
Supplementary Material to ‘Robust Nonparametric Regression under Poisoning Attack’

Anonymous Author(s)

Affiliation

Address

email

1 In this supplementary material, section 1 shows our implementation of the corrected estimator. Other
2 sections are proofs of the theoretical results.

3 1 Implementation of Corrected Estimator

4 The corrected estimation is

$$\hat{\eta}_c = \arg \min_{\|\nabla g\|_\infty \leq L} \|\hat{\eta}_0 - g\|_1. \quad (1)$$

5 In this section, we find a approximate numerical solution instead. In particular, we only optimize g at
6 grid points that are dense enough, and the values elsewhere can be simply calculated via interpolation.
7 The grid points are set to be $\mathbf{x}_{j_1, \dots, j_d} = \mathbf{x}_0 + (j_1, \dots, j_d)a$, with indices $j_k \in \{1, \dots, m_k\}$, m_k is
8 the grid count along k -th dimension. \mathbf{x}_0 and m_k need to satisfy

$$x_{0k} \leq \inf_{\mathbf{x} \in \mathcal{X}} x_k, \quad (2)$$

$$x_{0k} + m_k a \geq \sup_{\mathbf{x} \in \mathcal{X}} x_k, \quad (3)$$

9 so that these grid points cover the whole support. a is the grid size. Denote $\mathbf{j} = (j_1, \dots, j_d)$,
10 $g_{\mathbf{j}} = g(\mathbf{x}_{\mathbf{j}})$, and $r_{\mathbf{j}} = \hat{\eta}_0(\mathbf{x}_{\mathbf{j}})$. Then the discretized optimization problem can be formulated as
11 following:

$$\underset{g}{\text{minimize}} \quad \sum_{\mathbf{j}} |g_{\mathbf{j}} - r_{\mathbf{j}}| \quad (4)$$

$$\text{subject to} \quad |g_{\mathbf{j}} - g_{\mathbf{j}'}| \leq La, \forall |\mathbf{j}' - \mathbf{j}| = 1,$$

12 in which $|\mathbf{j}' - \mathbf{j}| = \sum_{k=1}^d |j'_k - j_k|$. With sufficiently small a , the discretized problem approximates
13 (1) well. (4) can be solved simply by optimizing each $g_{\mathbf{j}}$ iteratively.

14 2 Proof of Theorem 1: ℓ_2 Convergence of Initial Estimator

15 This section proves the convergence rate of the initial estimator

$$\hat{\eta}_0(\mathbf{x}) = \arg \min_{|s| \leq M} \sum_{i=1}^N K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) \phi(Y_i - s). \quad (5)$$

16 To begin with, we use the following notations.

17 **Definition 1.** Define

$$B_h(\mathbf{x}) = \{\mathbf{u} \mid \|\mathbf{u} - \mathbf{x}\| < h\} \quad (6)$$

18 as the ball centering at \mathbf{x} with radius h ,

$$q_h(\mathbf{x}) = |\{i | i \in \mathcal{B}, \mathbf{X}_i \in B_h(\mathbf{x})\}| \quad (7)$$

19 as the number of attacked samples within $B_h(\mathbf{x})$,

$$I_h(\mathbf{x}) = \{i | \mathbf{X}_i \in B_h(\mathbf{x})\} \quad (8)$$

20 as the set of the indices of all samples within $B_h(\mathbf{x})$, and

$$n_h(\mathbf{x}) = |I_h(\mathbf{x})| \quad (9)$$

21 as the total number of samples within $B_h(\mathbf{x})$.

22 **Definition 2.** Define $a(\mathbf{x})$, $b(\mathbf{x})$ as

$$a(\mathbf{x}) = \arg \min_{|s| \leq M} \sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) \phi(\eta(\mathbf{X}_i) + W_i - s), \quad (10)$$

23

$$b(\mathbf{x}) = \arg \min_{|s| \leq M} \sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) (\eta(\mathbf{X}_i) + W_i - s)^2, \quad (11)$$

24 $a(\mathbf{x})$ is the estimated value with no adversarial attacks. $b(\mathbf{x})$ is just the ordinary kernel regression
25 estimates clipped into $[-M, M]$. Then

$$|\hat{\eta}_0(\mathbf{x}) - \eta(\mathbf{x})| \leq |\hat{\eta}_0(\mathbf{x}) - a(\mathbf{x})| + |a(\mathbf{x}) - b(\mathbf{x})| + |b(\mathbf{x}) - \eta(\mathbf{x})|. \quad (12)$$

26 Note that $a(\mathbf{x})$ and $b(\mathbf{x})$ is not affected by the behavior of the attacker. Hence

$$\begin{aligned} R &= \mathbb{E} \left[\sup_{\mathcal{A}} (\hat{\eta}_0(\mathbf{X}) - \eta(\mathbf{X}))^2 \right] \\ &\leq 3\mathbb{E} \left[\sup_{\mathcal{A}} (\hat{\eta}_0(\mathbf{X}) - a(\mathbf{X}))^2 \right] + 3\mathbb{E} [(a(\mathbf{X}) - b(\mathbf{X}))^2] + 3\mathbb{E} [(b(\mathbf{X}) - \eta(\mathbf{X}))^2] \\ &:= 3(I_1 + I_2 + I_3), \end{aligned} \quad (13)$$

27 now we bound these three terms separately.

28 **Bound of I_1 .** Define a new random variable

$$Z = 2Lh + \max_{i \in [N]} W_i - \min_{i \in [N]} W_i, \quad (14)$$

29 in which $[N] = \{1, \dots, N\}$. Then Z can be bounded using the following lemma.

30 **Lemma 1.** If $t > 2Lh$, then

$$P(Z > t) \leq 2 \exp \left[- \min \left\{ \frac{(t - 2Lh)^2}{8\sigma^2}, \frac{t - 2Lh}{4\sigma} \right\} + \ln N \right], \quad (15)$$

31 and for $t > 2Lh + 4\sigma \ln N$,

$$\mathbb{E}[Z^2 \mathbf{1}(Z > t)] \leq 2N(t^2 + 32\sigma^2 + 8t\sigma) e^{-\frac{t-2Lh}{4\sigma}}. \quad (16)$$

32 Given Z , $|\hat{\eta}_0(\mathbf{x}) - a(\mathbf{x})|$ can be bounded. Define

$$r(\mathbf{x}) = \frac{C_K q_h(\mathbf{x})}{c_K (n_h(\mathbf{x}) - q_h(\mathbf{x}))}, \quad (17)$$

33 in which n_h is defined in (9), and

$$n_0 = \frac{1}{2} \alpha f_m v_d h^d N. \quad (18)$$

34 Then the following lemmas hold:

35 **Lemma 2.** If $r(\mathbf{x}) \leq (T - Z)/(T + Z)$, then $|\hat{\eta}_0(\mathbf{x}) - a(\mathbf{x})| \leq (T + Z)r(\mathbf{x})$.

36 **Lemma 3.** *Under the following three conditions:*

37 (a) $n_h(\mathbf{x}) \geq n_0$, in which v_d is the volume of d dimensional unit ball;

38 (b) $Z \leq 2Lh + 8\sigma \ln N$;

39 (c) $q_h(\mathbf{x}) \leq c_K n_0 / (3C_K + c_K)$,

40 then

$$|\hat{\eta}_0(\mathbf{x}) - a(\mathbf{x})| \leq \frac{2TC_K q_h(\mathbf{x})}{c_K n_0}. \quad (19)$$

41 Moreover, since $|\hat{\eta}_0(\mathbf{x})| \leq M$, and according to Assumption 1(b), $|\eta(\mathbf{x})| \leq M$, $|\hat{\eta}_0(\mathbf{x})| \leq 2M$
 42 always hold, regardless of whether the conditions (a)-(c) in Lemma 3 are satisfied. Therefore

$$\begin{aligned} I_1 &= \mathbb{E} \left[\sup_{\mathcal{A}} (\hat{\eta}_0(\mathbf{X}) - a(\mathbf{X}))^2 \right] \\ &= \mathbb{E} \left[\sup_{\mathcal{A}} \int (\hat{\eta}_0(\mathbf{x}) - a(\mathbf{x}))^2 f(\mathbf{x}) d\mathbf{x} \right] \\ &\leq \frac{4C_K^2 T^2}{c_K^2 n_0^2} f_M \sup_{\mathcal{A}} \int q_h^2(\mathbf{x}) d\mathbf{x} + 4M^2 [\mathbb{P}(n_h(\mathbf{x}) < n_0) + \mathbb{P}(Z > 2Lh + 8\sigma \ln N)] \\ &\quad + \sup_{\mathcal{A}} \mathbb{P} \left(q_h(\mathbf{X}) > \frac{c_K}{3C_K + c_K} n_0 \right). \end{aligned} \quad (20)$$

