
Spotting LLMs With Binoculars: Zero-Shot Detection of Machine-Generated Text

Abhimanyu Hans^{* 1} Avi Schwarzschild^{* 2} Valeriia Cherepanova¹ Hamid Kazemi¹ Aniruddha Saha¹
Micah Goldblum³ Jonas Geiping⁴ Tom Goldstein¹

Abstract

Detecting text generated by modern large language models is thought to be hard, as both LLMs and humans can exhibit a wide range of complex behaviors. However, we find that a score based on contrasting two closely related language models is highly accurate at separating human-generated and machine-generated text. Based on this mechanism, we propose a novel LLM detector that only requires simple calculations using a pair of pre-trained LLMs. The method, called *Binoculars*, achieves state-of-the-art accuracy without any training data. It is capable of spotting machine text from a range of modern LLMs without any model-specific modifications. We comprehensively evaluate *Binoculars* on a number of text sources and in varied situations. Over a wide range of document types, *Binoculars* detects over 90% of generated samples from ChatGPT (and other LLMs) at a false positive rate of 0.01%, despite not being trained on any ChatGPT data. Code available at <https://github.com/ahans30/Binoculars>.

1. Introduction

We present a method to detect LLM-generated text that works in the zero-shot setting in which no training examples are used from the LLM source. Even with this strict limitation, our scheme still out-performs all open-source methods for ChatGPT detection and is competitive with or better than commercial APIs, despite these competitors using training samples from ChatGPT (Mitchell et al., 2023;

^{*}Equal contribution ¹University of Maryland ²Carnegie Mellon University ³New York University ⁴ELLIS Institute Tübingen, MPI Intelligent Systems. Correspondence to: Abhimanyu Hans <ahans1@umd.edu>, Avi Schwarzschild <schwarzschild@cmu.edu>.

Verma et al., 2023). At the same time, because of the zero-shot nature of our detector, the very same detector can spot multiple different LLMs with high accuracy—something that all existing solutions fail to do.

The ability to detect LLMs in the zero-shot setting addresses issues of growing importance. Prior research on combating academic plagiarism (Turnitin.com) has fixated strongly on ChatGPT because of its simple and accessible interface. But more sophisticated actors use LLM APIs to operate bots, create fake product reviews, and spread misinformation on social media platforms at a large scale. These actors have a wide range of LLMs available to them beyond just ChatGPT, making zero-shot, model-agnostic detection critical for social media moderation and platform integrity assurance (Crothers et al., 2022; Bail et al., 2023). Our zero-shot capability is a departure from existing detectors that rely on model-specific training data and often fail to transfer to new models.

Our proposed detector, called *Binoculars*, works by viewing text through two lenses. First, we compute the log perplexity of the text in question using an “observer” LLM. We then compute next-token predictions using a “performer” LLM and compute their perplexity according to the observer. We call this metric *cross-perplexity*. We observe that perplexity per cross-perplexity is a surprisingly powerful signal to detect LLM-text. We first motivate this simple observation, and then show that it is sufficient to build a strong zero-shot detector, which we extensively stress-test in a number of text domains.

2. The LLM Detection Landscape

Successful efforts to spot machine-generated text show promise on early models whose generation output is not convincingly human. However, with the rise of transformer models for language modeling (Radford et al., 2019; Brown et al., 2020; Chowdhery et al., 2022; Touvron et al., 2023), primitive mechanisms to detect machine-generated text are rendered useless. While one approach is to record (Krishna et al., 2023) or watermark all generated text (Kirchenbauer et al., 2023), these *preemptive detection* approaches can only be implemented with full control over

