Necessary and Sufficient Watermark for Large Language Models

Anonymous ACL submission

⁰⁰¹ Abstract

 Large language models (LLMs) can now gener- ate texts that are indistinguishable from those written by humans. Such remarkable perfor- mance of LLMs increases their risk of being used for malicious purposes. Thus, it is nec- essary to develop methods for distinguishing texts written by LLMs from those written by humans. Watermarking is one of the most pow- erful methods for achieving this. Although existing methods have successfully detected texts generated by LLMs, they inevitably de- grade the text quality. In this study, we propose the Necessary and Sufficient Watermark (NS- Watermark) for inserting watermarks into gen-**erated texts with minimum text quality degra-**017 dation. More specifically, we derive minimum constraints required to be imposed on the gen- erated texts to distinguish whether LLMs or hu- mans write the texts, and we formulate the NS- Watermark as a constrained optimization prob- lem. Through the experiments, we demonstrate that the NS-Watermark can generate more nat- ural texts than existing watermarking methods and distinguish more accurately between texts written by LLMs and those written by humans. Especially in machine translation tasks, the NS- Watermark can outperform the existing water-marking method by up to 30 BLEU scores.

⁰³⁰ 1 Introduction

 Large language models (LLMs) have achieved re- markable performances in a wide range of NLP tasks, including language generation [\(Chen et al.,](#page-8-0) [2021\)](#page-8-0), question answering [\(Joshi et al.,](#page-8-1) [2017;](#page-8-1) [Kwiatkowski et al.,](#page-9-0) [2019\)](#page-9-0), and reasoning tasks [\(Bisk et al.,](#page-8-2) [2020;](#page-8-2) [Kojima et al.,](#page-8-3) [2022\)](#page-8-3). Recently, [m](#page-8-4)any pre-trained LLMs have been released [\(Brown](#page-8-4) [et al.,](#page-8-4) [2020;](#page-8-4) [Chung et al.,](#page-8-5) [2022;](#page-8-5) [Zhang et al.,](#page-9-1) [2022;](#page-9-1) [Touvron et al.,](#page-9-2) [2023\)](#page-9-2), which can now generate nat- ural and fluent texts that are indistinguishable from texts written by humans. For instance, [Brown et al.](#page-8-4) [\(2020\)](#page-8-4) evaluated the quality of the news articles

generated by GPT-3, demonstrating that humans **043** can hardly distinguish between news articles gener- **044** ated by GPT-3 and those written by humans. **045**

As the performance of LLMs improves for var- **046** ious tasks, the risk that LLMs are used for mali- **047** cious purposes, such as generating fake news, also **048** increases [\(Zellers et al.,](#page-9-3) [2019\)](#page-9-3). Thus, it is crucial **049** to develop methods to identify whether LLMs or **050** humans write texts. Watermarking is one of the **051** powerful techniques for this purpose, which inserts **052** information into texts such that the inserted infor- **053** mation is imperceptible to humans and can be eas- **054** ily identified by some algorithms [\(Venugopal et al.,](#page-9-4) **055** [2011;](#page-9-4) [He et al.,](#page-8-6) [2021,](#page-8-6) [2022;](#page-8-7) [Zhao et al.,](#page-9-5) [2023b;](#page-9-5) **056** [Kuditipudi et al.,](#page-8-8) [2023;](#page-8-8) [Zhao et al.,](#page-9-6) [2023a;](#page-9-6) [Kirchen-](#page-8-9) **057** [bauer et al.,](#page-8-9) [2023a](#page-8-9)[,b;](#page-8-10) [Christ et al.,](#page-8-11) [2023\)](#page-8-11). Recently, **058** [Kirchenbauer et al.](#page-8-9) [\(2023a\)](#page-8-9) proposed the Hard/Soft- **059** Watermark, which inserts watermarks by generat- **060** ing text using only a subset of vocabulary.^{[1](#page-0-0)} Texts 061 generated by the watermarked LLMs consist only **062** of a subset of vocabulary, whereas texts written by **063** humans consist of an entire vocabulary. Thus, we **064** can identify whether LLMs or humans write texts **065** [u](#page-8-9)sing statistical hypothesis testing. [Kirchenbauer](#page-8-9) **066** [et al.](#page-8-9) [\(2023a\)](#page-8-9) demonstrated that texts generated by **067** LLMs with the Hard/Soft-Watermark can be distin- **068** guished from human-written texts almost perfectly. **069** However, the generated texts are often low-quality **070** because LLMs generate texts with only a subset of **071** vocabulary. 072

In this study, we propose a novel method for **073** inserting watermarks into generated text without **074** sacrificing both text quality and detection accuracy, which we refer to as the Necessary and Suffi- **076** cient Watermark (NS-Watermark). Our method **077** is based on the observation that the constraint im- **078** posed by the Hard/Soft-Watermark is overly conser- **079** vative for identifying LLM-generated texts, espe- **080**

¹We coined the name "Hard/Soft-Watermark" to refer to the watermarking methods by [Kirchenbauer et al.](#page-8-9) [\(2023a\)](#page-8-9).

 cially when the generated texts are long. Hence, we derive minimum constraints required to be imposed on the generated texts to detect LLM-generated texts. We find that the constraints on the gener- ated text can be relaxed without decreasing the detection accuracy as the length of the generated text increases. Based on this observation, we pro- pose the NS-Watermark, which can change the con- straints according to the length and impose mini- mum constraints on the generated text. Owing to the minimum constraints, the text generated with the NS-Watermark can be more natural than the text with the Hard/Soft-Watermark. We experimentally evaluate the effectiveness of the NS-Watermark and demonstrate that the NS-Watermark can out- perform the Soft-Watermark in terms of both text quality and detection accuracy. Particularly in the machine translation tasks, we demonstrate that the NS-Watermark can outperform the Soft-Watermark by up to 30 BLEU scores and achieve competitive

¹⁰³ 2 Background

102 methods without watermarks.

 In this section, we briefly describe the water- marking methods proposed by [Kirchenbauer et al.](#page-8-9) [\(2023a\)](#page-8-9). Further discussions on related studies are deferred to Sec. [5.](#page-7-0)

101 BLEU scores compared to conventional decoding

Hard-Watermark. Let x_{prompt} be a prompt, V 109 be vocabulary, and $\gamma \in (0, 1)$ be a hyperparameter. 110 Given a word x_t , using x_t as the seed value, we randomly split V into two disjoint subsets: *green words* $V^{\text{green}}(x_t)$ and *red words* $V^{\text{red}}(x_t)(:= V \setminus$ $V^{\text{green}}(x_t)$) such that $|V^{\text{green}}(x_t)| = \gamma |V|$. Then, the Hard-Watermark generates text as follows:

115
$$
\arg \max_{x_{1:T}, T} p(x_{1:T} | x_{\text{prompt}})
$$
 (1)
116 **s.t.** $x_{t+1} \in V^{\text{green}}(x_t)$ $(t = 1, 2, \dots, T - 1)$.

 If humans write the text, the green words appear 118 with probability γ , whereas texts written by LLMs consist of only green words. Thus, we can use sta- tistical hypothesis testing to identify whether LLMs or humans write the text. Specifically, the null and alternative hypotheses are given as follows:

- 123 H_0 : The green words appear in a text with proba-124 **bility** γ .
- 125 H_1 : The green words appear in a text with a prob-**126** ability greater than γ.