43 Now we bound each term separately. For the third term in (20),

$$\begin{aligned} \sup_{\mathcal{A}} \int q_h^2(\mathbf{x}) d\mathbf{x} &\leq \sup_{\mathcal{A}} \int \left(\sum_{i \in \mathcal{B}} \mathbf{1}(\|\mathbf{x} - \mathbf{X}_i\| < h) \right)^2 d\mathbf{x} \\ &\leq |\mathcal{B}| \sup_{\mathcal{A}} \int \sum_{i \in \mathcal{B}} \mathbf{1}(\|\mathbf{x} - \mathbf{X}_i\| < h) d\mathbf{x} \\ &= |\mathcal{B}|^2 v_d h^d = q^2 v_d h^d; \end{aligned} \quad (21)$$

44 For the second term in (20), since $\mathbb{E}[n_h(\mathbf{x})] \geq f_m \alpha v_d h^d N = 2n_0$,

$$\mathbb{P}(n_h(\mathbf{x}) < n_0) \leq e^{-(1-\ln 2)n_0}. \quad (22)$$

45 Assumption 3 requires $h > \ln^2 N / N$. Recall (18), $n_0 \sim Nh^d \gtrsim \ln^2 N$, thus (22) decays faster than
 46 any polynomial of n_0 . For the third term in (20), from Lemma 1,

$$\mathbb{P}(Z > 2Lh + 8\sigma \ln N) \leq \frac{2}{N}; \quad (23)$$

47 Finally, for the last term in (20),

$$\mathbb{P} \left(q_h(\mathbf{X}) > \frac{c_K}{3C_K + c_K} n_0 \right) \leq \frac{\mathbb{E}[q_h^2(\mathbf{X})]}{\left(\frac{c_K}{3C_K + c_K} n_0 \right)^2} \leq \frac{(3C_K + c_K)^2 f_M}{c_K^2 n_0^2} \int q_h^2(\mathbf{x}) d\mathbf{x} \lesssim \frac{q^2 h^d}{n_0^2}. \quad (24)$$

48 Therefore

$$I_1 \lesssim \frac{T^2 q^2 h^d}{n_0^2} + e^{-(1-\ln 2)n_0} + \frac{2}{N} + \frac{q^2 h^d}{n_0} \lesssim \frac{T^2 q^2}{N^2 h^d}. \quad (25)$$

49 **Bound of I_2 .**

50 **Lemma 4.** *If $Z \leq T$, then $a(\mathbf{x}) - b(\mathbf{x}) = 0$.*

51 Lemma 4 will also be used later in other theorems.

Proof.

$$\max_{i \in I_h(\mathbf{x})} (\eta(\mathbf{X}_i) + W_i) - \min_{i \in I_h(\mathbf{x})} (\eta(\mathbf{X}_i) + W_i) \leq T. \quad (26)$$

52 Therefore $\phi(\eta(\mathbf{X})_i + W_i - s) = (\eta(\mathbf{X}_i) + W_i - s)^2$ for $\min_{i \in I_h(\mathbf{x})} (\eta(\mathbf{X}_i) + W_i) \leq s \leq \max_{i \in I_h(\mathbf{x})} (\eta(\mathbf{X}_i) +$
 53 $W_i)$. From (10) and 11, $a(\mathbf{x}) - b(\mathbf{x}) = 0$. \square

54 If $Z > T$, (10) and (11) gives $|a(\mathbf{x}) - b(\mathbf{x})| \leq 2M$. Therefore, from Lemma 1,

$$I_2 = \mathbb{E}[(a(\mathbf{X}) - b(\mathbf{X}))^2] \leq 4M^2\mathbb{P}(Z > T) \leq \frac{8M^2}{N^3}. \quad (27)$$

55 **Bound of I_3 .** Since W_i is sub-exponential, it is straightforward to show that the variance is bounded
56 by σ^2 :

$$\mathbb{E}[W_i^2] = \mathbb{E} \left[\lim_{\lambda \rightarrow 0} \frac{2}{\lambda^2} (e^{\lambda W_i} - 1 - \lambda W_i) \right] \leq \liminf_{\lambda \rightarrow 0} \frac{2}{\lambda^2} (e^{\frac{1}{2}\sigma^2\lambda^2} - 1) = \sigma^2, \quad (28)$$

57 in which we used Fatou's lemma in the second step. Then I_3 can simply be bounded by standard
58 analysis of kernel regression [4, 5, 1]. For the completeness of the paper, we provide a brief proof
59 here.

60 If $n_h(\mathbf{x}) \geq n_0$, in which n_0 is defined in (18), then with the Lipschitz assumption (Assumption 1(a)),

$$\begin{aligned} |b(\mathbf{x}) - \eta(\mathbf{x})| &\leq \left| \frac{\sum_{i \in I_h(\mathbf{x})} K\left(\frac{\mathbf{x} - \mathbf{X}_i}{h}\right) (\eta(\mathbf{X}_i) - \eta(\mathbf{x}))}{\sum_{i \in I_h(\mathbf{x})} K\left(\frac{\mathbf{x} - \mathbf{X}_i}{h}\right)} \right| + \left| \frac{\sum_{i \in I_h(\mathbf{x})} K\left(\frac{\mathbf{x} - \mathbf{X}_i}{h}\right) W_i}{\sum_{i \in I_h(\mathbf{x})} K\left(\frac{\mathbf{x} - \mathbf{X}_i}{h}\right)} \right| \\ &\leq Lh + \frac{1}{n_0 c_K} \left| \sum_{i \in I_h(\mathbf{x})} K\left(\frac{\mathbf{x} - \mathbf{X}_i}{h}\right) W_i \right|. \end{aligned} \quad (29)$$

61 If $n_h(\mathbf{x}) < n_0$, then $|b(\mathbf{x}) - \eta(\mathbf{x})| \leq 2M$. Since $\mathbb{E}[W_i] = 0$, $\mathbb{E}[W_i^2] \leq \sigma^2$,

$$\mathbb{E}[(b(\mathbf{x}) - \eta(\mathbf{x}))^2] \leq L^2 h^2 + \frac{\sigma^2 C_k^2}{n_0 c_K^2} + 4M^2 \mathbb{P}(n_h(\mathbf{x}) < n_0). \quad (30)$$

62 Using (22), integrate (30) over the whole support,

$$I_3 \lesssim h^2 + \frac{1}{n_0} \sim h^2 + \frac{1}{Nh^d}. \quad (31)$$

63 Combine (13), (25), (27) and (31),

$$R \lesssim \frac{T^2 q^2}{N^2 h^d} + h^2 + \frac{1}{Nh^d}. \quad (32)$$

64 **3 Proof of Theorem 2: ℓ_∞ Convergence of Initial Estimator**

65 In the following proof, we assume that

$$h > \left(\frac{2(3C_K + c_K)q}{c_K \alpha f_m v_d N} \right)^{\frac{1}{d}}. \quad (33)$$

66 If (33) does not hold, then $q/(Nh^d) \gtrsim 1$. Since $|\hat{\eta}_0(\mathbf{x})| \leq M$ always hold, we have

$$|\hat{\eta}_0(\mathbf{x}) - \eta(\mathbf{x})| \leq 2M \lesssim \frac{q}{Nh^d} \lesssim \frac{Tq}{Nh^d} + h + \frac{\ln N}{\sqrt{Nh^d}}, \quad (34)$$

67 thus Theorem 2 is proved trivially. From now on, assume (33) holds.