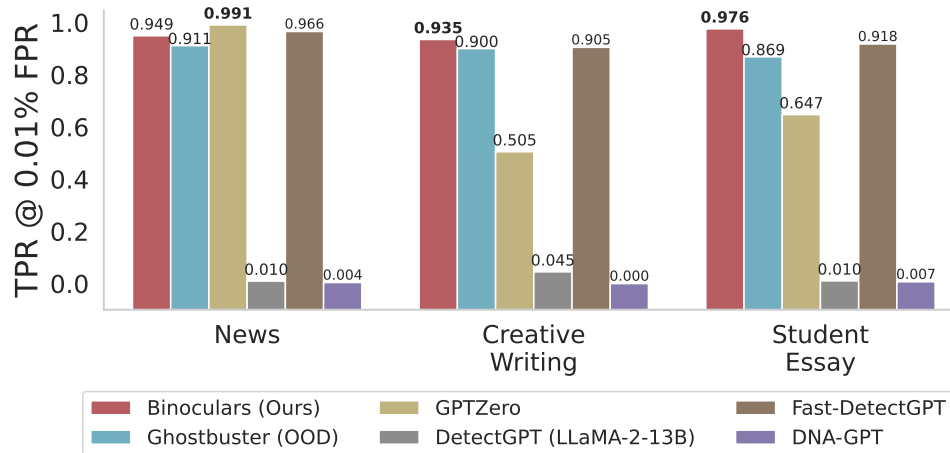


Figure 1. **Detection of Machine-Generated Text from ChatGPT.** Our detection approach using *Binoculars* is highly accurate at separating machine-generated and human-written samples from *News*, *Creative Writing* and *Student Essay* datasets with a false positive rate of 0.01%. *Binoculars*, based on open-source Falcon models with no finetuning, outperforms commercial detection systems, such as GPTZero, as well as open-source detectors – even though both of these baselines are specifically tuned to detect ChatGPT (Verma et al., 2023; Tian, 2023a). Our approach operates entirely in a zero-shot setting and has not been tuned on ChatGPT specifically.

the generative model.

Instead, the recent spread of machine-generated text, especially via ChatGPT, has led to a flurry of work on *post-hoc detection* approaches that can be used to detect machine text without cooperation from model owners. These detectors can be separated into two main groups. The first is trained detection models, where a pretrained language model backbone is finetuned for the binary classification task of detection (Solaiman et al., 2019; Zellers et al., 2019; Yu et al., 2023; Zhan et al., 2023), including techniques like adversarial training (Hu et al., 2023) and abstention (Tian et al., 2023). Alternatively, instead of finetuning the whole backbone, a linear classifier can be fit on top of frozen learned features, which allows for the inclusion of commercial API outputs (Verma et al., 2023).

The second category of approaches comprises statistical signatures that are characteristic of machine-generated text. These approaches have the advantage of requiring none or little training data and they can easily be adapted to newer model families (Pu et al., 2022). Examples include detectors based on perplexity (Tian, 2023b; Vasilatos et al., 2023; Wang et al., 2023), perplexity curvature (Mitchell et al., 2023), log rank (Su et al., 2023), intrinsic dimensionality of generated text (Tulchinskii et al., 2023), and n-gram analysis (Yang et al., 2023a). Our coverage of the landscape is non-exhaustive, and we refer to recent surveys Ghosal et al. (2023); Tang et al. (2023); Dhaini et al. (2023); Guo et al. (2023) for additional details.

From a theoretical perspective, Varshney et al. (2020), Helm et al. (2023), and Sadasivan et al. (2023) all dis-

cuss the limits of detection. These works generally agree that fully general-purpose models of language would be, by definition, impossible to detect. However, Chakraborty et al. (2023) note that even models that are arbitrarily close to this optimum are technically detectable given a sufficient number of samples. In practice, the relative success of detection approaches, such as the one we propose and analyze in this work, provides constructive evidence that current language models are imperfect representations of human writing – and thereby detectable. Finally, the robustness of detectors to attacks attempting to circumvent detection can provide stronger practical limits on reliability in the worst case (Bhat & Parthasarathy, 2020; Wolff & Wolff, 2022; Liyanage & Buscaldi, 2023).

With an understanding of how much work exists on LLM detection, a crucial question arises: How do we appropriately and thoroughly evaluate detectors? Many works focus on accuracy on balanced test sets and/or AUC of their proposed classifiers, but these metrics are not well-suited for the high-stakes question of detection. Ultimately, only detectors with low false positive rates across a wide distribution of human-written text, truly reduce harm. Further, Liang et al. (2023) note that detectors are often only evaluated on relatively easy datasets that are reflective of their training data. Their performance on out-of-domain samples is often abysmal. For example, TOEFL essays written by non-native English speakers were wrongly marked as machine-generated 48-76% of the time by commercial detectors (Liang et al., 2023).