When the null hypothesis is rejected, we conclude 127 that the text is generated by LLMs. The number **128** of green words follows a binomial distribution in **129** texts written by humans. Thus, we can test this by **130** checking whether the z-score of text $x_{1:T}$, defined 131 below, exceeds a given threshold Z. **132**

$$
z(x_{1:T}) \coloneqq \frac{|x_{1:T}|_G - \gamma(T-1)}{\sqrt{\gamma(1-\gamma)(T-1)}},\qquad(2)
$$

where $|x_{1:T}|_G := |\{x_{t+1} \mid x_{t+1} \in V^{\text{green}}(x_t)\}|.$ 134

Soft-Watermark. Although the Hard- **135** Watermark is a simple and efficient method **136** for distinguishing LLM-generated texts from **137** those written by humans, the generated texts **138** are often of low quality. This is partly because **139** the constraints of the Hard-Watermark may **140** prevent the generation of common phrases, e.g., **141** "Barack Obama," even if the probabilities of these **142** phrases are very high just because "Obama" is **143** not contained in V^{green} ("Barack"). To mitigate 144 this issue, [Kirchenbauer et al.](#page-8-9) [\(2023a\)](#page-8-9) also **145** proposed the Soft-Watermark: instead of making **146** all words contained in the generated text green **147** words, the Soft-Watermark adds an offset and **148** increases the probability of generating green **149** words. This relaxation allows the Soft-Watermark **150** to generate "Barack Obama" when the probability **151** that "Obama" appears after "Barack" is high, and **152** the Soft-Watermark can generate higher-quality **153** text than the Hard-Watermark. However, the **154** Soft-Watermark still suffers from low-quality text, **155** as we demonstrate in the experiments. **156**

3 Proposed Method **¹⁵⁷**

3.1 Necessary and Sufficient Watermark **158**

In this section, we show that the constraints of the **159** Hard/Soft-Watermark are too restrictive and derive **160** the minimum constraint to identify whether LLMs **161** or humans write the text. By rewriting Eq. [\(1\)](#page-1-0), the **162** Hard-Watermark is reformulated as follows: **163**

$$
\underset{x_{1:T},T}{\arg \max} p(x_{1:T} \mid x_{\text{prompt}}) \text{ s.t. } \frac{|x_{1:T}|_{G}}{T-1} = 1. (3)
$$

= 1. (3) **164**

Let $\hat{x}_{1:T}$ be the solution of Eq. [\(3\)](#page-1-1). The z-score 165 $z(\hat{x}_{1:T})$ is $\mathcal{O}(\sqrt{T})$, and we can identify whether 166 LLMs or humans write the text by testing whether **167** the z-score exceeds the hyperparameter Z. How- **168** ever, the z-score $z(\hat{x}_{1:T})$ increases with the length 169 of the generated text T, whereas the threshold Z **170** remains constant. Therefore, the above formula- **171** tion in Eq. [\(3\)](#page-1-1) imposes too restrictive constraint **172**

Figure 1: Visualization of the table $T[t][g]$ for $T_{\text{max}} = 200$, $\gamma = 0.2$, $\hat{T} = 75$, $\alpha = 2$, $Z = 4$, and $G_{\text{max}} = 63$. The areas colored in blue and light blue indicate the range in $T[t][q]$ where we need to calculate, and the areas colored in blue indicate the range that satisfies the constraint of Eq. [\(4\)](#page-2-0). The red line indicates the minimum number of green words required to satisfy the constraint. Note that in the middle and right figures, $T[t][G_{\text{max}}]$ does not denote the set of texts of length t containing G_{max} green words, but denotes the set of texts containing at least G_{max} green words.

173 on the generated text, especially when ensuring 174 $z(x_{1:T}) \geq Z$ for long texts.

175 Alternatively, the following constraint is suffi-**176** cient to ensure that the z-score of the generated text **177** is greater than or equal to the threshold Z:

178
\n
$$
\arg \max_{x_{1:T}, T} p(x_{1:T} | x_{\text{prompt}})
$$
\n
$$
\text{s.t. } \frac{|x_{1:T}|_{\text{G}}}{T-1} \ge \gamma + Z \sqrt{\frac{\gamma(1-\gamma)}{T-1}}. \tag{4}
$$

If text $x_{1:T}$ is written by humans, the proportion 181 of green words contained in a text $\frac{|x_{1:T}|_G}{T-1}$ is γ on average. Thus, the second term in the constraint is the minimum margin for identifying whether the texts are written by LLMs. We refer to the above problem as the Necessary and Sufficient Watermark (NS-Watermark). By comparing Eq. [\(3\)](#page-1-1) with Eq. [\(4\)](#page-2-0), the constraint of the NS- Watermark is looser than that in Eq. [\(3\)](#page-1-1), although the z-score of the generated text is guaranteed to be greater than or equal to Z because of the constraint in Eq. [\(4\)](#page-2-0). Thus, the NS-Watermark can gener- ate higher quality and more natural texts than the Hard/Soft-Watermark without decreasing detection accuracy. In the next section, we propose an effi-cient algorithm for computing the NS-Watermark.

196 3.2 Naive Algorithm for Necessary and **197** Sufficient Watermark

 The Hard/Soft-Watermark can be computed using the conventional beam search because the Hard- Watermark generates texts using only green words, and the Soft-Watermark just adds an offset to the probability that green words appear. However, the

NS-Watermark needs to control the proportion of **203** green words contained in generated texts and needs **204** to optimize where green words should be inserted. **205** Moreover, the constraint in Eq. [\(4\)](#page-2-0) depends on the **206** length of the generated text T , which is unknown 207 until the text is generated. This makes solving the **208** NS-Watermark more challenging, which hinders **209** the application of the conventional beam search to **210** the NS-Watermark. In this section, we propose an **211** algorithm to solve the NS-Watermark. **212**

Let k be the beam size. Let $T[t][g]$ be a set of 213 k texts of length t containing g green words. For **214** simplicity, we explain the cases in which $1 \leq g$ 215 and $1 \leq t$. Texts of length $t + 1$ containing g green 216 words can be generated by adding a green word to **217** texts of length t containing $q - 1$ green words or **218** adding a red word to texts of length t containing g 219 green words. Formally, we generate text of length **220** $t + 1$ containing g green words as follows:

$$
T[t+1][g] = \underset{x_{1:t+1} \in X_1 \cup X_2}{\arg \text{top-k}} p(x_{1:t+1} | x_{\text{prompt}}).
$$

By calculating $T[t][q]$ for all q and t and generating 226 the text with the highest probability among the texts **227** that satisfy the constraint in Eq. [\(4\)](#page-2-0), we can solve **228** Eq. [\(4\)](#page-2-0). **229**

Let T_{max} a hyperparameter that controls the max-
230 imum length of generated texts. We need to fill **231** the table $T[t][g]$ for all $(t,g) \in \{(t,g) \in \mathbb{Z}^2\}$ $1 \le t \le T_{\text{max}}$, $0 \le g \le t - 1$, which requires 233 the time complexity $\mathcal{O}(kT_{\text{max}}^2)$ (see the left figure 234 in Fig. [1a\)](#page-2-1). However, if $G_{\text{max}} := \lceil \gamma (T_{\text{max}} - 1) + 235 \rceil$

| **232**

 $Z\sqrt{\gamma(1-\gamma)(T_{\text{max}}-1)}$) green words appear af- ter generating t words, it is not necessary to count the number of green words that appear in the re- maining text because the constraint in Eq. [\(4\)](#page-2-0) is satisfied regardless of the remaining text. Based on this observation, we can reduce the time complex-242 ity by changing $T[t][G_{\text{max}}]$ to store texts of length t containing *at least* Gmax green words, instead of texts containing exactly Gmax green words. Owing to this modification, we do not need to count the number of green words after Gmax green words ap- pear in texts and can reduce the time complexity **b** to $\mathcal{O}(\gamma k T_{\text{max}}^2)$. We provide a visual explanation in the figure on the right side of Fig. [1a](#page-2-1) and show the pseudo-code in Alg. [1.](#page-4-0)

251 3.3 Linear Time Algorithm for Necessary and **252** Sufficient Watermark

 Algorithm [1](#page-4-0) in the previous section has the time **complexity of** $\mathcal{O}(\gamma k T_{\text{max}}^2)$ **, which is practically not** suitable for LLMs with an extremely large number of parameters. We resort to an approximation and reduce the time complexity to linear.

 The major bottleneck of the quadratic time com- plexity in Tmax is that Alg. [1](#page-4-0) requires us to fill the **entire table T**[t][g] for all $(t, g) \in \{(t, g) \mid 1 \leq$ $t \leq T_{\text{max}}$, $0 \leq g \leq \min\{t-1, G_{\text{max}}\}\$. This al- lows generated texts to contain many green words *locally* because the constraint in Eq. [\(4\)](#page-2-0) only re- stricts the green words to appear above a certain number in generated texts. To reduce this computa- tion, we additionally impose a constraint such that the green words appear *periodically* in generated texts. Technically, it is challenging because the pro- portion of green words appearing in the generated 270 text depends on its length T as in Eq. [\(4\)](#page-2-0), which is unknown a priori. For instance, a generated text is typically short for a closed-ended question, and the proportion of green words needs to be large. By contrast, generated texts tend to be long for news articles, and the proportion of green words can be reduced. Thus, to make green words appear period- ically in the generated text, we need to estimate the length of the generated text before generating it.