68 To begin with, define event E , which is true if all of the three conditions hold:

69 (1) $\max_i W_i \leq 4\sigma \ln N$, $\min_i W_i \geq -4\sigma \ln N$;

70 (2) $n_0 \leq n_h(\mathbf{x}) \leq n_M$, $\forall \mathbf{x} \in \mathcal{X}$, in which n_0 is defined in (18), $n_h(\mathbf{x})$ is defined in (9), and

$$n_M = \frac{3}{2} N f_M v_d h^d; \quad (35)$$

71 (3) For all $\mathbf{x} \in \mathcal{X}$ and any $k \in \{1, \dots, N\}$,

$$\left| \sum_{i \in \mathcal{N}_k(\mathbf{x})} W_i \right| \leq \sigma \max\{\sqrt{k} \ln N, \ln^2 N\}, \quad (36)$$

72 in which $\mathcal{N}_k(\mathbf{x})$ is the set of all samples among k nearest neighbors of \mathbf{x} . We remark that according
 73 to (14), (1) implies that $Z \leq 2Lh + 8\sigma \ln N$.

74 Denote the complement of E as E^c . Now we bound $P(E^c)$. From (83), $P(\max_i W_i > 4\sigma \ln N) \leq$
 75 $1/N$. Similar bound holds for $\min_i W_i$. This bounds the probability of violating (1). (2) and (3) can
 76 be bounded using the following two lemmas:

77 **Lemma 5.** *For sufficiently large N , with probability at least $1 - 1/N$,*

$$\inf_{\mathbf{x} \in \mathcal{X}} n_h(\mathbf{x}) \geq n_0, \quad (37)$$

$$\sup_{\mathbf{x} \in \mathcal{X}} n_h(\mathbf{x}) \leq n_M. \quad (38)$$

78 **Lemma 6.** *Let $[N] = \{1, \dots, N\}$. Then*

$$P\left(\exists \mathbf{x} \in \mathbf{X}, \exists k \in [N], \left| \sum_{i \in \mathcal{N}_k(\mathbf{x})} W_i \right| > \sigma \max\{\sqrt{k} \ln N, \ln^2 N\}\right) \leq 2dN^{2d+1} e^{-\frac{1}{2} \ln^2 N}. \quad (39)$$

79 Therefore

$$P(E^c) \leq \frac{3}{N} + 2dN^{2d+1} e^{-\frac{1}{2} \ln^2 N}. \quad (40)$$

80 Now we bound ℓ_∞ error with the condition that E is true.

$$|\hat{\eta}_0(\mathbf{x}) - \eta(\mathbf{x})| \leq |\hat{\eta}_0(\mathbf{x}) - a(\mathbf{x})| + |a(\mathbf{x}) - b(\mathbf{x})| + |b(\mathbf{x}) - \eta(\mathbf{x})|. \quad (41)$$

81 **Bound of the first term in (41).** Under E , condition (a), (b) in Lemma 3 are satisfied. Moreover,
 82 from (33) and (18), condition (c) also hold. According to Lemma 3,

$$|\hat{\eta}_0(\mathbf{x}) - a(\mathbf{x})| \leq \frac{2TC_K q}{c_K n_0}. \quad (42)$$

83 **Bound of the second term in (41).** Recall that $Z \leq 2Lh + 8\sigma \ln N < T$, from Lemma 4,
 84 $a(\mathbf{x}) - b(\mathbf{x}) = 0$.

85 **Bound of the third term in (41).** We use the following additional lemma:

86 **Lemma 7.** *If E is true, then*

$$\left| \sum_{i=1}^N K\left(\frac{\mathbf{x} - \mathbf{X}_i}{h}\right) W_i \right| \leq C_K \sqrt{n_M} \ln N. \quad (43)$$

87 From (29) and Lemma 7,

$$|b(\mathbf{x}) - \eta(\mathbf{x})| \leq Lh + \frac{C_K}{n_0 c_K} \sqrt{n_M} \ln N. \quad (44)$$

88 Substitute these results into (41), and recall that $n_0 \sim Nh^d$, $n_M \sim Nh^d$, under E ,

$$|\hat{\eta}_0(\mathbf{x}) - \eta(\mathbf{x})| \lesssim \frac{Tq}{Nh^d} + h + \frac{\ln N}{\sqrt{Nh^d}}, \quad (45)$$

89 Under E^c , $|\hat{\eta}_0(\mathbf{x}) - \eta(\mathbf{x})|$ can be bounded by $2M$, hence

$$\begin{aligned} \mathbb{E}[\|\hat{\eta}_0 - \eta\|] &\leq \mathbb{E}[\|\hat{\eta}_0 - \eta\| \mathbf{1}(E)] + 2MP(E^c) \\ &\lesssim \frac{Tq}{Nh^d} + h + \frac{\ln N}{\sqrt{Nh^d}}. \end{aligned} \quad (46)$$

90 The proof is complete.

91 **4 Proof of Theorem 3: Minimax Convergence Rate**

92 The proof begins with the following lemma.

93 **Lemma 8.** *Let p_1, p_2 be the pdf of $\mathcal{N}(\mu_1, \sigma^2)$ and $\mathcal{N}(\mu_2, \sigma^2)$ respectively, with \mathcal{N} being the normal*
 94 *distribution. Then there exists $\alpha \in [0, |\mu_1 - \mu_2|/(2\sigma)]$ and two other pdfs q_1, q_2 , such that*

$$(1 - \alpha)p_1 + \alpha q_1 = (1 - \alpha)p_2 + \alpha q_2. \quad (47)$$

95 *Proof.* Let

$$\begin{aligned} q_1 &= \frac{1 - \alpha}{\alpha}(p_2 - p_1)\mathbf{1}(p_2 \geq p_1), \\ q_2 &= \frac{1 - \alpha}{\alpha}(p_1 - p_2)\mathbf{1}(p_2 < p_1), \end{aligned} \quad (48)$$

96 then (47) holds. Note that q_1 and q_2 need to be normalized:

$$\begin{aligned} \int q_1(u)du &= \frac{1 - \alpha}{\alpha} \int (p_2(u) - p_1(u))\mathbf{1}(p_2(u) \geq p_1(u))du \\ &= \frac{1 - \alpha}{\alpha} \mathbb{T}\mathbb{V}(p_1, p_2), \end{aligned} \quad (49)$$

97 in which $\mathbb{T}\mathbb{V}$ is the total variation distance. Hence (47) can be achieved with

$$\alpha = \frac{\mathbb{T}\mathbb{V}(p_1, p_2)}{1 + \mathbb{T}\mathbb{V}(p_1, p_2)}. \quad (50)$$

98 From Pinsker's inequality,

$$\mathbb{T}\mathbb{V}(p_1, p_2) \leq \sqrt{\frac{1}{2}D_{KL}(p_1||p_2)} = \frac{|\mu_1 - \mu_2|}{2\sigma}. \quad (51)$$

99 With (50) and (51), the proof is complete. \square

100 Let

$$\eta_1(\mathbf{x}) = 0, \quad (52)$$

$$\eta_2(\mathbf{x}) = L \max\{r - \|\mathbf{x}\|, 0\}, \quad (53)$$

101 in which

$$r = \left(\frac{\sigma(d+1)q}{f_m L v_d N} \right)^{\frac{1}{d+1}}. \quad (54)$$

102 Let $\eta \in \{\eta_1, \eta_2\}$. Furthermore, assume that the noise variables are Gaussian, i.e. $W_i \sim \mathcal{N}(0, \sigma^2)$.
 103 Assume $f = f_m$ for $\mathbf{x} \in \mathcal{X}$. Design the attack strategy as following: go through all samples from
 104 $i = 1$ to N , and initialize $|\mathcal{B}_0| = \emptyset$, then

105 (1) If $\|\mathbf{X}_i\| > r$, do not attack;

106 (2) If $\|\mathbf{X}_i\| \leq r$, then find α_i, q_{i1}, q_{i2} such that $(1 - \alpha_i)p_{i1} + \alpha_i q_{i1} = (1 - \alpha_i)p_{i2} + \alpha_i q_{i2}$, in which $p_{i1},$
 107 p_{i2} is the pdf of $\mathcal{N}(\eta_1(\mathbf{X}_i), \sigma^2)$ and $\mathcal{N}(\eta_2(\mathbf{X}_i), \sigma^2)$, respectively. With probability α_i , incorporate
 108 sample i into \mathcal{B}_0 ;

109 (3) Repeat (1), (2) for $i = 1, \dots, N$;

110 (4) If $|\mathcal{B}_0| \leq q$, then attack all samples in \mathcal{B}_0 . Otherwise, pick q samples randomly from \mathcal{B}_0 to attack.
 111 For each attacked sample $i \in \mathcal{B}_0$, let it follow distribution q_1 if $\eta = \eta_1$ and q_2 if $\eta = \eta_2$.

