v) \right\|_2 \leq L_h \| h - r(h) \|_2 + L_G \sum_{v \in C} |\gamma_v(h)||v - r(h)\|_2^2,$$

then, we have

$$\left\| G_u \left( \sum_{v \in C} \gamma_v(h)v \right) - \sum_{v \in C} \gamma_v(h)G_u(v) \right\|_2 = \left\| G_u \left( \sum_{v \in C} \gamma_v(h)v \right) - G_u(h) + G_u(h) - \sum_{v \in C} \gamma_v(h)G_u(v) \right\|_2 \leq \left\| G_u \left( \sum_{v \in C} \gamma_v(h)v \right) - G_u(h) \right\|_2 + \left\| G_u(h) - \sum_{v \in C} \gamma_v(h)G_u(v) \right\|_2 \leq 2L_h \| h - r(h) \|_2 + L_G \sum_{v \in C} |\gamma_v(h)||v - r(h)\|_2^2,$$

where $r(h) = \sum_{v \in C} \gamma_v(h)v$. $\square$

9. Proof of Theorem 1

In order to provide a generalization bound w.r.t. the neural net distance, we first give some relevant lemmas and theorems. When the latent points lie on a latent manifold and the generator is Lipschitz smooth, $Q_{L_h, L_G}(\gamma, C)$ has a bound as follows.

**Lemma 3 (Manifold Coding (Yu et al., 2009))** If the latent points lie on a compact smooth manifold $\mathcal{M}$, given an $(L_h, L_G)$-Lipschitz smooth generator $G_u(h)$ and any $\epsilon > 0$, there exist anchor points $C \subset \mathcal{M}$ and coding $\gamma$ such that

$$Q_{L_h, L_G}(\gamma, C) \leq \left[ L_h c_{\mathcal{M}} + \left( 1 + \sqrt{d_{\mathcal{M}}} + 4 \sqrt{d_{\mathcal{M}}} \right) L_G \right] \epsilon^2.$$  

Lemma 3 shows that the complexity of local coordinate coding depends on the intrinsic dimension of the manifold instead of the dimension of the basis.

**Theorem 1** Suppose measuring function $\phi(\cdot)$ is Lipschitz smooth: $|\phi'(\cdot)| \leq L_\phi$, and bounded in $[-\Delta, \Delta]$. Consider coordinate coding $(\gamma, C)$, an example set $\mathcal{H}$ in latent space and the empirical distribution $\mathcal{D}_{\text{real}}$. If the generator is Lipschitz smooth, then the expected generalization error satisfies the inequality:

$$\mathbb{E}_{\mathcal{H}} \left[ d_{F, \phi} \left( \mathcal{D}_{G_{\hat{\phi}}(\gamma(h)), \hat{D}_{\text{real}}} \right) \right] \leq \inf_{\hat{\phi}} \mathbb{E}_{\mathcal{H}} \left[ d_{F, \phi} \left( \mathcal{D}_{G_{\gamma(h)}, \hat{D}_{\text{real}}} \right) \right] + \epsilon(d_{\mathcal{M}}),$$

where $\epsilon(d_{\mathcal{M}}) = L_\phi Q_{L_h, L_G}(\gamma, C) + 2 \Delta$, and generative quality $Q_{L_h, L_G}(\gamma, C)$ has an upper bound w.r.t. $d_{\mathcal{M}}$ in Lemma 3 of supplementary material.

**Proof** Let $\mathcal{H}^{(k)} = \left\{ h_1^{(k)}, h_2^{(k)}, \ldots, h_r^{(k)} \right\}$ be a set of $r$ latent samples which lie on the latent distribution. Consider $n + 1$ independent experiments over the latent distribution, we have $\mathcal{H}_{r,n+1} = \left\{ \mathcal{H}^{(1)}, \mathcal{H}^{(2)}, \ldots, \mathcal{H}^{(n+1)} \right\}$. Recall the optimization problem, we consider an empirical version of the expected loss:

$$[\hat{w}] = \arg \min_{w} \left[ \frac{1}{n} \sum_{i=1}^{n+1} d_{F, \phi} \left( \mathcal{D}_{G_{w, \gamma(h^{(i)})}, \hat{D}_{\text{real}}} \right) \right].$$  

(5)
Let $k$ be an integer randomly drawn from $\{1, 2, \ldots, n + 1\}$. Let $[\hat{w}^{(k)}]$ be the solution of

$$
[\hat{w}^{(k)}] = \arg \min_{[w]} \left[ \frac{1}{n} \sum_{i=1}^{n+1} d_{F, \phi} \left( D_{G_{w, \gamma(h)}^{(i)}(\hat{\gamma}(\gamma(h))), \hat{D}_{real} \right) \right],
$$

with the $k$-th example left-out.