 To estimate the text length, we leverage the ob- servation that the length of generated texts remains almost the same regardless of watermarks because the text length is generally determined by the con- tent of the generated texts, i.e., the prompt. Inspired by this observation, we propose generating the texts without watermarks using the conventional beam 286 search, obtaining the length of generated text \overline{T} ,

and generating text with watermarks by solving the **287** following problem: **288**

$$
\underset{x_{1:T},T}{\arg\max} p(x_{1:T} \mid x_{\text{prompt}}) \tag{5}
$$

$$
\text{s.t. } \frac{|x_{1:T}| \mathbf{G}}{T-1} \ge \gamma + Z \sqrt{\frac{\gamma(1-\gamma)}{T-1}},\tag{290}
$$

$$
\left| \frac{|x_{1:t}|}{t-1} - \min\left\{1, \gamma + Z\sqrt{\frac{\gamma(1-\gamma)}{\widehat{T}-1}}\right\} \right| \le \frac{\alpha}{t-1}
$$

$$
\text{or } |x_{1:t-1}|_{G} \ge G_{\text{max}} \quad (t = 2, \cdots, T), \tag{292}
$$

where $\alpha \geq 1$ denotes a hyperparameter that controls the approximation rate. Intuitively, the second **294** inequality makes green words appear periodically **295** and the last inequality verifies whether G_{max} green 296 words appear before the first $t - 1$ words. As ex-
297 plained in the previous section, if Gmax green words **²⁹⁸** appear after generating $t - 1$ words, the number **299** of green words added in the remaining texts needs **300** not be counted anymore. Thus, we only need to **301** impose the last inequality on the generated text un- **302** til G_{max} green words appear. We show the visual 303 explanation in Fig. [1b.](#page-2-1) Owing to this additional **304** constraint, we do not need to fill the table $T[t][g]$ 305 for all $(t, g) \in \{(t, g) \in \mathbb{N}^2 \mid 1 \le t \le T_{\max}, 0 \le$ 306 $g \le \min\{t-1, G_{\max}\}\}.$ We only need to fill the 307 table $T[t][g]$ for (t, g) that satisfies the conditions 308 in Eq. [5](#page-3-0) (i.e., the colored area in Fig. [1b\)](#page-2-1). Sub- **309** sequently, the time complexity can be reduced to **310** $\mathcal{O}(\alpha kT_{\text{max}})$. We show the pseudo-code in Sec. [E.](#page-14-1) 311

3.4 Robustness to Post-editing Attack **312**

In the previous sections, we proposed the water- **313** marking methods that impose the minimum con- **314** straint to detect LLM-generated texts. However, **315** due to the minimality of the constraint, the NS- **316** Watermark can be removed from the generated **317** texts by replacing only one green word with a red **318** word. To make the watermarks robust against such **319** editing, we can tighten the constraint as follows: **320**

$$
\underset{x_1; T, T}{\arg \max} p(x_1; T \mid x_{\text{prompt}}) \tag{6}
$$

s.t.
$$
\frac{|x_{1:T}|_{\mathcal{G}}}{T-1} \ge \gamma + \beta + Z\sqrt{\frac{\gamma(1-\gamma)}{T-1}},
$$

where $\beta \ge 0$ is a hyperparameter that controls the 323 robustness. Owing to the constraint in Eq. [\(6\)](#page-3-1), the **324** z-score of the generated texts exceeds Z even if **325** $\beta(T-1)$ green words are replaced with red words, 326 and we can identify them as the texts generated **327** by LLMs. Moreover, the constraint in Eq. [\(6\)](#page-3-1) is **328**

s.t.

Algorithm 1: Naive algorithm for the NS-Watermark.

Input: Maximum number of words T_{max} , vocabulary V, beam size k, and hyperparameter γ , Z.

1 $G_{\text{max}} \leftarrow \lceil \gamma (T_{\text{max}} - 1) + Z \sqrt{\gamma (1 - \gamma) (T_{\text{max}} - 1)} \rceil.$

2 Let T be a $T_{\text{max}} \times (G_{\text{max}} + 1)$ table and S be an empty set.

³ Function *update(*X*: feasible set,* t*: the number of words* g*: the number of green words)* is

4 | $T[t][q] \leftarrow \emptyset$. 5 while $|T[t][g]| < k$ do $\begin{array}{c|c} \text{\bf{6}} & x_{1:t} = \arg\max_{x_{1:t}\in X\setminus \boldsymbol{T}[t][g]} p(x_{1:t} \mid x_{\text{prompt}}). \end{array}$ σ **if** the last word x_t is EOS **then** 8 if $g \geq \gamma(t-1) + Z\sqrt{\gamma(1-\gamma)(t-1)}$ then 9 | | | $S \leftarrow S \cup \{x_{1:t}\}.$ 10 else 11 \vert \vert \vert $T[t][g] \leftarrow T[t][g] \cup \{x_{1:t}\}.$

¹² Function *feasible_set(*t*: the number of words,* g*: the number of green words)* is

 if $g = 0$ then $\Big| \quad | \quad X \leftarrow \{x_{1:t} \mid x_{1:t-1} \in T[t-1][g], x_t \in V^{\text{red}}(x_{t-1})\}.$ 15 else if $q = t - 1$ then $\Big| \quad | \quad X \leftarrow \{x_{1:t} \mid x_{1:t-1} \in T[t-1][g-1], x_t \in V^{\text{green}}(x_{t-1})\}.$ **else if** $1 \leq g < G_{max}$ then $\Big| \quad | \quad X \leftarrow \{x_{1:t} \mid x_{1:t-1} \in T[t-1][g-1], x_t \in V^{\text{green}}(x_{t-1})\}.$ $\Big| \quad | \quad X \leftarrow X \cup \{x_{1:t} \mid x_{1:t-1} \in T[t-1][g], x_t \in V^{\text{red}}(x_{t-1})\}.$ **else if** $g = G_{max}$ then $\Big|$ $X \leftarrow \{x_{1:t} \mid x_{1:t-1} \in T[t-1][g-1], x_t \in V^{\text{green}}(x_{t-1})\}.$ $\begin{array}{ll} \textbf{22} & | & | & X \leftarrow X \cup \{x_{1:t} \mid x_{1:t-1} \in \boldsymbol{T}[t-1][g], x_t \in V\}. \end{array}$ 23 **return** X $T[1][0] \leftarrow \arg \text{top-}k_{x_1 \in V} p(x_1 | x_{\text{prompt}}).$ 25 for $t = 2, \cdots, T_{max}$ do **for** $q = 0, \dots, \min\{t-1, G_{max}\}\)$ do $27 \mid X \leftarrow feasible_set(t, g).$ \vert *update* (X, t, q) . 29 return $\arg\max_{x_{1:t}\in S\cup T[T_{max}][G_{max}]} p(x_{1:t} \mid x_{prompt}).$

 also the minimum constraint required to be im- posed on the generated texts such that the z-score exceeds Z after 50β% words are replaced. In Sec. [4.4,](#page-6-0) we experimentally evaluate the trade- off between text quality and robustness against the post-editing attack, demonstrating that the NS- Watermark can achieve the better trade-off than the Soft-Watermark.

³³⁷ 4 Experiments

338 4.1 Comparison Methods

 In the following sections, we evaluate the following [t](#page-8-9)hree methods: (1) The Soft-Watermark [\(Kirchen-](#page-8-9) [bauer et al.,](#page-8-9) [2023a\)](#page-8-9), which generates texts such that almost all words contained in the texts be-come green words by increasing the probability that

green words appear. A hyperparameter $\delta > 0$ is a 344 positive offset for the probability that green words **345** appear. When δ is set to a larger value, more green 346 words appear in the generated texts. (2) The NS- **347** Watermark, which generates texts containing the **348** minimum number of green words to detect LLM- **349** generated texts, unlike the Soft-Watermark. (3) The **350** Adaptive Soft-Watermark, a simple extension of **351** the Soft-Watermark. The original Soft-Watermark **352** uses the same hyperparameter δ for all texts, and 353 the proportion of green words contained in a gener- **354** ated text is almost constant regardless of text length. **355** Thus, the probability offset δ used by the Soft- 356 Watermark increases the number of green words **357** more than necessary to detect LLM-generated texts, **358** especially for long texts. We improve the Soft- **359**

Figure 2: Relationships between z-score and the length of generated texts. We used the validation datasets of WMT'16 En→De. For each γ , we tuned the hyperparameter δ of the Soft-Watermark by increasing 4, 6, 8, \cdots and selecting the smallest value such that the FNR becomes less than 5%. We omit the results of the Soft-Watermark and Adaptive Soft-Watermark for $\gamma = 0.0001$ because the z-scores become too large. Full results are deferred to Sec. [D.3.](#page-12-0)

Table 1: BLEU scores and detection accuracy with NLLB-200-3.3B and WMT. For the NS-Watermark, we set α to one and β to zero. The best values among the watermarking methods are highlighted in bold.