112 Use Lemma 8, and denote s_d as the $d - 1$ dimensional surface area of a d dimensional unit ball.
 113 $s_d = dv_d$. Then

$$\begin{aligned}
 \mathbb{P}(i \in \mathcal{B}_0) &\leq \int f(\mathbf{x}) \frac{|\eta_2(\mathbf{x}) - \eta_1(\mathbf{x})|}{2\sigma} d\mathbf{x} \\
 &= \frac{f_m L}{2\sigma} \int_{\|\mathbf{x}\| \leq r} (r - \|\mathbf{x}\|) d\mathbf{x} \\
 &= \frac{f_m L}{2\sigma} \int_0^r (r - u) s_d u^{d-1} du \\
 &= \frac{f_m L s_d}{2\sigma d(d+1)} r^{d+1} \\
 &= \frac{q}{2N}. \tag{55}
 \end{aligned}$$

114 From Chernoff inequality, it can be easily shown that $\mathbb{P}(|\mathcal{B}_0| > q) \leq e^{-(\ln 2 - 1/2)q}$. Therefore with
 115 high probability, all samples in \mathcal{B}_0 will be attacked, and the distribution of Y_i conditional on the
 116 value of \mathbf{X}_i has no difference between η_1 and η_2 . This indicates that η_1 and η_2 are indistinguishable.
 117 Therefore

$$\begin{aligned}
 \inf_{\hat{\eta}_0} \sup_{(f, \eta, \mathbb{P}_N) \in \mathcal{F}} \mathbb{E} \left[\sup_{\mathcal{A}} (\hat{\eta}_0(\mathbf{X}) - \eta(\mathbf{X}))^2 \right] &\geq \inf_{\hat{\eta}_0} \sup_{\eta \in \{\eta_1, \eta_2\}} \mathbb{E} \left[\sup_{\mathcal{A}} (\hat{\eta}_0(\mathbf{X}) - \eta(\mathbf{X}))^2 \right] \\
 &\geq (1 - \mathbb{P}(|\mathcal{B}_0| > q)) \frac{1}{4} \int (\eta_1(\mathbf{x}) - \eta_2(\mathbf{x}))^2 d\mathbf{x} \\
 &\geq \frac{1}{4} \left(1 - e^{-(\ln 2 - \frac{1}{2})q}\right) L^2 \int_0^r (r - u)^2 s_d u^{d-1} du \\
 &\gtrsim r^{d+2} \\
 &\gtrsim \left(\frac{q}{N}\right)^{\frac{d+2}{d+1}}, \tag{56}
 \end{aligned}$$

118 and similarly, the ℓ_∞ error can be lower bounded by

$$\begin{aligned}
 \inf_{\hat{\eta}} \sup_{(f, \eta, \mathbb{P}_N) \in \mathcal{F}} \mathbb{E} \left[\sup_{\mathcal{A}} \sup_{\mathbf{x}} |\hat{\eta}(\mathbf{x}) - \eta(\mathbf{x})| \right] &\geq \frac{1}{4} \left(1 - e^{-(\ln 2 - \frac{1}{2})q}\right) Lr \\
 &\gtrsim r \\
 &\gtrsim \left(\frac{q}{N}\right)^{\frac{1}{d+1}}. \tag{57}
 \end{aligned}$$

119 Moreover, even if there are no adversarial samples, from standard minimax analysis [6], it can be
 120 easily shown that

$$\inf_{\hat{\eta}_0} \sup_{(f, \eta, \mathbb{P}_N) \in \mathcal{F}} \mathbb{E} \left[(\hat{\eta}_0(\mathbf{X}) - \eta(\mathbf{X}))^2 \right] \gtrsim N^{-\frac{2}{d+2}}, \tag{58}$$

121 and

$$\inf_{\hat{\eta}} \sup_{(f, \eta, \mathbb{P}_N) \in \mathcal{F}} \mathbb{E} \left[\sup_{\mathcal{A}} \sup_{\mathbf{x}} |\hat{\eta}(\mathbf{x}) - \eta(\mathbf{x})| \right] \gtrsim N^{-\frac{1}{d+2}}. \tag{59}$$

122 Combine (56), (57), (58) and (59), the proof is complete.

123 5 Proof of Uniqueness of Corrected Estimator

124 Suppose that there are two solutions, g_1^*, g_2^* , such that $g_1^*(\mathbf{x}) \neq g_2^*(\mathbf{x})$ for some \mathbf{x} , and

$$\|\hat{\eta}_0 - g_1^*\|_1 = \|\hat{\eta}_0 - g_2^*\| \leq \|\hat{\eta}_0 - g\|, \tag{60}$$

125 for any L -Lipschitz function g . Since g_1^* and g_2^* are Lipschitz continuous, there must be a compact
 126 region around \mathbf{x} such that $g_1^* \neq g_2^*$ everywhere in this region.

127 We first show that for all \mathbf{x} with $g_1^*(\mathbf{x}) \neq g_2^*(\mathbf{x})$,

$$(\hat{\eta}_0(\mathbf{x}) - g_1^*(\mathbf{x}))(\hat{\eta}_0(\mathbf{x}) - g_2^*(\mathbf{x})) \geq 0. \quad (61)$$

128 Let $g_a = (g_1^* + g_2^*)/2$. If $\hat{\eta}_0(\mathbf{x}) - g_1^*(\mathbf{x})$ and $\hat{\eta}_0(\mathbf{x}) - g_2^*(\mathbf{x})$ have opposite sign, then

$$|g_a(\mathbf{x}) - \hat{\eta}_0(\mathbf{x})| < \frac{1}{2}(|g_1^*(\mathbf{x}) - \hat{\eta}_0(\mathbf{x})| + |g_2^*(\mathbf{x}) - \hat{\eta}_0(\mathbf{x})|), \quad (62)$$

129 thus $\|g_a - \hat{\eta}_0\|_1 < (\|g_1^* - \hat{\eta}_0\|_1 + \|g_2^* - \hat{\eta}_0\|_1)$, contradicts (60). Therefore (61) holds. This
 130 indicates that the support \mathcal{X} can be divided into S_1 and S_2 , such that in $\max\{g_1^*, g_2^*\} \leq \hat{\eta}_0$ within
 131 S_1 , $\min\{g_1^*, g_2^*\} \geq \hat{\eta}_0$ within S_2 .

132 Then let

$$g_b(\mathbf{x}) = \begin{cases} \max\{g_1^*(\mathbf{x}), g_2^*(\mathbf{x})\} & \text{if } x \in S_1 \\ \min\{g_1^*(\mathbf{x}), g_2^*(\mathbf{x})\} & \text{if } x \in S_2, \end{cases} \quad (63)$$

133 then it can be easily shown that g_b is Lipschitz and $\|\hat{\eta}_0 - g\| < \max\{\|\hat{\eta}_0 - g_1^*\|, \|\hat{\eta}_0 - g_2^*\|\}$,
 134 contradicts (60). The proof is complete.

135 6 Proof of Theorem 4: Convergence Rate of Corrected Estimator

136 Denote $F[\eta]$ as the solution of the optimization problem

$$\begin{aligned} & \underset{g}{\text{minimize}} && \|\eta - g\|_1 \\ & \text{subject to} && \|\nabla g\|_\infty \leq L. \end{aligned} \quad (64)$$

137 Then the corrected estimate is $\hat{\eta}_c = F[\hat{\eta}_0]$, with $\hat{\eta}_0$ being the initial estimate. The following lemma
 138 holds:

139 **Lemma 9.** *For some η_1, η_2 , If $\eta_1(\mathbf{x}) \leq \eta_2(\mathbf{x}), \forall \mathbf{x} \in \mathcal{X}$, then $F[\eta_1](\mathbf{x}) \leq F[\eta_2](\mathbf{x}), \forall \mathbf{x} \in \mathcal{X}$.*

140 Denote E as the event that $\inf_x n_h(\mathbf{x}) \geq n_0$, $\sup_x n_h(\mathbf{x}) \leq 3Nf_M v_d h^d / 2$, and $Z \leq 2Lh + 8\sigma \ln N$.

141 From Lemma 1, $P(Z > 2Lh + 8\sigma \ln N) \leq 2/N$. Combine with Lemma 5, the probability of
 142 violating E can be bounded by

$$P(E^c) \leq \frac{3}{N}, \quad (65)$$

143 in which E^c is the complement of E .