Recall the definition of the neural net distance, we have

$$
d_{F, \phi}(\mu, \nu) = \sup_{\mathcal{F}} \left| \mathbb{E}_{x \sim \mu} [\phi(D_{\nu}(x))] + \mathbb{E}_{x \sim \nu} [\phi(D_{\nu}(x))] \right|,
$$

where $\mathcal{F} = \{D_{\nu}, \nu \in \mathcal{V}\}$. Given the $k$-th sample experiment, the same real distribution $\hat{D}_{real}$ over the training samples $x_1, x_2, \ldots, x_m$, and two different distributions generated by $G_{\tilde{\gamma}(h)}(\hat{\gamma}(h))$ and $G_{\tilde{\gamma}(h)}(\gamma(h))$, respectively, the difference value of the neural net distance between these two generated distributions is:

$$
d_{F, \phi} \left( \hat{D}_{G_{\tilde{\gamma}(h)}(\hat{\gamma}(h)), \hat{D}_{real}}, \tilde{D}_{G_{\tilde{\gamma}(h)}(\gamma(h)), \hat{D}_{real}} \right) - d_{F, \phi} \left( \hat{D}_{G_{\tilde{\gamma}(h)}(\hat{\gamma}(h)), \hat{D}_{real}}, \tilde{D}_{G_{\tilde{\gamma}(h)}(\gamma(h)), \hat{D}_{real}} \right)
\leq \sup_{h \in H(k)} \left[ \phi \left( \tilde{D}_{\nu}(G_{\tilde{\gamma}(h)}(\hat{\gamma}(h))) \right) \right] - \mathbb{E}_{x \sim H(k)} \left[ \phi \left( \tilde{D}_{\nu}(G_{\tilde{\gamma}(h)}(\gamma(h))) \right) \right]
\leq \sum_{h \in H(k)} \left[ \phi \left( \tilde{D}_{\nu}(G_{\tilde{\gamma}(h)}(\hat{\gamma}(h))) \right) \right] - \phi \left( \tilde{D}_{\nu}(G_{\tilde{\gamma}(h)}(\gamma(h))) \right) \leq 2\Delta,
$$

where $\tilde{D}_{\nu}(\cdot) = 1 - D_{\nu}(\cdot)$. In the above derivation, the first equality uses the definition of the neural net distance. The last inequality holds by the assumption that $\phi(\cdot)$ is $L_\phi$-Lipschitz and bounded in $[-\Delta, \Delta]$. By summing over $k$, and consider any fixed $G_{\nu} \in \mathcal{G}$, we obtain:

$$
\sum_{k=1}^{n+1} d_{F, \phi} \left( \hat{D}_{G_{\tilde{\gamma}(h)}(\hat{\gamma}(h)), \hat{D}_{real}}, \tilde{D}_{G_{\tilde{\gamma}(h)}(\gamma(h)), \hat{D}_{real}} \right) \leq \sum_{k=1}^{n+1} d_{F, \phi} \left( \hat{D}_{G_{\tilde{\gamma}(h)}(\hat{\gamma}(h)), \hat{D}_{real}}, \tilde{D}_{G_{\tilde{\gamma}(h)}(\gamma(h)), \hat{D}_{real}} \right) + 2(n+1)\Delta
\leq \sum_{h \in H(k), k=1}^{n+1} d_{F, \phi} \left( \hat{D}_{G_{\tilde{\gamma}(h)}(\hat{\gamma}(h)), \hat{D}_{real}}, \tilde{D}_{G_{\tilde{\gamma}(h)}(\gamma(h)), \hat{D}_{real}} \right) + 2(n+1)\Delta
\leq \sum_{h \in H(k), k=1}^{n+1} \sum_{k=1}^{n+1} \sum_{\nu \in \mathcal{V}} L_\phi Q_{\mathcal{L}_{h}, \mathcal{L}_{G}(\gamma, \nu)}(\gamma, \nu) + 2(n+1)\Delta,
$$

where $Q_{\mathcal{L}_{h}, \mathcal{L}_{G}(\gamma, \nu)}(\gamma, \nu) = \mathbb{E}_{h} [L_h \| h - r(h) \|_2^2 + L_G \sum_{\nu \in \mathcal{C}} |\gamma| \| v - r(h) \|_2^2]$. In the above derivation, the second inequality holds since $\tilde{w}$ is the minimizer of Problem (5). The third inequality follows from the concavity of $\phi(\cdot)$ and Lemma 1:

$$
d_{F, \phi} \left( \hat{D}_{G_{\tilde{\gamma}(h)}(\hat{\gamma}(h)), \hat{D}_{real}}, \tilde{D}_{G_{\tilde{\gamma}(h)}(\gamma(h)), \hat{D}_{real}} \right) = \sup_{\mathcal{F} \in \hat{D}_{real}} \left[ \mathbb{E}_{x \sim \mu} [\phi(D_{\nu}(x))] + \mathbb{E}_{x \sim \nu} [\phi(D_{\nu}(x))] \right]
\leq \sup_{\mathcal{F} \in \hat{D}_{real}} \left[ \mathbb{E}_{x \sim \mu} [\phi(D_{\nu}(x))] + \mathbb{E}_{x \sim \nu} [\phi(D_{\nu}(G_{\nu}(h))))] \right] + L_\phi Q_{\mathcal{L}_{h}, \mathcal{L}_{G}(\gamma, \nu)}(\gamma, \nu),
$$
where $\hat{Q}_{L_h,L_G}(\gamma,C) = L_h \| h - r(h) \|_2 + L_G \sum_{v \in C} \| v - r(h) \|_2^2$ and $E_h[\hat{Q}_{L_h,L_G}(\gamma,C)] = Q_{L_h,L_G}(\gamma,C)$. In the above derivation, the first equality holds by the definition of the neural net distance. The second inequality because of Lemma 1 and the fact that $\phi(\cdot)$ is a concave measuring function in Definition 4. Here, we suppose $\phi(\cdot)$ is a monotonically increasing function. The second inequality holds by the following derivation:

$$
\left| \phi \left( \hat{D}_v (G_u(h)) + \hat{Q}_{L_h,L_G}(\gamma,C) \right) - \phi \left( \hat{D}_v (G_u(h)) \right) \right|
\leq \left| \phi' \left( \hat{D}_v (G_u(h)) \right) \left[ \left( \hat{D}_v (G_u(h)) + \hat{Q}_{L_h,L_G}(\gamma,C) \right) - \hat{D}_v (G_u(h)) \right] \right|
= \left| \phi' \left( \hat{D}_v (G_u(h)) \right) \left[ \hat{Q}_{L_h,L_G}(\gamma,C) \right] \right|
\leq L_\phi \hat{Q}_{L_h,L_G}(\gamma,C),
$$

In the above derivation, the first inequality uses the concavity of measuring function $\phi(\cdot)$. The last inequality follows from that $|\phi'| \leq L_\phi$. Now by taking expectation w.r.t. $H_{r,n+1}$, we obtain

$$
E_{H \subseteq H_{r,n+1}} \left[ d_{f,\phi} \left( \hat{D}_{G_u,h}(\gamma(h)), D_{real} \right) \right] 
\leq E_{H \subseteq H_{r,n+1}} \left[ d_{f,\phi} \left( \hat{D}_{G_u,h}(\gamma(h)), D_{real} \right) + L_\phi \hat{Q}_{L_h,L_G}(\gamma,C) + 2\Delta. \right.
$$

10. Proof of Theorem 2

**Theorem 2** Under the condition of Theorem 1, and given an empirical distribution $\hat{D}_{real}$ drawn from $D_{real}$, then the following holds with probability at least $1 - \delta$,

$$
\left| E_H \left[ d_{f,\phi} \left( \hat{D}_{G_u,h}(\gamma(h)), D_{real} \right) \right] - \inf_{G} E_H \left[ d_{f,\phi} \left( D_{G_u,h}, D_{real} \right) \right] \right| 
\leq 2R_X(F) + 2\Delta \sqrt{\frac{2}{N} \log \left( \frac{1}{\delta} \right)} + 2\epsilon(d_M),
$$

where $R_X(F) = \max_{x \in X} \sum_{i=1}^{N} \sigma_i(D_v(x_i))$ and $\sigma_i \in \{-1,1\}$, $i = 1,2,\ldots,m$ are independent uniform random variables.