	$En \rightarrow De$		$De \rightarrow En$	
	BLEU ↑	$FNR \downarrow$ / $FPR \downarrow$	BLEU \uparrow	FNR \downarrow / FPR \downarrow
w/o Watermark	36.4	n.a.	42.6	n.a.
Soft-Watermark	5.2	3.0% / 0.4%	7.5	3.3% / 0.5%
Adaptive Soft-Watermark	20.5	0.0 % / 2.6%	20.6	0.0 % / 1.9%
NS-Watermark	32.7	0.0% / 0.3 $\%$	38.2	0.0% / 0.0 $\%$
	$En \rightarrow Fr$		$Fr \rightarrow En$	
	BLEU \uparrow	$FNR \downarrow$ / $FPR \downarrow$	BLEU \uparrow	FNR \downarrow / FPR \downarrow
w/o Watermark	42.6	n.a.	40.8	n.a.
Soft-Watermark	9.6	5.4% / 0.3 $\%$	7.6	3.6% / 0.6%
Adaptive Soft-Watermark	23.3	0.0 % / 2.2%	19.5	0.0 % / 2.8%
NS-Watermark	38.8	0.0% / 0.3 $\%$	36.8	0.0% / 0.1 %

Watermark such that δ **is tuned for each text, which** we refer to as the *Adaptive Soft-Watermark*. Specif- ically, the Adaptive Soft-Watermark finds δ by bi-**nary search and uses** δ **such that the z-score is min-** imum and exceeds the threshold Z. We present the pseudo-code in Sec. [E.](#page-14-1)

366 4.2 Machine Translation

 Experimental Setting. We evaluate the effective- ness of the NS-Watermark on machine translation tasks. We used NLLB-200-3.3B model [\(Team et al.,](#page-9-7) [2022\)](#page-9-7) with the test dataset of WMT'14 French (Fr) \leftrightarrow English (En) and WMT'16 German (De) \leftrightarrow [E](#page-8-9)nglish (En). Following the prior work [\(Kirchen-](#page-8-9) [bauer et al.,](#page-8-9) [2023a\)](#page-8-9), we set the hyperparameter Z to 4. For other hyperparameters, we split the data into the validation and test datasets with 10/90 ra- tio and used the validation dataset to tune. For the NS-Watermark, we selected γ with the best BLEU score [\(Papineni et al.,](#page-9-8) [2002\)](#page-9-8) on the vali-dation dataset using a grid search. The z-score

of texts generated by the NS-Watermark is guar- **380** anteed to be greater than or equal to Z, and the **381** FNR of the NS-Watermark becomes exactly 0% **382** for any hyperparameters. By contrast, the z-score **383** of text generated by the Soft-Watermark and Adap- **384** tive Soft-Watermark is not guaranteed to be greater **385** than or equal to Z . Thus, to fairly compare the NS- 386 Watermark with the Soft-Watermark and Adaptive **387** Soft-Watermark, we selected the hyperparameters **388** of these methods with the best BLEU score while **389** achieving more than 95% FNR in the validation **390** dataset using a grid search. See Sec. [C](#page-11-0) for more **391** detailed hyperparameter settings. **392**

Results.[2](#page-5-0) Table [1](#page-5-1) shows that the NS-Watermark **³⁹³** outperforms the Soft-Watermark and Adaptive Soft- **394** Watermark in terms of both text quality and detec- **395** tion accuracy. For all datasets, the Soft-Watermark **396** significantly degraded the BLEU scores. The **397** Adaptive Soft-Watermark improved the BLEU **398** scores by tuning δ for each text, although it still \qquad 399 achieved lower BLEU scores than the generated **400** texts without watermarks. By contrast, the NS- **401** Watermark outperformed the Soft-Watermark by **402** approximately 30 BLEU scores and achieved com- **403** petitive BLEU scores with the conventional beam **404** search without watermarks. Moreover, the NS- **405** Watermark can achieve 100.0% TPR because the 406 NS-Watermark is guaranteed to insert a sufficient **407** number of green words into the generated texts. 408

Analysis of z-score and Length of Texts. Fig- **409** ure [2](#page-5-2) shows the z-scores and length of generated **410** texts. We also plot the relationship between the **411**

²Note that [Kirchenbauer et al.](#page-8-9) [\(2023a\)](#page-8-9) evaluated text quality and detection accuracy with only texts consisting of approximately 200 words, while we evaluated them with all generated texts, which contain both short and long texts.

Figure 3: Text quality when varying α . We used the validation dataset of WMT'16 En→De.

 number of green words and the text length in Sec. [D.3.](#page-12-0) In the Soft-Watermark, the z-score in- creased as generated texts became longer. As dis- cussed in Sec. [3.3,](#page-3-2) the proportion of green words can be reduced as the length of generated texts increases. However, the Soft-Watermark cannot change the proportion of green words adaptively to the text length, resulting in generating texts with unnecessarily many green words for long texts. The Adaptive Soft-Watermark mitigates this prob- lem by tuning δ for each text, although its z-score still increases as the length increases. By contrast, the NS-Watermark can change the proportion of green words adaptively to the length, and the z- score does not increase even if the text length in- creases. Thus, the NS-Watermark imposes the min- imum constraint to make the z-score of generated 429 texts exceed the threshold $Z(= 4)$ and can gener- ate more natural and higher-quality texts than the Soft-Watermark and Adaptive Soft-Watermark.

 Analysis of Approximation Rate α . In the above experiments, we demonstrated that the NS- Watermark outperforms the Soft-Watermark and Adaptive Soft-Watermark when α is set to one. As we explained in Sec. [3.3,](#page-3-2) the text quality can be improved using the larger α . In this section, we [3](#page-6-1)8 **analyze the sensitivity of** α **on text quality. Figure 3** shows the results when varying α . The results indi-440 cate that when γ is large, the BLEU scores increase with α , but when γ is small, the BLEU scores are almost the same. This is because more green words need to be contained in the generated texts when γ is large. Therefore, the larger γ , the greater the influence of the approximation, and we need to **use large** α **to generate high-quality texts. Fortu-** nately, because the NS-Watermark achieved the best BLEU score when γ was small, we can use the small α without degrading text quality much in practice. In Sec. [D.1,](#page-12-1) the running time is presented when α is varied.

Table 2: Text quality and detection accuracy with LLaMA-7B and C4 dataset. For the NS-Watermark, we set $(\alpha, \beta) = (1, 0)$. The best values among the watermarking methods are shown in bold.

	$PPL \perp$	FNR \downarrow / FPR \downarrow
w/o Watermark	1.85	n.a.
Soft-Watermark	6.25	2.8% / 0.1 %
Adaptive Soft-Watermark	2.48	0.2% / 0.8%
NS-Watermark	1.92	0.0 % / 0.3%

4.3 Natural Language Generation **452**

Experimental Setting. Next, we compare the NS- **453** Watermark and the Soft-Watermark in terms of **454** [p](#page-9-2)erplexity (PPL). We used LLaMA-7B model [\(Tou-](#page-9-2) **455** [vron et al.,](#page-9-2) [2023\)](#page-9-2) with the subsets of C4, realnews- **456** like dataset [\(Raffel et al.,](#page-9-9) [2020\)](#page-9-9). Based on the prior **457** work [\(Kirchenbauer et al.,](#page-8-9) [2023a\)](#page-8-9), we split each **458** text and used the first 90% of words as the prompt **459** to infer the remaining 10% of words using LLMs. **460** We regarded the last 10% of words contained in 461 the data as the text written by humans and com- **462** pared the NS-Watermark with the Soft-Watermark **463** and Adaptive Soft-Watermark in terms of PPL and **464** detection accuracy. Then, we set the hyperparame- **465** ter Z to 4. To tune hyperparameters, we split the 466 dataset into validation and test datasets with $10/90$ 467 ratio. As in the previous section, we selected the hy- **468** perparameters of the Soft-Watermark and Adaptive **469** Soft-Watermark with the best PPL while achiev- **470** ing more than 95% FNR in the validation dataset **471** using a grid search. See Sec. [C](#page-11-0) for more detailed **472** hyperparameter settings. **473**

Results. The results are listed in Table [2.](#page-6-2) The **474** results were consistent with those presented in **475** Sec. [4.2.](#page-5-3) The NS-Watermark can outperform the **476** Soft-Watermark and Adaptive Soft-Watermark in **477** terms of text quality and detection accuracy. **478**

4.4 Robustness to Post-editing Attack **479**

In this section, we analyze the trade-off between **480** text quality degradation and robustness to post- **481** editing, demonstrating that the NS-Watermark can **482** achieve a better trade-off than the Soft-Watermark. **483**

Experimental Setting. To simulate the post- **484** editing attack, we randomly select $\epsilon\%$ words in 485 the generated texts and replace them with ran- **486** dom words. We then analyzed how much FNR **487** increases after the editing. We used LLaMA-7B **488** model and the validation dataset of C4. For the NS- **489** Watermark, we showed the results when varying **490** $\beta \in \{0, 0.05, 0.1, 0.2\}$. For other hyperparameters, 491 we used the values shown in Sec. [C.](#page-11-0) 492

Figure 4: Trade-off between text quality and robustness against post-editing. To make the figure more readable, the results with FNR greater than 25% were omitted. Surprisingly, the NS-Watermark is generally more robust against the post-editing than the Soft-Watermark even with a small offset $\beta = 0.05$.