In Section 3, we motivate our approach and discuss why detecting language model text, especially in the ChatGPT

world, is difficult. In this work, our emphasis is directed toward baselines that function within post-hoc, out-of-domain (zero-shot), and black-box detection scenarios. We use the state-of-the-art open source detector Ghostbuster (Verma et al., 2023), the commercially deployed GPTZero¹, DetectGPT (Mitchell et al., 2023) and its efficient version Fast-DetectGPT (Bao et al., 2023) and finally DNA-GPT (Yang et al., 2023b) to compare detection performance across various datasets in Section 4. In Section 5, we evaluate the reliability of *Binoculars* in various settings that constitute edge cases and crucial deployment behaviors that a detector based on *Binoculars* has to take into account. Please see appendix A.1.3 for more details.

3. Binoculars: How it works

Our approach, *Binoculars*, is so named as we look at inputs through the lenses of two different language models. It is well known that perplexity – a common baseline for machine/human classification – is insufficient on its own, leading prior work to disfavor approaches based on statistical signatures. However, we propose using a ratio of perplexity measurement and *cross-perplexity*, a notion of how surprising the next token predictions of one model are to another model. This two-model mechanism is the basis for our general and accurate detector, and we show that this mechanism is able to detect a number of LLMs, even when they are unrelated to the two models used by *Binoculars*.

3.1. Background & Notation

A string of characters s can be parsed into tokens and represented as a list of token indices \vec{x} by a tokenizer T . Let x_i denote the token ID of the i -th token, which refers to an entry in the LLMs vocabulary $V = \{1, 2, \dots, n\}$. Given a token sequence as input, a language model \mathcal{M} predicts the next token by outputting a probability distribution over the vocabulary:

$$\begin{aligned} \mathcal{M}(T(s)) &= \mathcal{M}(\vec{x}) = Y \\ Y_{ij} &= P(v_j | x_{0:i-1}) \text{ for all } j \in V. \end{aligned} \quad (1)$$

We abbreviate $\mathcal{M}(T(s))$ as $\mathcal{M}(s)$ where the tokenizer is implicitly the one used in training \mathcal{M} . We define $\log \text{PPL}$, the log-perplexity, as the average negative log-likelihood of all tokens in the given sequence. Formally, let

$$\begin{aligned} \log \text{PPL}_{\mathcal{M}}(s) &= -\frac{1}{L} \sum_{i=1}^L \log(Y_{ix_i}), \\ \text{where } \vec{x} &= T(s), Y = \mathcal{M}(\vec{x}), \\ \text{and } L &= \text{number of tokens in } s. \end{aligned} \quad (2)$$

Intuitively, log-perplexity measures how “surprising” a string is to a language model. As mentioned above, perplexity has been used to detect LLMs, as humans produce more surprising text than LLMs. This is reasonable, as log PPL is also the loss function used to train generative LLMs, and models are likely to score their own outputs as unsurprising. Our method also measures how surprising the output of one model is to another. We define the *cross-perplexity*, which takes two models and a string as its arguments. Let $\log \text{X-PPL}_{\mathcal{M}_1, \mathcal{M}_2}(s)$ measure the average per-token cross-entropy between the outputs of two models, \mathcal{M}_1 and \mathcal{M}_2 , when operating on the tokenization of s .²

$$\log \text{X-PPL}_{\mathcal{M}_1, \mathcal{M}_2}(s) = -\frac{1}{L} \sum_{i=1}^L \mathcal{M}_1(s)_i \cdot \log(\mathcal{M}_2(s)_i). \quad (3)$$

Note that \cdot denotes the dot product between two vector-valued quantities.

3.2. What makes detection hard? A primer on the capybara problem.

Why do we require measurements of both perplexity and cross-perplexity? Unsurprisingly, LLMs tend to generate text that is unsurprising to an LLM. Meanwhile, because humans differ from machines, human text has higher perplexity according to an LLM observer. For this reason, it is tempting to use raw perplexity for LLM detection, as high perplexity is a strong sign of a human author.