144 In the following analysis, we bound the estimation error under the condition that E is true. We show
 145 the following additional lemma:

Lemma 10.

$$P\left(\left|\sum_{i \in I_h(\mathbf{x})} K\left(\frac{\mathbf{x} - \mathbf{X}_i}{h}\right) W_i\right| > 3C_k \sigma \sqrt{N f_M v_d h^d \ln N} | E\right) \leq \frac{2}{N^2}. \quad (66)$$

146 With these lemmas, we analyze the corrected estimator $\hat{\eta}_c$ under E . To begin with, $\hat{\eta}_0$ satisfies

$$|\hat{\eta}_0(\mathbf{x}) - \eta(\mathbf{x})| \leq |\hat{\eta}_0(\mathbf{x}) - a(\mathbf{x})| + |a(\mathbf{x}) - b(\mathbf{x})| + |b(\mathbf{x}) - \eta(\mathbf{x})|. \quad (67)$$

147 From Lemma 3, Under E ,

$$|\hat{\eta}_0(\mathbf{x}) - a(\mathbf{x})| \leq \frac{2TC_K q_h(\mathbf{x})}{c_K n_0} + 2M\mathbf{1}\left(q_h(\mathbf{x}) > \frac{c_k n_0}{3C_K + c_K}\right); \quad (68)$$

148 From Lemma 4, under E , and Assumption 3, $Z \leq T/2$, thus $a(\mathbf{x}) - b(\mathbf{x}) = 0$;

149 From (29),

$$\begin{aligned} |b(\mathbf{x}) - \eta(\mathbf{x})| & \leq Lh + \frac{3C_K \sigma}{c_K n_0} \sqrt{N f_M v_d h^d \ln N} \\ & \quad + 2M\mathbf{1}\left(\left|\sum_{i \in I_h(\mathbf{x})} K\left(\frac{\mathbf{x} - \mathbf{X}_i}{h}\right) W_i\right| > 3C_K \sigma \sqrt{N f_M v_d h^d \ln N}\right). \end{aligned} \quad (69)$$

150 Define

$$S := \left\{ \mathbf{x} \mid \left| \sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) W_i \right| > 3C_K \sigma \sqrt{N f_M v_d h^d \ln N} \right\}, \quad (70)$$

151

$$\delta(\mathbf{x}) := \frac{2TC_K q_h(\mathbf{x})}{c_K n_0} + Lh + 3C_K \sigma \sqrt{N f_M v_d h^d \ln N} + 2M \mathbf{1} \left(q_h(\mathbf{x}) > \frac{c_k n_0}{3C_K + c_K} \right) + 2M \mathbf{1}(\mathbf{x} \in S). \quad (71)$$

152 Therefore, under E , $|\hat{\eta}_0(\mathbf{x}) - \eta(\mathbf{x})| \leq \delta(\mathbf{x})$. Furthermore, define

$$\eta_1(\mathbf{x}) := \eta(\mathbf{x}) - \delta(\mathbf{x}), \quad (72)$$

$$\eta_2(\mathbf{x}) := \eta(\mathbf{x}) + \delta(\mathbf{x}), \quad (73)$$

153 then $\eta_1 \leq \hat{\eta}_0 \leq \eta_2$ under E . From Lemma 9, $F[\eta_1] \leq F[\eta_0] \leq F[\eta_2]$. The error of $F[\eta_0]$ can be
154 bounded by the error of $F[\eta_1]$ and $F[\eta_2]$. Define

$$\Delta := Lh + 3C_K \sigma \sqrt{N f_M v_d h^d \ln N}. \quad (74)$$

155 The next lemma bounds $\|F[\eta_1] - \eta\|_2^2$ and $\|F[\eta_2] - \eta\|_2^2$:

156 **Lemma 11.** Under E ,

$$\max \{ \|F[\eta_1] - \eta\|_2^2, \|F[\eta_2] - \eta\|_2^2 \} \lesssim \left(\frac{Tq}{N} \right)^{\frac{d+2}{d+1}} + h^2 + \frac{\ln N}{Nh^d}. \quad (75)$$

157 Therefore

$$\|F[\hat{\eta}_0] - \eta\|_2^2 \lesssim \left(\frac{Tq}{N} \right)^{\frac{d+2}{d+1}} + h^2 + \frac{\ln N}{Nh^d}. \quad (76)$$

158 The overall risk can be bounded by

$$\begin{aligned} \mathbb{E} \left[\sup_{\mathcal{A}} (\hat{\eta}_c(\mathbf{X}) - \eta(\mathbf{X}))^2 \right] &\leq f_M \mathbb{E} \left[\sup_{\mathcal{A}} \|\hat{\eta}_c - \eta\|_2^2 \mathbf{1}(E) \right] + 4M^2 \mathbf{P}(E^c) \\ &\lesssim \left(\frac{Tq}{N} \right)^{\frac{d+2}{d+1}} + h^2 + \frac{\ln N}{Nh^d}. \end{aligned} \quad (77)$$

159 The proof of ℓ_2 bound is complete.

160 For the ℓ_∞ bound, note that

$$\hat{\eta}_0 \leq \eta + \|\hat{\eta}_0 - \eta\|_\infty, \quad (78)$$

161 thus from Lemma 9,

$$\hat{\eta}_c = F[\hat{\eta}_0] \leq F[\eta + \|\hat{\eta}_0 - \eta\|_\infty] = \eta + \|\hat{\eta}_0 - \eta\|_\infty. \quad (79)$$

162 Similarly,

$$\hat{\eta}_c \geq \eta - \|\hat{\eta}_0 - \eta\|_\infty. \quad (80)$$

163 Hence

$$\|\hat{\eta}_c - \eta\|_\infty \leq \|\hat{\eta}_0 - \eta\|_\infty. \quad (81)$$

164 This indicates that the ℓ_∞ error of the corrected estimator does not exceed the initial estimator.
165 Therefore, Theorem 2 can be directly used here.

166 7 Proof of Lemmas

167 7.1 Proof of Lemma 1

168 **Proof of (15).** Recall Assumption 1(d). Let $W_{max} = \max_i W_i$, $W_{min} = \min_i W_i$ for $i = 1, \dots, N$.
169 For $|\lambda| \leq 1/\sigma$,

$$\mathbb{E}[e^{\lambda W_{max}}] \leq \sum_{i=1}^N \mathbb{E}[e^{\lambda W_i}] \leq N e^{\frac{1}{2} \lambda^2 \sigma^2}. \quad (82)$$

170 Then

$$\begin{aligned} \mathbb{P}(W_{max} > t) &\leq N \inf_{|\lambda| \leq 1/\sigma} e^{-\lambda t} e^{\frac{1}{2}\lambda^2 \sigma^2} \\ &\leq \exp \left[-\min \left\{ \frac{t^2}{2\sigma^2}, \frac{t}{2\sigma} \right\} + \ln N \right]. \end{aligned} \quad (83)$$

171 Similar bound holds for W_{min} . Then

$$\begin{aligned} \mathbb{P}(W_{max} - W_{min} > t) &\leq \mathbb{P} \left(W_{max} > \frac{t}{2} \right) + \mathbb{P} \left(W_{min} < -\frac{t}{2} \right) \\ &\leq 2 \exp \left[-\left\{ \frac{t^2}{8\sigma^2}, \frac{t}{4\sigma} \right\} + \ln N \right]. \end{aligned} \quad (84)$$

172 From (14), $Z = W_{max} - W_{min} + 2Lh^\gamma$, hence (15) holds.

173 **Proof of (16).**

$$\begin{aligned} \mathbb{E}[Z^2 \mathbf{1}(Z > t)] &\leq \int_0^{t^2} \mathbb{P}(Z > t) du + \int_{t^2}^\infty \mathbb{P}(Z > \sqrt{u}) du \\ &= t^2 \mathbb{P}(Z > t) + 2 \int_{t^2}^\infty \exp \left[-\frac{\sqrt{u} - 2Lh^\gamma}{4\sigma} + \ln N \right] du \\ &\leq 2N(s^2 + 32\sigma^2 + 8s\sigma) e^{\frac{t - 2Lh^\gamma}{4\sigma}}. \end{aligned} \quad (85)$$

174 7.2 Proof of Lemma 2

175 We first discuss the case when

$$\sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) \phi'(\eta(\mathbf{X}_i) + W_i - a(\mathbf{x})) = 0. \quad (86)$$