 Results. Figure [4](#page-7-1) shows the relationship be- tween text quality and robustness against post- editing of the NS-Watermark and Soft-Watermark with various hyperparameters. By comparing the results of the NS-Watermark and Soft-Watermark with the same level of PPL, we observe that the NS- Watermark achieved a smaller FNR than the Soft- Watermark. Thus, the NS-Watermark can achieve a better trade-off between text quality and robust- ness than the Soft-Watermark. In Sec. [D.2,](#page-12-2) we also compared the NS-Watermark with the Adap- tive Soft-Watermark and demonstrated that the NS- Watermark can achieve a better trade-off than the Adaptive Soft-Watermark.

⁵⁰⁷ 5 Related Work

 Watermarking Methods. Watermarking methods detect LLM-generated texts by inserting impercep- tible information into generated texts. Watermark- ing methods have been extensively studied for im- ages and audio [\(Luo et al.,](#page-9-10) [2020;](#page-9-10) [Liu et al.,](#page-9-11) [2023\)](#page-9-11). However, due to the discrete structure of language, watermarking methods for natural language have been more challenging than those for images and audio. Recently, [Kirchenbauer et al.](#page-8-9) [\(2023a\)](#page-8-9) pro- posed the first practical watermarking method for LLMs. [Kuditipudi et al.](#page-8-8) [\(2023\)](#page-8-8) have extended it and proposed methods that are robust against post- editing, and [Christ et al.](#page-8-11) [\(2023\)](#page-8-11) proposed unde- tectable methods. These methods skew the distri- butions of generated texts (e.g., the ratio of green and red words) and detect LLM-generated texts us- ing statistical hypothesis testing. One advantage of watermarking methods is their high detection accu- racy. Furthermore, thanks to statistical hypothesis testing, the FPR can be explicitly adjusted by the

hyperparameter. However, because watermarking **528** methods need to modify generated texts, generated **529** texts are often of low quality. Our experiments in- **530** dicated that the existing methods underestimated **531** text quality degradation caused by watermarking, **532** and the NS-Watermark differs from them in that it **533** aims to minimize text-quality degradation. **534**

Post-hoc Detection Methods. As an alternative **535** approach, post-hoc detection methods have been **536** proposed [\(Zellers et al.,](#page-9-3) [2019;](#page-9-3) [Gehrmann et al.,](#page-8-12) **537** [2019;](#page-8-12) [Tian and Cui,](#page-9-12) [2023;](#page-9-12) [Mitchell et al.,](#page-9-13) [2023\)](#page-9-13). **538** [Zellers et al.](#page-9-3) [\(2019\)](#page-9-3) and [Tian and Cui](#page-9-12) [\(2023\)](#page-9-12) pro- **539** posed training additional models to detect LLM- **540** generated texts. [Mitchell et al.](#page-9-13) [\(2023\)](#page-9-13) also found **541** that LLM-generated texts tend to be texts at which **542** the curvature of the LLMs' log-likelihood becomes **543** negative and demonstrated that those can be identi- **544** fied without training additional models. These post- **545** hoc methods do not degrade text quality because **546** they do not modify generated texts. However, post- **547** hoc methods are inferior to watermarking methods **548** in detection accuracy [\(Krishna et al.,](#page-8-13) [2023\)](#page-8-13). **549**

6 Conclusion **⁵⁵⁰**

In this study, we proposed the NS-Watermark for **551** inserting watermarks into generated texts with min- **552** imum text quality degradation. Specifically, we **553** proposed the NS-Watermark that imposes the mini- **554** mum constraint required to detect LLM-generated **555** texts on generated texts. We conducted the ex- **556** periments on various tasks, showing that the NS- **557** Watermark can achieve 0% false negative rate with **558** negligible text quality degradation. Furthermore, **559** the experimental results demonstrated that the NS- **560** Watermark improves the quality-detectability trade- **561** off for post-editing attacks. **562**

⁵⁶³ 7 Limitations

 The NS-Watermark can minimize text quality degradation, while it increases the time complexity. We proposed the approximation methods to allevi- ate this issue, but its time complexity is still higher than that of the Soft-Watermark. Reducing the time complexity of the NS-Watermark is one of the promising research directions. Besides the meth- ods that minimize text quality degradation, several papers studied undetectable watermarking methods [\(Hu et al.,](#page-8-14) [2024;](#page-8-14) [Christ et al.,](#page-8-11) [2023\)](#page-8-11). It is also a very promising research direction to study undetectable watermarking methods with minimum text quality degradation by extending our work.

⁵⁷⁷ References

- **578** Yonatan Bisk, Rowan Zellers, Ronan Le Bras, Jianfeng **579** Gao, and Yejin Choi. 2020. PIQA: reasoning about **580** physical commonsense in natural language. In *AAAI* **581** *Conference on Artificial Intelligence*.
- **582** Tom Brown, Benjamin Mann, Nick Ryder, Melanie **583** Subbiah, Jared D Kaplan, Prafulla Dhariwal, Arvind **584** Neelakantan, Pranav Shyam, Girish Sastry, Amanda **585** Askell, Sandhini Agarwal, Ariel Herbert-Voss, **586** Gretchen Krueger, Tom Henighan, Rewon Child, **587** Aditya Ramesh, Daniel Ziegler, Jeffrey Wu, Clemens **588** Winter, Chris Hesse, Mark Chen, Eric Sigler, Ma-**589** teusz Litwin, Scott Gray, Benjamin Chess, Jack **590** Clark, Christopher Berner, Sam McCandlish, Alec **591** Radford, Ilya Sutskever, and Dario Amodei. 2020. **592** Language models are few-shot learners. In *Advances* **593** *in Neural Information Processing Systems*.
- **594** Mark Chen, Jerry Tworek, Heewoo Jun, Qiming **595** Yuan, Henrique Ponde, Jared Kaplan, Harrison Ed-**596** wards, Yura Burda, Nicholas Joseph, Greg Brockman, **597** Alex Ray, Raul Puri, Gretchen Krueger, Michael **598** Petrov, Heidy Khlaaf, Girish Sastry, Pamela Mishkin, **599** Brooke Chan, Scott Gray, Nick Ryder, Mikhail **600** Pavlov, Alethea Power, Lukasz Kaiser, Moham-**601** mad Bavarian, Clemens Winter, Philippe Tillet, Fe-**602** lipe Petroski Such, David W. Cummings, Matthias **603** Plappert, Fotios Chantzis, Elizabeth Barnes, Ariel **604** Herbert-Voss, William H. Guss, Alex Nichol, Igor **605** Babuschkin, S. Arun Balaji, Shantanu Jain, Andrew **606** Carr, Jan Leike, Joshua Achiam, Vedant Misra, Evan **607** Morikawa, Alec Radford, Matthew M. Knight, Miles **608** Brundage, Mira Murati, Katie Mayer, Peter Welinder, **609** Bob McGrew, Dario Amodei, Sam McCandlish, Ilya **610** Sutskever, and Wojciech Zaremba. 2021. Evaluating **611** large language models trained on code. In *ArXiv*.
- **612** Miranda Christ, Sam Gunn, and Or Zamir. 2023. Unde-**613** tectable watermarks for language models. In *arXiv*.
- **614** Hyung Won Chung, Le Hou, Shayne Longpre, Barret **615** Zoph, Yi Tay, William Fedus, Yunxuan Li, Xuezhi