Unfortunately, this intuition breaks when hand-crafted prompts are involved. Prompts have a strong influence over downstream text, and prompts are typically unknown to the detector. On the one hand, the prompt “1, 2, 3,” might result in the very low perplexity completion “4, 5, 6.” On the other hand, the prompt “Can you write a few sentences about a capybara that is an astrophysicist?” will yield a response that seems more surprising. In the presence of a prompt, the response may be unsurprising (low perplexity). But in the absence of the prompt, a response containing the curious words “capybara” and “astrophysicist” in the same sentence will have high perplexity, resulting in the false determination that the text was written by a human, see the example in Table 1. Clearly, certain contexts will result in high perplexity and others low perplexity, regardless of whether the author is human or machine. We refer to this dilemma as “the capybara problem” – in the absence of the prompt, LLM detection seems difficult and naive perplexity-based detection fails.

3.3. Our Detection Score

Binoculars solves the *capybara problem* by providing a

¹<https://gptzero.me/>

²This requires that \mathcal{M}_1 and \mathcal{M}_2 share a tokenizer.

“Dr. Capy Cosmos, a capybara unlike any other, astounded the scientific community with his groundbreaking research in astrophysics. With his keen sense of observation and unparalleled ability to interpret cosmic data, he uncovered new insights into the mysteries of black holes and the origins of the universe. As he peered through telescopes with his large, round eyes, fellow researchers often remarked that it seemed as if the stars themselves whispered their secrets directly to him. Dr. Cosmos not only became a beacon of inspiration to aspiring scientists but also proved that intellect and innovation can be found in the most unexpected of creatures.” – GPT 4

Table 1. This quote is LLM output from ChatGPT (GPT-4) when prompted with “Can you write a few sentences about a capybara that is an astrophysicist?” The Falcon LLM assigns this sample a high perplexity (2.20), well above the mean for both human and machine data. Despite this problem, our detector correctly assigns a *Binoculars* score of 0.73, which is well below the global threshold of 0.901, resulting in a correct classification with high confidence. For reference, DetectGPT wrongly assigns a score of 0.14, which is below its threshold of 0.17, and classifies the text as human. GPTZero assigns a 49.71% score that this text is generated by AI.

mechanism for estimating the baseline perplexity induced by the prompt. By comparing the perplexity of the observed text to this expected baseline, we observe a surprising LLM text signature.

Motivation. LLM-generated text may exhibit a high perplexity score depending on the prompt specified which yields a simple perplexity-based detector ineffective (see the “Capybara Problem” in Table 1). To calibrate for prompts that yield high-perplexity generation, we use *cross-perplexity* introduced Equation (3) as a normalizing factor that intuitively encodes the perplexity level of next-token predictions from two models.

Rather than examining raw perplexity scores, we instead propose measuring whether the tokens that appear in a string are surprising *relative to the baseline perplexity of an LLM acting on the same string*. A string might have properties that result in high perplexity when completed by any agent, machine or human. Yet, we expect the next-token choices of humans to be even higher perplexity than those of a machine. By normalizing the observed perplexity by the expected perplexity of a machine acting on the same text, we can arrive at a detection metric that is fairly invariant to the prompt; see Table 1.

We propose the *Binoculars* score B as a sort of normalization or reorientation of perplexity. In particular, we look at the ratio of perplexity to cross-perplexity.

$$B_{\mathcal{M}_1, \mathcal{M}_2}(s) = \frac{\log \text{PPL}_{\mathcal{M}_1}(s)}{\log \text{X-PPL}_{\mathcal{M}_1, \mathcal{M}_2}(s)} \quad (4)$$

Here, the numerator is simply the perplexity, which measures how surprising a string is to \mathcal{M}_1 . The denominator measures how surprising the token predictions of \mathcal{M}_2 are when observed by \mathcal{M}_1 . Intuitively, we expect a human to diverge from \mathcal{M}_1 more than \mathcal{M}_2 diverges from \mathcal{M}_1 , provided the LLMs \mathcal{M}_1 and \mathcal{M}_2 are more similar to each other than they are to a human.

The *Binoculars* score is a general mechanism that captures a statistical signature of machine text. In the sections below, we show that for most obvious choices of \mathcal{M}_1 and \mathcal{M}_2 , *Binoculars* separates machine and human text better than perplexity alone—and it is capable of detecting generic machine text generated by a third model altogether.