**Proof** For the real distribution $D_{real}$, we are interested in the generalization error in term of the following neural net distance:

$$
\left| E_H \left[ d_{f,\phi} \left( \hat{D}_{G_u,h}(\gamma(h)), D_{real} \right) \right] - \inf_{\gamma} E_H \left[ d_{f,\phi} \left( D_{G_u,h}, D_{real} \right) \right] \right|
\leq E_H \left[ d_{f,\phi} \left( \hat{D}_{G_u,h}(\gamma(h)), D_{real} \right) \right] - \inf_{\gamma} E_H \left[ d_{f,\phi} \left( D_{G_u,h}, D_{real} \right) \right]
= \left| E_H \left[ d_{f,\phi} \left( \hat{D}_{G_u,h}(\gamma(h)), D_{real} \right) - d_{f,\phi} \left( \hat{D}_{G_u,h}(\gamma(h)), D_{real} \right) \right] \right|
\leq \left| E_H \left[ d_{f,\phi} \left( \hat{D}_{G_u,h}(\gamma(h)), D_{real} \right) - d_{f,\phi} \left( \hat{D}_{G_u,h}(\gamma(h)), D_{real} \right) \right] \right|
\leq 2E_H \left[ \sup_{\gamma} \left| d_{f,\phi} \left( D_{G_u,h}, D_{real} \right) - d_{f,\phi} \left( D_{G_u,h}, D_{real} \right) \right| + \epsilon(d_M) \right]
\leq 2 \sum_{v \in F} \left| E_{D_v} \left[ \phi(D_v(x)) \right] - E_{D_v} \left[ \phi(D_v(x)) \right] \right| + \epsilon(d_M) \right|
\leq 2 \sum_{v \in F} \left| E_{D_v} \left[ \phi(D_v(x)) \right] - E_{D_v} \left[ \phi(D_v(x)) \right] \right| + 2\epsilon(d_M).
$$

In the above derivation, the first inequality holds by by Jensen’s inequality and the concavity of the infimum function. The second inequality holds by Theorem 1. The third inequality satisfies when we take supremum w.r.t. $G_u \in \mathcal{G}$. The
Adversarial Learning with Local Coordinate Coding

last inequality uses the definition of the neural net distance and holds by triangle inequality. This reduces the problem to bounding the distance

\[ d'_{F}(\hat{D}_{real}, \hat{D}_{real}) := \sup_{D_v \in F} \left| E_{x \in D_{real}} \left[ \phi(D_v(x)) \right] - E_{x \in \hat{D}_{real}} \left[ \phi(D_v(x)) \right] \right|, \]

between the true distribution and its empirical distribution. This can be achieved by the uniform concentration bounds developed in statistical learning theory, and thus the distance \( d'_{F}(\hat{D}_{real}, \hat{D}_{real}) \) can be achieved by the Rademacher complexity. Let \( x_1, x_2, \ldots, x_N \in \mathcal{X} \) be a set of \( N \) independent random samples in data space. We introduce a function

\[ h(x_1, x_2, \ldots, x_N) = \sup_{D_v \in F} \left| E_{x \in D_{real}} \left[ \phi(D_v(x)) \right] - E_{x \in \hat{D}_{real}} \left[ \phi(D_v(x)) \right] \right|. \]

Since measuring function \( \phi \) is Lipschitz and bounded in \([-\Delta, \Delta]\), changing \( x_i \) to another independent sample \( x'_i \) can change the function \( h \) by no more than \( 4\Delta N \), that is,

\[ h(x_1, \ldots, x_i, \ldots, x_N) - h(x_1, \ldots, x'_i, \ldots, x_N) \leq \frac{4\Delta}{N}, \]

for all \( i \in [1, N] \) and any points \( x_1, \ldots, x_N, x'_i \in \mathcal{X} \). McDiarmid’s inequality implies that with probability at least \( 1 - \delta \), the following inequality holds:

\[ \sup_{D_v \in F} \left| E_{x \in D_{real}} \left[ \phi(D_v(x)) \right] - E_{x \in \hat{D}_{real}} \left[ \phi(D_v(x)) \right] \right| \leq 2\sqrt{\frac{2\log \left( \frac{1}{\delta} \right)}{N}}. \]  

(8)

From the bound on Rademacher complexity, we have

\[ E \left[ \sup_{D_v \in F} \left| E_{x \in D_{real}} \left[ \phi(D_v(x)) \right] - E_{x \in \hat{D}_{real}} \left[ \phi(D_v(x)) \right] \right| \right] \leq 2E_{x,F} \left[ \sup_{D_v \in F} \frac{1}{N} \sum_{i=1}^{N} \phi(D_v(x_i)) \right] = 2R_X(F). \]  

(9)

Combining the inequalities (7), (8) and (9), we have

\[ E_H \left[ d_{F,\phi}(\hat{D}_{G_u}, \hat{D}_{real}) \right] - \inf_{G_u} E_H \left[ d_{F,\phi}(D_{G_u}, \hat{D}_{real}) \right] \leq 2R_X(F) + 2\Delta \sqrt{\frac{2\log \left( \frac{1}{\delta} \right)}{N}} + 2\epsilon(d_M). \]

\[ \square \]