Wang, Mostafa Dehghani, Siddhartha Brahma, Al- **616** bert Webson, Shixiang Shane Gu, Zhuyun Dai, **617** Mirac Suzgun, Xinyun Chen, Aakanksha Chowdh- **618** ery, Alex Castro-Ros, Marie Pellat, Kevin Robinson, **619** Dasha Valter, Sharan Narang, Gaurav Mishra, Adams **620** Yu, Vincent Zhao, Yanping Huang, Andrew Dai, **621** Hongkun Yu, Slav Petrov, Ed H. Chi, Jeff Dean, Ja- **622** cob Devlin, Adam Roberts, Denny Zhou, Quoc V. Le, **623** and Jason Wei. 2022. Scaling instruction-finetuned **624** language models. In *arXiv*. **625**

- Sebastian Gehrmann, Hendrik Strobelt, and Alexander **626** Rush. 2019. GLTR: Statistical detection and visual- **627** ization of generated text. In *Annual Meeting of the* **628** *Association for Computational Linguistics*. **629**
- Xuanli He, Qiongkai Xu, L. Lyu, Fangzhao Wu, and **630** Chenguang Wang. 2021. Protecting intellectual prop- **631** erty of language generation apis with lexical water- **632** mark. In *AAAI Conference on Artificial Intelligence*. **633**
- Xuanli He, Qiongkai Xu, Yi Zeng, Lingjuan Lyu, **634** Fangzhao Wu, Jiwei Li, and Ruoxi Jia. 2022. **635** CATER: Intellectual property protection on text gen- **636** eration APIs via conditional watermarks. In *Ad-* **637** *vances in Neural Information Processing Systems*. **638**
- Zhengmian Hu, Lichang Chen, Xidong Wu, Yihan Wu, **639** Hongyang Zhang, and Heng Huang. 2024. Unbiased **640** watermark for large language models. In *Interna-* **641** *tional Conference on Learning Representations*. **642**
- Mandar Joshi, Eunsol Choi, Daniel Weld, and Luke **643** Zettlemoyer. 2017. TriviaQA: A large scale distantly **644** supervised challenge dataset for reading comprehen- **645** sion. In *Annual Meeting of the Association for Com-* **646** *putational Linguistics*. **647**
- John Kirchenbauer, Jonas Geiping, Yuxin Wen, **648** Jonathan Katz, Ian Miers, and Tom Goldstein. 2023a. **649** A watermark for large language models. In *Interna-* **650** *tional Conference on Machine Learning*. **651**
- John Kirchenbauer, Jonas Geiping, Yuxin Wen, Manli **652** Shu, Khalid Saifullah, Kezhi Kong, Kasun Fernando, **653** Aniruddha Saha, Micah Goldblum, and Tom Gold- **654** stein. 2023b. On the reliability of watermarks for **655** large language models. In *arXiv*. **656**
- Takeshi Kojima, Shixiang (Shane) Gu, Machel Reid, Yu- **657** taka Matsuo, and Yusuke Iwasawa. 2022. Large lan- **658** guage models are zero-shot reasoners. In *Advances* **659** *in Neural Information Processing Systems*. **660**
- Kalpesh Krishna, Yixiao Song, Marzena Karpinska, **661** John Wieting, and Mohit Iyyer. 2023. Paraphras- **662** ing evades detectors of ai-generated text, but retrieval **663** is an effective defense. In *arXiv*. **664**
- Rohith Kuditipudi, John Thickstun, Tatsunori **665** Hashimoto, and Percy Liang. 2023. Robust 666 distortion-free watermarks for language models. In **667** *arXiv*. **668**
- Tom Kwiatkowski, Jennimaria Palomaki, Olivia Red- field, Michael Collins, Ankur Parikh, Chris Alberti, Danielle Epstein, Illia Polosukhin, Jacob Devlin, Ken- ton Lee, Kristina Toutanova, Llion Jones, Matthew Kelcey, Ming-Wei Chang, Andrew M. Dai, Jakob Uszkoreit, Quoc Le, and Slav Petrov. 2019. Natu- ral questions: A benchmark for question answering research. In *Transactions of the Association for Com-putational Linguistics*.
- Chang Liu, Jie Zhang, Han Fang, Zehua Ma, Weim- ing Zhang, and Nenghai Yu. 2023. Dear: A deep- learning-based audio re-recording resilient water- marking. In *AAAI Conference on Artificial Intel-ligence*.
- Xiyang Luo, Ruohan Zhan, Huiwen Chang, Feng Yang, and Peyman Milanfar. 2020. Distortion agnostic deep watermarking. In *IEEE/CVF Conference on Com-puter Vision and Pattern Recognition*.
- Eric Mitchell, Yoonho Lee, Alexander Khazatsky, Christopher D Manning, and Chelsea Finn. 2023. DetectGPT: Zero-shot machine-generated text detec- tion using probability curvature. In *International Conference on Machine Learning*.
- Kishore Papineni, Salim Roukos, Todd Ward, and Wei- Jing Zhu. 2002. Bleu: A method for automatic evalu- ation of machine translation. In *Annual Meeting on Association for Computational Linguistics*.
- Colin Raffel, Noam Shazeer, Adam Roberts, Katherine Lee, Sharan Narang, Michael Matena, Yanqi Zhou, Wei Li, and Peter J. Liu. 2020. Exploring the limits of transfer learning with a unified text-to-text trans-former. In *Journal of Machine Learning Research*.
- NLLB Team, Marta R. Costa-jussà, James Cross, Onur Çelebi, Maha Elbayad, Kenneth Heafield, Kevin Hef- fernan, Elahe Kalbassi, Janice Lam, Daniel Licht, Jean Maillard, Anna Sun, Skyler Wang, Guillaume Wenzek, Al Youngblood, Bapi Akula, Loic Bar- rault, Gabriel Mejia Gonzalez, Prangthip Hansanti, John Hoffman, Semarley Jarrett, Kaushik Ram Sadagopan, Dirk Rowe, Shannon Spruit, Chau Tran, Pierre Andrews, Necip Fazil Ayan, Shruti Bhosale, Sergey Edunov, Angela Fan, Cynthia Gao, Vedanuj Goswami, Francisco Guzmán, Philipp Koehn, Alexandre Mourachko, Christophe Ropers, Safiyyah Saleem, Holger Schwenk, and Jeff Wang. 2022. No language left behind: Scaling human-centered machine translation. In *arXiv*.
- [E](https://gptzero.me)dward Tian and Alexander Cui. 2023. [Gptzero: To-](https://gptzero.me) [wards detection of ai-generated text using zero-shot](https://gptzero.me) [and supervised methods.](https://gptzero.me)
- Hugo Touvron, Thibaut Lavril, Gautier Izacard, Xavier Martinet, Marie-Anne Lachaux, Timothée Lacroix, Baptiste Rozière, Naman Goyal, Eric Hambro, Faisal Azhar, Aurelien Rodriguez, Armand Joulin, Edouard Grave, and Guillaume Lample. 2023. Llama: Open and efficient foundation language models. In *arXiv*.
- Ashish Venugopal, Jakob Uszkoreit, David Talbot, **725** Franz Och, and Juri Ganitkevitch. 2011. Watermark- **726** ing the outputs of structured prediction with an ap- **727** plication in statistical machine translation. In *Con-* **728** *ference on Empirical Methods in Natural Language* **729** *Processing*. **730**
- Rowan Zellers, Ari Holtzman, Hannah Rashkin, **731** Yonatan Bisk, Ali Farhadi, Franziska Roesner, and **732** Yejin Choi. 2019. Defending against neural fake **733** news. In *Advances in Neural Information Processing* **734** *Systems*. **735**
- Susan Zhang, Stephen Roller, Naman Goyal, Mikel **736** Artetxe, Moya Chen, Shuohui Chen, Christopher De- **737** wan, Mona Diab, Xian Li, Xi Victoria Lin, Todor Mi- **738** haylov, Myle Ott, Sam Shleifer, Kurt Shuster, Daniel **739** Simig, Punit Singh Koura, Anjali Sridhar, Tianlu **740** Wang, and Luke Zettlemoyer. 2022. OPT: Open pre- **741** trained transformer language models. In *arXiv*. **742**
- Xuandong Zhao, Prabhanjan Ananth, Lei Li, and Yu- **743** Xiang Wang. 2023a. Provable robust watermarking **744** for ai-generated text. In *arXiv*. **745**
- Xuandong Zhao, Yu-Xiang Wang, and Lei Li. 2023b. **746** Protecting language generation models via invisible **747** watermarking. In *International Conference on Ma-* **748** *chine Learning*. **749**

⁷⁵⁰ A Necessary and Sufficient Watermark is **⁷⁵¹** Provably Better than Soft-Watermark

 In Sec. [4,](#page-4-1) we demonstrated that the Soft-Watermark imposes overly restrictive constraints on gener- ated texts and inserts too many green words to detect LLM-generated texts. The Adaptive Soft- Watermark tunes δ for each text, but Sec. [4](#page-4-1) showed that the Adaptive Soft-Watermark remains to insert too many green words into texts. We rigorously analyze this issue, providing the following theorem, which shows that no matter how well the hyperpa- rameter δ is tuned for each text, the Soft-Watermark cannot precisely control the number of green words in generated texts and generates text that contains more than the required number of green words.