Interestingly, we can draw some connection to other approaches that contrast two language models, such as contrastive decoding (Li et al., 2023), which aims to generate high-quality text completions by generating text that roughly maximizes the difference between a weak and a strong model. Speculative decoding is similar (Chen et al., 2023; Leviathan et al., 2023), it uses a weaker model to plan completions. Both approaches function best when pairing a strong model with a very weak secondary model. However, as we show below, our approach works best for two models that are very close to each other in performance. In the remainder of this work, we use the open-source models Falcon-7b model (\mathcal{M}_1) and the Falcon-7b-instruct (\mathcal{M}_2) (Almazrouei et al., 2023). The full set of combinations of scoring models used can be found in Table 3 in the appendix.

4. Accurate Zero-Shot Detection

In this section, we evaluate *Binoculars* as a zero-shot LLM detector in multiple domains. In our experiments, we focus on the problem setting of detecting machine-generated text from a modern LLM, as generated in common use cases without consideration for the detection mechanism.

4.1. Datasets

We start our experiments with several datasets described in the LLM detection literature. The most recent baseline to which we compare is Ghostbuster. Verma et al. (2023), who propose this method, also introduce three datasets that we include in our study: *Writing Prompts*, *News*, and *Student Essay*. These are balanced datasets with equal num-

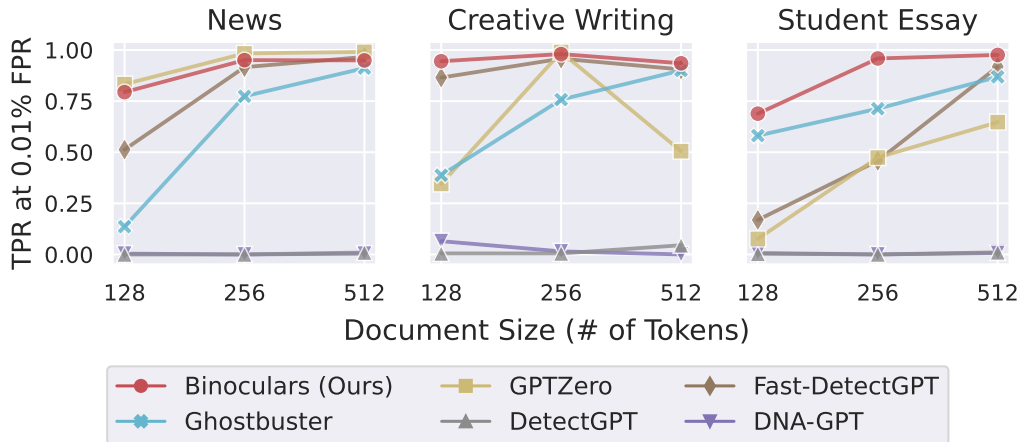


Figure 2. **Impact of Document Size on Detection Performance.** The plot displays the TPR at 0.01% FPR across varying document sizes by prefixing sample documents. The x-axis represents the number of tokens of the observed document, while the y-axis indicates the corresponding detection performance, highlighting the *Binoculars* ability to detect with a low number of tokens.

bers of human samples and machine samples. The machine samples are written by ChatGPT.³

We also generate several datasets of our own to evaluate our capability in detecting other language models aside from ChatGPT. Drawing samples of human-written text from CCNews (Hamborg et al., 2017), PubMed (Sen et al., 2008), and CNN (Hermann et al., 2015), we generate corresponding, machine-generated completions using LLaMA-2-7B and Falcon-7B (see details in Appendix A.1.1). Further, we use the Orca dataset (Lian et al., 2023), which provides several million instruction prompts with their machine-generated completions from GPT-3 and GPT-4.

4.2. Metrics

Since detectors are binary classifiers, the standard suite of binary classification metrics is relevant. It is often considered comprehensive to look at ROC curves and only report under the curve (AUC) as a performance metric. In fact, Verma et al. (2023) and Mitchell et al. (2023) only report performance as measured by AUC and F1 scores. We argue that these metrics alone are inadequate when evaluating LLM detection performance.