176 According to (10), this happens if the minimum value in (10) is reached within $[-M, M]$.

$$\begin{aligned} \left| \sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) \phi'(Y_i - a(\mathbf{x})) \right| &= \left| \sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) [\phi'(Y_i - a(\mathbf{x})) - \phi'(\eta(\mathbf{X}_i) + W_i - a(\mathbf{x}))] \right| \\ &\leq \sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) |\phi'(Y_i - a(\mathbf{x})) - \phi'(\eta(\mathbf{X}_i) + W_i - a(\mathbf{x}))| \\ &\stackrel{(a)}{\leq} \sum_{i \in I_h(\mathbf{x}) \cap \mathcal{B}} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) |\phi'(Y_i - a(\mathbf{x})) - \phi'(\eta(\mathbf{X}_i) + W_i - a(\mathbf{x}))| \\ &\stackrel{(b)}{\leq} 2 \sum_{i \in I_h(\mathbf{x}) \cap \mathcal{B}} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) (T + Z) \\ &\stackrel{(c)}{\leq} 2(T + Z) C_K q_h(\mathbf{x}). \end{aligned} \quad (87)$$

177 For (a), recall that $Y_i \neq \eta(\mathbf{X}_i) + W_i$ only for attacked sample. For (b), recall (10), we have

$$\min_{j \in I_h(\mathbf{x})} \eta(\mathbf{X}_j) + W_j \leq a(\mathbf{x}) \leq \max_{j \in I_h(\mathbf{x})} \eta(\mathbf{X}_j) + W_j, \quad (88)$$

178 therefore $|\eta(\mathbf{x}) + W_i - a| \leq Z, \forall i \in I_h(\mathbf{x})$. Recall that

$$\phi'(u) = \begin{cases} 2u & \text{if } |u| \leq T \\ 2T & \text{if } u > T \\ -2T & \text{if } u < -T, \end{cases} \quad (89)$$

179 thus $|\phi'(\eta(\mathbf{X}_i) + W_i - a(\mathbf{x}))| \leq 2Z$. (c) just uses Assumption 2.

180 Moreover, if $\delta \leq T - Z$,

$$\begin{aligned}
& \sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) [\phi'(Y_i - a(\mathbf{x})) - \phi'(Y_i - (a(\mathbf{x}) + \delta))] \\
& \geq 2\delta \sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) \mathbf{1}(|Y_i - a(\mathbf{x})| < T, |Y_i - (a(\mathbf{x}) + \delta)| < T) \\
& \geq 2\delta c_K |I_h(\mathbf{x}) \setminus B| \\
& \geq 2\delta c_K (n_h(\mathbf{x}) - q_h(\mathbf{x})). \tag{90}
\end{aligned}$$

181 Similarly,

$$\sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) [\phi'(Y_i - (a(\mathbf{x}) - \delta)) - \phi'(Y_i - a(\mathbf{x}))] \geq 2\delta c_K (n_h(\mathbf{x}) - q_h(\mathbf{x})). \tag{91}$$

182 Let $\delta = (T + Z)r(\mathbf{x})$, with condition $r(\mathbf{x}) \leq (T - Z)/(T + Z)$, $\delta \leq T - Z$, thus (90) and (91)
183 hold. From (87), (90) and (91),

$$\sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) \phi'(Y_i - (a(\mathbf{x}) + \delta)) \leq 0 \leq \sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) \phi'(Y_i - (a(\mathbf{x}) - \delta)). \tag{92}$$

184 Therefore $\hat{\eta}_0(\mathbf{x}) \in [a - \delta, a + \delta]$.

185 Now it remains to discuss the case when (86) is violated, which indicates that the minimum in (10) is
186 not reached in $[-M, M]$. Then $a(\mathbf{x}) = M$ or $a(\mathbf{x}) = -M$. If $a(\mathbf{x}) = M$,

$$\sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) \phi'(\eta(\mathbf{X}_i) + W_i - a(\mathbf{x})) > 0, \tag{93}$$

187 then go through (87),

$$\left| \sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) \phi'(Y_i - a(\mathbf{x})) \right| > -2(T + Z)C_K q_h(\mathbf{x}). \tag{94}$$

188 With (91) and $\delta = (T + Z)r(\mathbf{x})$,

$$\left| \sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) \phi'(Y_i - (a(\mathbf{x}) - \delta)) \right| > 0. \tag{95}$$

189 Therefore $\hat{\eta}_0(\mathbf{x}) \geq a(\mathbf{x}) - \delta$, and from (5), $\hat{\eta}_0(\mathbf{x}) \leq M$. Therefore $|\hat{\eta}_0(\mathbf{x}) - a(\mathbf{x})| \leq \delta$ still holds.
190 Similar argument holds for $a(\mathbf{x}) = -M$. The proof is complete.

191 7.3 Proof of Lemma 3

192 From Assumption 3, $T \geq 4Lh + 16\sigma \ln N$, thus by condition (b) in Lemma 3, $T \geq 2Z$, $(T -$
193 $Z)/(T + Z) \geq 1/3$, and

$$r(\mathbf{x}) = \frac{C_K q_h(\mathbf{x})}{c_K (n_h(\mathbf{x}) - q_h(\mathbf{x}))} \leq \frac{C_K \frac{c_K}{3C_K + c_K} n_0}{c_K \left(1 - \frac{c_K}{3C_K + c_K}\right) n_0} = \frac{1}{3} \leq \frac{T - Z}{T + Z}. \tag{96}$$

194 Therefore from Lemma 2,

$$\begin{aligned}
|\hat{\eta}_0(\mathbf{x}) - a(\mathbf{x})| & \leq (T + Z)r(\mathbf{x}) \\
& \leq T \left(1 + \frac{1 - r(\mathbf{x})}{1 + r(\mathbf{x})}\right) r(\mathbf{x}) \\
& = \frac{2T}{\frac{1}{r(\mathbf{x})} + 1} \\
& \leq \frac{2TC_K q_h(\mathbf{x})}{c_K n_h(\mathbf{x})} \\
& \leq \frac{2TC_K q_h(\mathbf{x})}{c_K n_0}. \tag{97}
\end{aligned}$$

195 **7.4 Proof of Lemma 5**

196 Define

$$p_h(\mathbf{x}) = \int_{\|\mathbf{u}-\mathbf{x}\|\leq h} f(\mathbf{u})d\mathbf{u} \quad (98)$$

197 as the probability mass of ball centering at \mathbf{x} with radius h .

198 **Lemma 12.** ([2], Lemma 3) with probability at least $1 - 1/N$, for all $\mathbf{x} \in \mathcal{X}$,

$$\left| p_h(\mathbf{x}) - \frac{n_h(\mathbf{x})}{N} \right| \leq \beta_N \sqrt{p_h(\mathbf{x})} + \beta_N^2, \quad (99)$$

199 in which $\beta_N = \sqrt{4(d+3)\ln(2N)/N}$.

200 Assumption 3 requires that $h \geq (\ln^2 N/N)^{1/d}$, hence for sufficiently large N ,

$$\frac{\beta_N}{\sqrt{p_h(\mathbf{x})}} \leq \frac{\beta_N}{\sqrt{f_m \alpha v_d h^d}} = \sqrt{\frac{4(d+3)\ln(2N)}{f_m \alpha v_d h^d N}} \leq \frac{1}{3}, \quad (100)$$

201 and $\beta_N^2/p_h(\mathbf{x}) \leq 1/9$. Therefore

$$\left| p_h(\mathbf{x}) - \frac{n_h(\mathbf{x})}{N} \right| \leq p_h(\mathbf{x}) \left(\frac{\beta_N}{\sqrt{p_h(\mathbf{x})}} + \frac{\beta_N^2}{p_h(\mathbf{x})} \right) \leq \frac{4}{9} p_h(\mathbf{x}), \quad (101)$$

202 which yields

$$n_h(\mathbf{x}) \geq \frac{5}{9} N p_h(\mathbf{x}) > \frac{1}{2} N f_m \alpha v_d h^d = \frac{1}{2} n_0. \quad (102)$$

203 For the upper bound, note that $p_h(\mathbf{x}) \leq f_M v_d h^d$,

$$n_h(\mathbf{x}) \leq \frac{13}{9} N p_h(\mathbf{x}) \leq \frac{3}{2} N f_M v_d h^d. \quad (103)$$