Theorem 1 (Informal). *If we select minimum* $\delta^* \in$ R *such that the z-score of the text generated by the Soft-Watermark exceeds the threshold* Z*, the Soft- Watermark generates a text that contains more than the required number of green words with non-zero probability.*

 The formal theorem and its proof are presented in Sec. [B.](#page-10-0) Unlike the Soft-Watermark and Adaptive Soft-Watermark, the NS-Watermark can insert the minimum number of green words into generated texts using dynamic programming and thus can generate higher-quality texts than these methods.

⁷⁷⁷ B Proof of Theorem [1](#page-10-1)

778 Assumption 1. *The beam size is set to one.*

779 Assumption 2. *The length of generated texts* T *is* **780** *sufficiently long.*

781 **Assumption 3.** $\Delta = \mathbb{R}$.

 Assumption 4. *The hyperparameter* γ *is suffi- ciently small such that the text generated by the greedy search does not contain green words, and texts containing a single green word have a z-score greater than the threshold* Z *for any length* T*.*

 Assumption 5. *For any prompt* x*prompt and gener-ated text* $x_{1:T}$, $L_t(x_{1:T})$, *defined below, is an inde- pendent and identically distributed random vari-**able that follows the distribution* $L_t(x_{1:T}) \sim p(\cdot)$:

791
$$
L_t(x_{1:T}) := logit(x_t | x_{1:t-1}, x_{prompt})
$$

\n $- \max_{x \in V^{green}(x_{t-1})} logit(x | x_{1:t-1}, x_{prompt}),$

 where logit(· | ·) *is the output just before the last softmax layer in LLMs. Furthermore, we assume that its cumulative distribution function is strictly increasing.*

Lemma 1. Let $r_{1:T}$ be the text generated by greedy $\frac{797}{2}$ *search (i.e., text without watermarks). We then se-* **798** *lect the minimum* $\delta^* \in \Delta$ *such that the z-score of* 799 *the text generated by the Soft-Watermark exceeds* **800** *the threshold* Z*. Under Assumptions [1,](#page-10-2) [2,](#page-10-3) [4,](#page-10-4) and [5,](#page-10-5)* **801** *the selected hyperparameter* δ^* *satisfies the follow-* 802 *ing:* **803**

$$
\delta^* := \min_{\delta} \{ \delta \in \Delta \mid \delta \ge \min_t L_t(r_{1:T}) \}. \tag{804}
$$

Furthermore, under Assumption [3,](#page-10-6) δ ⋆ *satisfies* **805**

$$
\delta^* = \min_t L_t(r_{1:T}). \tag{806}
$$

Proof. If δ < min_t $L_t(r_{1:T})$, the text generated 807 by the Soft-Watermark is $r_{1:T}$ and does not con- 808 tain green words. If $\delta \ge \min_t L_t(r_{1:T})$, $(\min\{t \mid s_{00}$ $L_t(r_{1:T}) \leq \delta$. The word becomes a green word, 810 and the text contains at least one green word. Thus, **811** we can obtain the statement. **B**

Theorem 1 (Formal). We select the minimum $\delta^* \in \mathbb{R}^{313}$ ∆ *such that the z-score of the text generated by the* **814** *Soft-Watermark exceeds the threshold* Z*. Under* **815** *Assumptions [1,](#page-10-2) [2,](#page-10-3) [3,](#page-10-6) [4,](#page-10-4) and [5,](#page-10-5) the text generated by* **816** *the Soft-Watermark with* δ^* *contains two or more* 817 *green words with probability* $1 - \log 2$. 818

Proof. Let $r_{1:T}$ be the text generated by the greedy 819 search. We define $c(\cdot)$ and L_{min} as follows: 820

 \overline{c}

$$
(a) \coloneqq \int_{a}^{\infty} p(l) d_l, \tag{82}
$$

$$
L_{\min} := \min_t L_t(r_{1:T}).
$$

From Lemma [1,](#page-10-7) we have $\delta^* = \min_t L_t(r_{1:T})$ and 823 $t^*(\coloneqq \min\{t \mid L_t(r_{1:T}) \leq \delta\})$ -th word becomes 824 a green word in the text generated by the Soft- **825** Watermark. Then, the probability that the remain- **826** ing text has no green words is $c(L_{\text{min}})^{T-t^*}$. More- 827 over, giving that the t^* has equal probabilities for 828 $2, 3, \cdots, T$, the probability that the texts generated 829 by the Soft-Watermark with δ^* contain only one 830 green word is given as **831**

$$
\frac{1}{T-1} \sum_{t=2}^{T} c(L_{\min})^{T-t} = \frac{1 - c(L_{\min})^{T-1}}{(T-1)(1 - c(L_{\min}))}.
$$
\n(7)

Next, we consider the distribution of L_{min} . Now, 833 we have **834**

$$
\Pr(L_{\min} \ge a) = c(a)^{T-1}.
$$

832

836 **Thus, by substituting** $a = c^{-1}(1 - \frac{s}{T-1})$, we can **837** get

838
$$
\Pr(L_{\min} \ge c^{-1}(1 - \frac{s}{T-1})) = (1 - \frac{s}{T-1})^{T-1},
$$

839
$$
\Pr(\frac{s}{T-1} \le 1 - c(L_{\min})) = (1 - \frac{s}{T-1})^{T-1}.
$$

840 **Defining** $Y = (T - 1)(1 - c(L_{min}))$, we obtain

841
$$
\Pr(Y \le s) = 1 - (1 - \frac{s}{T - 1})^{T - 1}
$$

$$
\xrightarrow{q} 1 - e^{-s}.
$$
 (8)

845

843 By substituting the definition of Y, we can rewrite **844** Eq. [\(7\)](#page-10-8) as follows:

845

$$
\frac{1}{T-1} \sum_{t=2}^{T} c(L_{\min})^{T-t} = \frac{1 - (1 - \frac{Y}{T-1})^{T-1}}{Y}
$$

$$
\xrightarrow{T \to \infty} \frac{1 - e^{-Y}}{Y}.
$$
 (9)

847 Combining Eqs. [\(8\)](#page-11-1) and [\(9\)](#page-11-2), we can obtain the **848** statement. \Box

 Assumption [4](#page-10-4) indicates that a single green word is sufficient to make the z-score exceed the thresh- old. However, Theorem [1](#page-10-1) indicates that texts gen- erated by the Soft-Watermark contain two or more green words with non-zero probability, even if we 854 tune the hyperparameter δ for each text.

⁸⁵⁵ C Hyperparameter Setting

856 In our experiments, we set the hyperparameters as **857** follows.

> Table 3: Hyperparameter settings for the NS-Watermark.

	Pre-trained model NLLB-200 / LLaMA
$T_{\rm max}$	100
	Grid search over $\{0.1, 0.01, 0.001, 0.0001\}$.

Table 4: Hyperparameter settings for the Soft-Watermark.

Table 5: Hyperparameter settings for the Adaptive Soft-Watermark.

	Pre-trained model NLLB-200 / LLaMA
k.	
$T_{\rm max}$	100
γ	Grid search over $\{0.1, 0.01, 0.001, 0.0001\}$.
	$\{4, 6, 8, 10, 12, 14\}$
	Binary search over Δ for each text.

⁸⁵⁹ D Additional Experimental Reuslts

860 D.1 Running Time

861 Fig. [5](#page-12-3) shows the running time when varying α . The **862** results indicate that the running time increases as 863 **a** increases when γ is large. This result was con-**864** sistent with the time complexity of Alg. [2,](#page-14-0) which 865 we discussed in Sec. [3.3.](#page-3-2) Then, when γ was small, 866 the running time was almost the same even if α 867 **increased.** This is because when γ is small, G_{max} 868 is small, and the range in the table $T[t][q]$ where **869** we need to fill in Alg. [1](#page-4-0) is small. Thus, the range 870 in $T[t][q]$ where we need to calculate does not in-871 **crease even if** α **increases when** γ **is small.**

Figure 5: Time required to generate a text when varying α . To measure the running time, we used the validation dataset of WMT'16 En→De and reported the average running time. For $\gamma = 0.1, 0.01, 0.001, 0.0001, G_{\text{max}}$ is 22, 5, 2, and 1, respectively.