In LLM detection, the most concerning harms often arise from *false positives*, i.e., instances when human text is wrongly labeled as machine-generated. For this reason, we focus on true-positive rates (TPR) at low false-positive rates (FPR), and adopt a standard FPR threshold of 0.01%.⁴ We also note that AUC scores are often uncorrelated with

³In the following we will always use ChatGPT as short-hand for the chat versions of GPT-3.5-(turbo).

⁴The smallest threshold we can comprehensively evaluate to sufficient statistical significance with our compute resources.

TRP@FPR when the FPR is below 1% (Table 4). When evaluating F1-Score, we purely use the “out-of-domain” threshold. (see Appendix A.1.2 for details).

4.3. Benchmark Performance

Using a handful of datasets, we compare the AUC and TPR of *Binoculars* to Ghostbuster (Verma et al., 2023), GPTZero (Tian, 2023a), the commercially deployed GPTZero, and DetectGPT (using LLaMA-2-13B to score curvature) (Mitchell et al., 2023). We highlight that these comparisons on machine samples from ChatGPT are *in favor* of GPTZero and Ghostbuster, as these detectors have been tuned to detect ChatGPT output, and comparisons using samples from LLaMA models are *in favor* of DetectGPT for the same reason.

Ghostbuster Datasets. The Ghostbuster detector is a recent detector tuned to detect output from ChatGPT. Using the same three datasets introduced and examined in the original work by Verma et al. (2023), we compare TPR at 0.01% FPR in Figure 1 (and F1-Score in Figure 9 in Appendix) to show that *Binoculars* outperforms Ghostbuster in the “out-of-domain” setting. A desirable property for detectors is that with more information they get stronger. Figure 2 shows that both *Binoculars* and Ghostbuster have this property, and that the advantages of *Binoculars* are even clearer in the few-token regime.

Open-Source Language Models. We show that our detector is capable of detecting the output of several LLMs, such as LLaMA as shown in Figure 3 and Falcon as shown in Figure 12 in the appendix. Here we also observe that Ghostbuster is indeed only capable of detecting ChatGPT, and it fails to reliably detect LLaMA generated text.

The detailed ROC plots in Figure 3 compare performance across thresholds for all methods.

5. Reliability in the Wild

How well does *Binoculars* work when faced with scenarios encountered in the wild? The key takeaway that we want to highlight throughout this section is that the score underlying *Binoculars*, i.e. Equation (4) is a *machine-text detector*. Intuitively, this means that it predicts how likely it is that the given piece of text could have been generated by a similar language model. This has a number of crucial implications regarding memorized samples, text from non-native speakers, modified prompting strategies, and edge cases, all of which we comprehensively evaluate in this section.

5.1. Varied Text Sources

We start our investigation by exploring detector performance in additional settings outside of the English language. To this end we investigate the Multi-generator, Multi-domain, and Multi-lingual (M4) detection datasets (Wang et al., 2023). These samples come from Arxiv, Reddit, Wikihow, and Wikipedia sources, and include examples in varied languages, such as Urdu, Russian, Bulgarian, and Arabic. Machine text samples in this dataset are generated via ChatGPT. In Figure 4, we show the precision and recall of *Binoculars* and four other baselines, showing that our method generalizes across domains and languages. These baselines, released with the M4 Datasets, include fine-tuned RoBERTa (Liu et al., 2019) classifier (Zellers et al., 2019; Solaiman et al., 2019), Logistic Regression over Giant Language Model Test Room (LR GLTR) (Gehrmann et al., 2019) which generates features assuming predictions are sampled from a specific token distribution, Stylistic (Li et al., 2014) which employs syntactic features at character, word, and sentence level, News Landscape classifiers (NELA) (Horne et al., 2019) which generates and leverages semantic and structural features for veracity classification. We reprint this result from the benchmark for reference. Results with more source models appear in Figure 5.

5.2. Other languages

When evaluating *Binoculars* on languages that are not well represented in Common Crawl data (standard LLM pre-training data), we find that false-positive rates remain low, which is highly desirable from a harm reduction perspective. However, machine text in these low-resource languages is often classified as human. Figure 6 shows that we indeed have reasonable precision but poor recall in these settings. While this ordering of scores is a win for harmlessness, why is multilingual text detection limited?