204 With probability at least $1 - 1/N$, (102) and (103) hold uniformly for all $\mathbf{x} \in \mathcal{X}$.

205 **7.5 Proof of Lemma 6**

206 For $i, j \in [N]$, let A_{ij} be a $d - 1$ dimensional hyperplane that perpendicularly bisects \mathbf{X}_i and \mathbf{X}_j .
 207 The number of planes is $N_p = N(N - 1)/2$. The number of regions divided by these planes can be
 208 bounded by

$$N_r = \sum_{j=0}^d \binom{N_p}{j} \leq d N_p^d \leq d N^{2d}. \quad (104)$$

209 For all \mathbf{x} within a specific region, its nearest neighbors should be the same. Hence

$$|\{\mathcal{N}_k(\mathbf{x}) | \mathbf{x} \in \mathcal{X}, k \in [N]\}| \leq d N^{2d+1}. \quad (105)$$

210 Similar formulation was used in [3], proof of Lemma 3.

211 For each $\mathcal{N}_k(\mathbf{x})$, from Assumption 1(d), conditional on positions of $\mathbf{X}_1, \dots, \mathbf{X}_N$

$$\mathbb{E} \left[\exp \left(\lambda \sum_{i \in \mathcal{N}_k(\mathbf{x})} W_i \right) \middle| \mathbf{X}^N \right] \leq e^{\frac{k}{2} \lambda^2 \sigma^2}, \forall \lambda \leq \frac{1}{\sigma}, \quad (106)$$

212 in which we use \mathbf{X}^N to substitute $\mathbf{X}_1, \dots, \mathbf{X}_N$ for brevity. Then the following Chernoff bound holds:

$$\begin{aligned} \mathbb{P} \left(\sum_{i \in \mathcal{N}_k(\mathbf{x})} W_i > t \middle| \mathbf{X}^N \right) &\leq \inf_{0 \leq \lambda \leq 1/\sigma} \exp \left(-\lambda t + \frac{k}{2} \lambda^2 \sigma^2 \right) \\ &\leq \begin{cases} e^{-\frac{t^2}{2k\sigma^2}} & \text{if } t \leq k\sigma \\ e^{-\frac{t}{2\sigma}} & \text{if } t > k\sigma. \end{cases} \end{aligned} \quad (107)$$

213 If $t \geq \ln^2 N$, let $t = \sqrt{k}\sigma \ln N$. Otherwise, let $t = \sigma \ln^2 N$. Then

$$\mathbf{P} \left(\sum_{i \in \mathcal{N}_k(\mathbf{x})} W_i > t | \mathbf{X}^N \right) \leq e^{-\frac{1}{2} \ln N}. \quad (108)$$

214 Combine with (105), the proof is complete.

215 7.6 Proof of Lemma 7

216 Recall that the statement of Theorem 2 requires that $K(\mathbf{u})$ monotonic decrease with $\|\mathbf{u}\|$. Define

$$r_j := \sup \{ \|u\| | K(\mathbf{u}) \geq c_K + j\Delta \}. \quad (109)$$

217 Cut K into m slices above c_K , whose heights are $\Delta = (C_K - c_K)/m$. Define the truncated kernel
218 as

$$K_T(\mathbf{u}) := \sum_{j=1}^m \Delta \mathbf{1}(\|\mathbf{u}\| \leq r_j) + c_K \mathbf{1}(\|\mathbf{u}\| \leq 1), \quad (110)$$

219 then $0 \leq K(\mathbf{u}) - K_T(\mathbf{u}) \leq \Delta$, under E ,

$$\left| \sum_{i=1}^N \left(K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) - K_T \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) \right) W_i \right| \leq \Delta \max_i |W_i| \leq 4\sigma \Delta \ln N, \quad (111)$$

220 and

$$\begin{aligned} \left| \sum_{i=1}^N K_T \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) W_i \right| &\leq \left| \sum_{i=1}^N c_K \mathbf{1}(\|\mathbf{x} - \mathbf{X}_i\| < h) W_i + \sum_{j=1}^m \sum_{i=1}^N \Delta \mathbf{1}(\|\mathbf{X}_i - \mathbf{x}\| \leq hr_j) W_i \right| \\ &\leq c_K \left| \sum_{i \in \mathcal{N}_{n_h}(\mathbf{x})} W_i \right| + \delta \sum_{j=1}^m \left| \sum_{i \in \mathcal{N}_{n_{hr_j}}(\mathbf{x})} W_i \right| \\ &\leq (c_K + m\Delta) \sqrt{n_M} \ln N \\ &= C_K \sqrt{n_M} \ln N. \end{aligned} \quad (112)$$

221 in which the last step uses Lemma 6. Since m can be arbitrarily large and Δ can be arbitrarily small,
222 from (111) and (112),

$$\left| \sum_{i=1}^N K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) W_i \right| \leq C_K \sqrt{n_M} \ln N. \quad (113)$$

223 The proof is complete.

224 7.7 Proof of Lemma 9

225 Denote $g_1 = F[\eta_1]$, $g_2 = F[\eta_2]$, $g = F[\eta]$. If $g_1 \leq g_2$ is not satisfied somewhere, then define

$$S = \{\mathbf{x} | g_1(\mathbf{x}) > g_2(\mathbf{x})\}. \quad (114)$$

226 Since $g_1 = F(\eta_1)$, due to the uniqueness of optimization solution (Proposition ??), $\|\eta_1 - g_1\| <$
227 $\|\eta_1 - g\|_1$ for all L -Lipschitz function g . Hence

$$\|\eta_1 - g_1\|_1 < \|\eta_1 - \min\{g_1, g_2\}\|_1, \quad (115)$$

228 thus

$$\int_S |\eta_1(\mathbf{x}) - g_1(\mathbf{x})| d\mathbf{x} < \int_S |\eta_1(\mathbf{x}) - g_2(\mathbf{x})| d\mathbf{x}. \quad (116)$$

229 In S , $g_2(\mathbf{x}) < g_1(\mathbf{x})$, since $\eta_2(\mathbf{x}) > \eta_1(\mathbf{x})$,

$$|\eta_2(\mathbf{x}) - g_2(\mathbf{x})| - |\eta_2(\mathbf{x}) - g_1(\mathbf{x})| \geq |\eta_1(\mathbf{x}) - g_2(\mathbf{x})| - |\eta_1(\mathbf{x}) - g_1(\mathbf{x})|. \quad (117)$$

230 Therefore

$$\int_S |\eta_2(\mathbf{x}) - g_1(\mathbf{x})| d\mathbf{x} < \int_S |\eta_2(\mathbf{x}) - g_2(\mathbf{x})| d\mathbf{x}, \quad (118)$$

231 which yields

$$\|\eta_2 - \min\{g_1, g_2\}\|_1 < \|\eta_2 - g_2\|, \quad (119)$$

232 contradict with that $g_2 = F[\eta_2]$ is the solution of the optimization problem (64). Therefore $g_1 \leq g_2$
233 everywhere.

234 7.8 Proof of Lemma 10

235 According to Assumption 1(d), which requires that W_i is sub-exponential with parameter σ , we have

$$\mathbb{E} \left[\exp \left[\lambda \sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) W_i \right] \middle| \mathbf{X}_1, \dots, \mathbf{X}_N \right] \leq \exp \left[\frac{1}{2} \lambda^2 C_K^2 \sigma^2 n_h(\mathbf{x}) \right], \forall |\lambda| \leq \frac{1}{C_K \sigma}, \quad (120)$$

236 and

$$\mathbb{P} \left(\sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) W_i > t \middle| \mathbf{X}_1, \dots, \mathbf{X}_N \right) \leq \inf_{|\lambda| \leq 1/(C_K \sigma)} e^{-\lambda t + \lambda^2 C_K^2 \sigma^2 n_h(\mathbf{x})} / 2. \quad (121)$$

237 Therefore for sufficiently large N , let $t = 2C_K \sigma \sqrt{n_h(\mathbf{x}) \ln N}$,

$$\mathbb{P} \left(\sum_{i \in I_h(\mathbf{x})} K \left(\frac{\mathbf{x} - \mathbf{X}_i}{h} \right) W_i > 2C_K \sigma \sqrt{n_h(\mathbf{x}) \ln N} \middle| \mathbf{X}_1, \dots, \mathbf{X}_N \right) \leq e^{-2 \ln N} = \frac{1}{N^2}. \quad (122)$$

238 The opposite side can be proved similarly. Recall that under E , $n_h(\mathbf{x}) \leq 3N f_M v_d h^d / 2$. The proof
239 is complete.