872 D.2 Robustness to Post-editing Attack

 In this section, we compare the NS-Watermark with the Adaptive Soft-Watermark regarding a trade-off between text quality and robustness. The Adap-**tive Soft-Watermark tunes the hyperparameter** δ for each text such that the z-score is the minimum and exceeds the threshold Z. Thus, the Adaptive **Soft-Watermark may be removed from the gener-** ated texts by replacing only one green word with a red word. To fairly compare the NS-Watermark with the Adaptive Soft-Watermark, we modify the Adaptive Soft-Watermark as in Sec. [3.4](#page-3-3) such that 884 the z-score exceeds the threshold Z after replac-885 ing 50 β % words, where β is the hyperparameter 886 that controls the robustness against post-editing. The pseudo-code is presented in Alg. [4.](#page-15-0) Then, we compare the NS-Watermark with the Adaptive Soft- Watermark, demonstrating that the NS-Watermark can generate more natural texts than the Adaptive **Soft-Watermark when** β **is the same.**

892 Experimental Setting. We used LLaMA-7B 893 with C4 dataset. We set α to one for the NS-

Table 6: Trade-off between text quality and the hyperparameter β . The best values are highlighted in bold.

ß	Method	$PPL \downarrow$	FNR \downarrow / FPR \downarrow
0.0	Adaptive Soft-Watermark	2.48	0.2% / 0.8%
	NS-Watermark	1.92	0.0% / 0.3%
0.05	Adaptive Soft-Watermark	3.43	0.2% / 0.8 %
	NS-Watermark	3.37	0.0% / 0.8%
0.1	Adaptive Soft-Watermark	4.28	0.1% / 0.1 %
	NS-Watermark	3.76	0.0% / 0.1%
0.2	Adaptive Soft-Watermark	6.02	0.1% / 0.1 %
	NS-Watermark	5.42	0.0% / 0.1 %

Watermark and tuned the hyperparameter γ using 894 the validation dataset for the NS-Watermark and **895** Adaptive Soft-Watermark. Then, we show the re- **896** sults when varying $\beta \in \{0, 0.05, 0.1, 0.2\}$. See 897 Sec [C](#page-11-0) for more detailed hyperparameter settings. **898**

Results. Table [6](#page-12-4) lists the results. Compar- **899** ing the PPL of the NS-Watermark and Adap- **900** tive Soft-Watermark with the same β , the NS- **901** Watermark consistently outperforms the Adap- **902** tive Soft-Watermark. Thus, the NS-Watermark **903** achieves a better trade-off between text quality and **904** robustness against post-editing than the Adaptive **905** Soft-Watermark. **906**

D.3 Visualization 907

Figures [6](#page-13-0) and [7](#page-13-1) show the relationship between z- **908** score and text length and that between the number **909** of green words and text length, respectively. **910**

Figure 6: Relationships between z-score and the length of generated texts. We used the validation datasets of WMT'16 En→De. For each γ , we tuned the hyperparameter δ of the Soft-Watermark by increasing $4, 6, 8, \cdots$ and selecting the smallest value such that the FNR becomes less than 5%.

Figure 7: Relationships between the length of generated texts and the number of green words contained in generated texts. The experimental settings are the same as in Fig. [2.](#page-5-2)

E Pseudo-codes **911**

Input: Maximum number of words T_{max} , vocabulary V, beam size k, the length of generated texts

without watermarks \widehat{T} , hyperparameter γ , Z, α . 1 $G_{\text{max}} \leftarrow \lceil \gamma (T_{\text{max}} - 1) + Z \sqrt{\gamma (1 - \gamma) (T_{\text{max}} - 1)} \rceil$ 2 $L \leftarrow \min\{1, \gamma + Z\sqrt{\frac{\gamma(1-\gamma)}{\widehat{\gamma}-1}}\}$ $T-1$ } 3 Let T be a $T_{\text{max}} \times G_{\text{max}}$ table and S be an empty set. 4 $T[1][0] \leftarrow \arg \text{top-}k_{x_1 \in V} p(x_1 | x_{\text{prompt}}).$ 5 for $t = 2, \cdots, T_{max}$ do 6 $\left\{ g_{\min} \leftarrow \min\{G_{\max}, \max\{0, \lceil L(t-1) - \alpha \rceil\} \}$ $7 \mid g_{\text{max}} \leftarrow \min\{G_{\text{max}}, t-1, |L(t-1)+\alpha|\}$ 8 **for** $g = g_{min}, \dots, g_{max}$ do 9 | $X \leftarrow feasible_set(t, g)$ 10 \downarrow *update* (X, t, g) .

11 **return** $\arg\max_{x_{1:t}\in S\cup \boldsymbol{T}[T_{max}][G_{max}]} p(x_{1:t} \mid x_{prompt})$

Algorithm 3: Adaptive Soft-Watermark.

Input: Maximum number of words T_{max} , vocabulary V, beam size k, hyperparameter γ , Z, α , and set ∆. 1 Let $\delta_1, \cdots, \delta_{|\Delta|}$ be the elements in Δ in ascending order. 2 $a, c \leftarrow 1, |\Delta|$. 3 $z_{\min}, \delta^* \leftarrow \infty, \delta_{|\Delta|}.$ 4 while $a \leq c$ do $\mathfrak{s} \mid b \leftarrow \lceil \frac{a+c}{2} \rceil.$ 6 Generate a text using the Soft-Watermark with δ_b . ⁷ if *the z-score of the generated text is greater than or equal to* Z then $\begin{array}{c|c|c|c} \mathbf{s} & \mathbf{c} & \mathbf{c} & \mathbf{b} \end{array}$ ⁹ if *the z-score is less than* z*min* then 10 | Store z-score in z_{min} . 11 \vert \vert δ $\delta^* \leftarrow \delta_b$. ¹² else 13 $\vert \cdot \vert \cdot a \leftarrow b$. 14 **return** the text generated by the Soft-Watermark with δ^* .

Algorithm 4: Adaptive Soft-Watermark with β .

Input: Maximum number of words T_{max} , vocabulary V, beam size k, hyperparameter γ , Z, α , β , and set ∆. 1 Let $\delta_1, \cdots, \delta_{|\Delta|}$ be the elements in Δ in ascending order. 2 $a, c \leftarrow 1, |\Delta|$. 3 $z_{\min}, \delta^* \leftarrow \infty, \delta_{|\Delta|}.$ 4 while $a \leq c$ do $\mathfrak{s} \mid b \leftarrow \lceil \frac{a+c}{2} \rceil.$ 6 Generate a text using the Soft-Watermark with δ_b . 7 Let t be the length of generated text and $x_{1:t}$ be the generated text. $\hat{z} \leftarrow \frac{|x_{1:t}|_{\mathbf{G}}-(\gamma+\beta)(T-1)}{\sqrt{\gamma(1-\gamma)(T-1)}}.$ $\mathfrak{g} \;\; \mid \;\; \mathbf{if} \; \tilde{z} \geq Z \; \mathbf{then}$ 10 $\vert \vert \cdot \vert c \leftarrow b$. 11 **if** $\tilde{z} < z_{min}$ then 12 $|$ $z_{\min} \leftarrow \tilde{z}.$ 13 $\Big|$ $\delta^* \leftarrow \delta_b$. ¹⁴ else 15 $\Big|$ $a \leftarrow b$.

16 **return** the text generated by the Soft-Watermark with δ^* .

E.1 Examples of Generated Texts **912**

Hungary.

Table 7: Texts generated by the NS-Watermark on WMT'16 Ge→En.

Table 8: Texts generated by the Soft-Watermark on WMT'16 Ge→En.

Table 9: Texts generated by the Adaptive Soft-Watermark on WMT'16 Ge→En.

Table 10: Texts generated by the NS-Watermark on WMT'14 Fr→En.

Table 11: Texts generated by the Soft-Watermark on WMT'14 Fr→En.

Table 12: Texts generated by the Adaptive Soft-Watermark on WMT'14 Fr→En.

Table 14: Texts generated by the NS-Watermark on C4.

Table 15: Texts generated by the Soft-Watermark on C4.

Table 16: Texts generated by the Adaptive Soft-Watermark on C4.