Due to the limited capability of Falcon models (powering

Binoculars) in generating text in these low-resource languages in our experiments, we hypothesize that a stronger multilingual pair of models would lead to a version of *Binoculars* that could spot ChatGPT-generated text in these languages more effectively.

False-positive rates on non-native speakers’ writing A significant concern about LLM detection algorithms, as raised by Liang et al. (2023), is that LLM detectors are inadvertently biased against non-native English speakers (ESL) classifying their writing as machine-generated exceedingly often. To test this, we analyze essays from *EssayForum*, a web page for ESL students to improve their academic writing (EssayForum, 2022). This dataset contains both the original essays, as well as grammar-corrected versions. We compare the distribution of *Binoculars* scores across the original and the grammar-corrected samples. Interestingly, and in stark comparison to commercial detectors examined by Liang et al. (2023) on a similar dataset, *Binoculars* attains equal accuracy at 99.67% for both corrected and uncorrected essay datasets (see Figure 7). We also point out that the *Binoculars* score distribution on ESL’s text highly overlaps with that of grammar-corrected versions of the same essays, showing that detection through *Binoculars* is insensitive to this type of shift.

5.3. Memorization

One common feature of perplexity-based detection is that highly memorized examples are classified as machine-generated. For example, famous quotes that appear many times in the training data likely have low perplexity according to an observer model that has overfit to these strings. By looking at several examples, we examine how *Binoculars* performs on this type of data.

See Table 5 in Appendix A.4 for all famous texts evaluated in this study. First, we ask about the US Constitution – a document that is largely memorized by modern LLMs. This example has a *Binoculars* score of 0.76, well into the machine range. Of the 11 famous texts we study, this was the lowest score (most *machine-y*). Three of the 11 fall on the machine-side of our threshold. It is important to note that while this behavior may be surprising, and does require careful consideration in deployment, it is fully consistent with a machine-text detector. Memorized text is both text written by human writers, and text that is likely to be generated by an LLM. Classification of memorized text as machine generated may be acceptable or even desirable in some applications (e.g., plagiarism detection), or undesirable in others (e.g., removal of LLM-generated text from a training corpus).

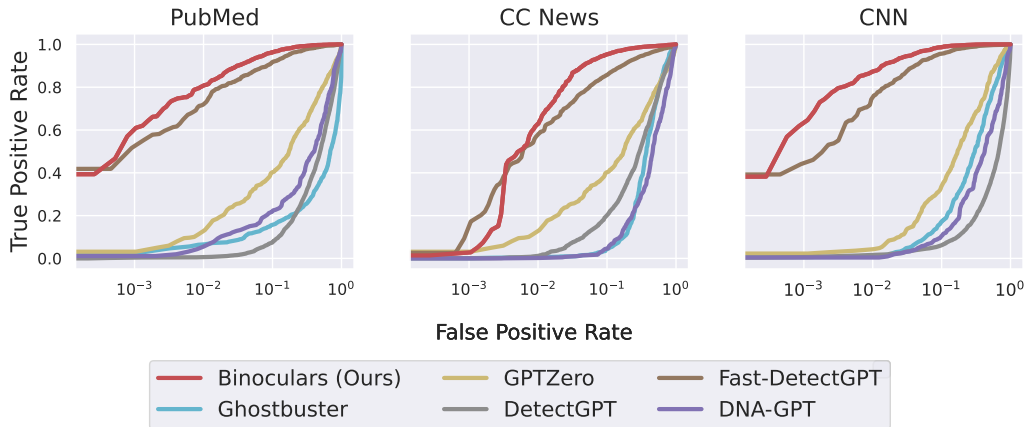


Figure 3. Detecting LLaMA-2-13B generations. *Binoculars* achieves higher TPRs for low FPRs (on log scale) than other methods.