240 7.9 Proof of Lemma 11

241 η is Lipschitz, thus $\eta - \Delta$ is Lipschitz. Since $F[\eta_1]$ is the solution of optimization problem (64) with
242 η_1 , we have

$$\|\eta_1 - F[\eta_1]\|_1 \leq \|\eta_1 - (\eta - \Delta)\|_1. \quad (123)$$

243 Hence

$$\|F[\eta_1] - (\eta - \Delta)\|_1 \leq \|F[\eta_1] - \eta_1\|_1 + \|\eta_1 - (\eta - \Delta)\|_1 \leq 2\|\eta_1 - (\eta - \Delta)\|_1. \quad (124)$$

244 It remains to bound $\|\eta_1 - (\eta - \Delta)\|_1$:

$$\begin{aligned} \|\eta_1 - (\eta - \Delta)\|_1 &\leq \|Lh + 3C_k \sigma \sqrt{N f_M v_d h^d \ln N} - \Delta\|_1 \\ &\leq \frac{2TC_K}{c_k n_0} \int q_h(\mathbf{x}) d\mathbf{x} + 2M \int \mathbf{1} \left(q_h(\mathbf{x}) > \frac{c_K n_0}{3C_K + c_K} \right) d\mathbf{x} + 2M \int_S d\mathbf{x} \\ &\leq \frac{2TC_K q v_d h^d}{c_K n_0} + \frac{2M(3C_K + c_K) q v_d h^d}{c_K n_0} + 2M \int_S d\mathbf{x}. \end{aligned} \quad (125)$$

245 $\|\eta_2 - F[\eta_2]\|_1$ can be bounded in the same way. Therefore

$$\max \{ \|F[\eta_1] - (\eta - \Delta)\|_1, \|F[\eta_2] - (\eta + \Delta)\|_1 \} \leq (C_1 T + C_2) \frac{q h^d}{n_0} + 2M \int_S d\mathbf{x}, \quad (126)$$

246 in which $C_1 = 4C_K v_d / c_K$, $C_2 = 4M(3C_K + c_K) v_d / c_K$. We then show the following lemma.

247 **Lemma 13.** *If a function g is L_d -Lipschitz with bounded $\|g\|_1$, then*

$$\|g\|_2^2 \lesssim \left(\frac{(d+1)d^{\frac{d}{2}} L^d}{v_d} \right)^{\frac{1}{d+1}} \|g\|_1^{\frac{d+2}{d+1}}. \quad (127)$$

248 *Proof.* g is continuous with bounded $\|g\|_1$, thus it reaches its maximum at some \mathbf{x}_0 . Then

$$|g(\mathbf{x})| \geq \|g\|_\infty - L_d \|\mathbf{x} - \mathbf{x}_0\|, \forall \|\mathbf{x} - \mathbf{x}_0\| \leq \|g\|_\infty / L_d. \quad (128)$$

249 Denote s_d as the surface area of d -dimension unit ball, $s_d = dv_d$, then

$$\begin{aligned} \|g\|_1 &= \int |g(\mathbf{x})| d\mathbf{x} \\ &\geq \int_{\|\mathbf{x}-\mathbf{x}_0\| \leq \|g\|_\infty / L_d} (\|g\|_\infty - L_d \|\mathbf{x} - \mathbf{x}_0\|) d\mathbf{x} \\ &= \int_0^{\|g\|_\infty / L_d} (\|g\|_\infty - L_d r) s_d r^{d-1} dr \\ &= \frac{s_d}{d} \|g\|_\infty \left(\frac{\|g\|_\infty}{L_d} \right)^d - \frac{L_d s_d}{d+1} \left(\frac{\|g\|_\infty}{L_d} \right)^{d+1} \\ &= \frac{v_d}{(d+1)L_d^d} \|g\|_\infty^{d+1}. \end{aligned} \quad (129)$$

250 Hence

$$\|g\|_\infty \leq \left(\frac{(d+1)L_d^d}{v_d} \|g\|_1 \right)^{\frac{1}{d+1}}, \quad (130)$$

251

$$\|g\|_2^2 \leq \|g\|_1 \|g\|_\infty \leq \left(\frac{(d+1)L_d^d}{v_d} \right)^{\frac{1}{d+1}} \|g\|_1^{\frac{d+2}{d+1}}. \quad (131)$$

252

□

253 Moreover, in (64), the derivative of g is bounded by L in each dimension, hence $F[\eta]$ is $\sqrt{d}L$ -
254 Lipschitz. Let $L_d = \sqrt{d}L$. Since $\eta - \Delta$, $F[\eta_1]$ are both L_d -Lipschitz, $\eta - \Delta - F[\eta_1]$ is $2L_d$ -Lipschitz,
255 hence

$$\|F[\eta_1] - (\eta - \Delta)\|_2^2 \lesssim \left(\frac{Tqh^d}{n_0} \right)^{\frac{d+2}{d+1}} + \left(\int_S d\mathbf{x} \right)^{\frac{d+2}{d+1}}, \quad (132)$$

256 and

$$\begin{aligned} \|F[\eta_1] - \eta\|_2^2 &\leq 2\|F[\eta_1] - (\eta - \Delta)\|_2^2 + 2\Delta^2 \int_{\mathcal{X}} d\mathbf{x} \\ &\lesssim \left(\frac{Tqh^d}{n_0} \right)^{\frac{d+2}{d+1}} + \left(\int_S d\mathbf{x} \right)^{\frac{d+2}{d+1}} + h^2 + \frac{\ln N}{Nh^d}. \end{aligned} \quad (133)$$

257 From Lemma 10,

$$\mathbb{E} \left[\int_S d\mathbf{x} \right] = \int_{\mathcal{X}} \mathbf{P}(\mathbf{x} \in S) d\mathbf{x} \leq \int_{\mathcal{X}} \frac{2}{N^2} d\mathbf{x} \leq \frac{2}{f_m N^2}, \quad (134)$$

258

$$\mathbb{E} \left[\left(\int_S d\mathbf{x} \right)^{\frac{d+2}{d+1}} \right] \leq \mathbb{E} \left[\int_S d\mathbf{x} \right] \left(\int_{\mathcal{X}} d\mathbf{x} \right)^{\frac{1}{d+1}} \leq \frac{1}{f_m^{\frac{1}{d+1}}} \mathbb{E} \left[\int_S d\mathbf{x} \right] \lesssim \frac{1}{N^2}. \quad (135)$$

259 Therefore the second term in (133) decays faster than other terms, and

$$\begin{aligned} \|F[\eta_1] - \eta\|_2^2 &\leq 2\|F[\eta_1] - (\eta - \Delta)\|_2^2 + 2\Delta^2 \int_{\mathcal{X}} d\mathbf{x} \\ &\lesssim \left(\frac{Tqh^d}{n_0} \right)^{\frac{d+2}{d+1}} + h^2 + \frac{\ln N}{Nh^d}. \end{aligned} \quad (136)$$

260 The bound also holds for $\|F[\eta_2] - \eta\|_2^2$. Substitute n_0 in (136) with (18). The proof is complete.

261 **References**

- 262 [1] Luc P Devroye. The uniform convergence of the nadaraya-watson regression function estimate.
263 *Canadian Journal of Statistics*, 6(2):179–191, 1978.
- 264 [2] Heinrich Jiang. Uniform convergence rates for kernel density estimation. In *International*
265 *Conference on Machine Learning*, pages 1694–1703. PMLR, 2017.
- 266 [3] Heinrich Jiang. Non-asymptotic uniform rates of consistency for k-nn regression. In *Proceedings*
267 *of the AAAI Conference on Artificial Intelligence*, volume 33, pages 3999–4006, 2019.
- 268 [4] Adam Krzyzak. The rates of convergence of kernel regression estimates and classification rules.
269 *IEEE Transactions on Information Theory*, 32(5):668–679, 1986.
- 270 [5] Yue-pok Mack and Bernard W Silverman. Weak and strong uniform consistency of kernel
271 regression estimates. *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, 61:405–
272 415, 1982.
- 273 [6] Alexandre B Tsybakov. *Introduction to Nonparametric Estimation*. Springer Series in Statistics,
274 2009.