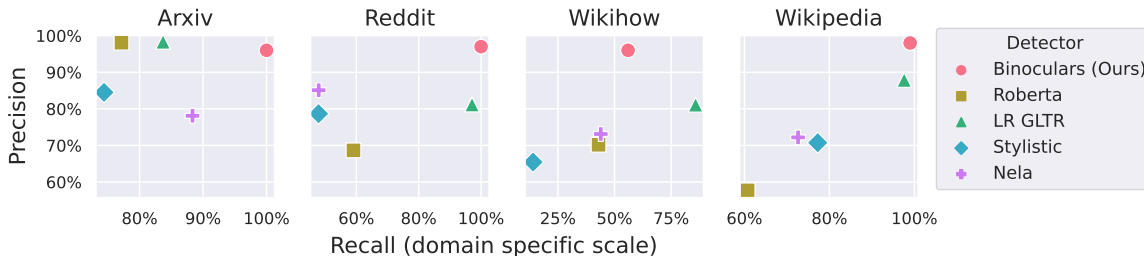


Figure 4. Detection of ChatGPT-generated text in various domains from M4 Dataset. *Binoculars* is more precise over 4 domains using the OOD threshold for detection. We use the mean of out-of-domain performance metrics reported by Wang et al. (2023)

Table 2. Excerpts from LLaMA-2-13B-chat generations using an Open-Orca sample prompt with varying system prompts. For the full modifications to the prompts to generate these stylized outputs, see Appendix A.6.

Prompt	Write an article based on this “Use an adjustable jump. Create your jump with cinder blocks and plywood. Use natural outdoor obstacles as jumps. Set down a treat on the far side of the jump. Practice at the lowest level until your dog is comfortable. Raise the bar gradually. Use the same method to teach your dog to jump through hoops.”
Default	A well-trained dog is not only a delight to be around, but it also provides a sense of pride and accomplishment to the owner. One captivating and useful skill that you may want to teach your dog is jumping. Whether you’re doing it for fun, agility competitions, or simply to keep your furry companion physically engaged, teaching your dog how to jump can be a bonding and rewarding experience.
Carl Sagan	Ah, my dear friend, we stand at the precipice of a most wondrous adventure, an odyssey of the canine kind. Our quest, to teach our loyal companions, those furry wonders of nature, to soar through the air with grace and agility. The tool at our disposal, the adjustable jump.
Non-Robotic	Hey there, fellow dog lovers! Are you looking for a fun and challenging way to keep your furry friend active and engaged? Look no further than an adjustable jump! Not only is it a great way to provide your dog with physical exercise, but it’s also a great way to bond with your pup.
Pirate	Arrrr, me hearties! Ye landlubbers be wantin’ yer pooch ta learn ta jump, eh? Well, fear not! I be here ta help ye teach yer furry first mate ta jump over obstacles like a proper salty sea dog! First things first, ye need ta create the jump. Now, I know what ye be thinkin’: “Cinder blocks and plywood? That be a bit...rugged, don’t ye think?” But never fear, me hearties!

5.4. Modified Prompting Strategies

The Open Orca dataset contains machine generations from both GPT-3 and GPT-4 for a wide range of tasks (Lian et al., 2023). This serves as a diverse test bed for measuring *Binoculars* on both of these modern high-performing LLMs. Impressively, *Binoculars* detects 92% of GPT-3 samples and 89.57% of GPT-4 samples when using the global threshold (from reference datasets). Note, we only report accuracy since this is over a set of machine-

generated text only. This dataset also allows us to explore how sensitive *Binoculars* is to modifying prompts.

Simple detection schemes are sometimes fooled by simple changes to prompting strategies, which can produce stylized text that deviates from the standard output distribution. With this in mind, we use LLaMA-2-13B-chat and prompts designed to tweak the style of the output. Specifically, we prompt LLaMA2-13B-chat with three different system prompts by appending to the standard system prompt a re-

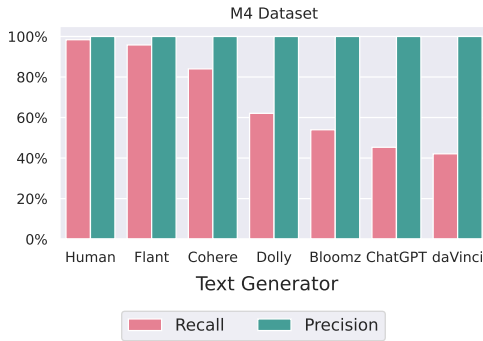


Figure 5. Performance of *Binoculars* on samples from various generative models.

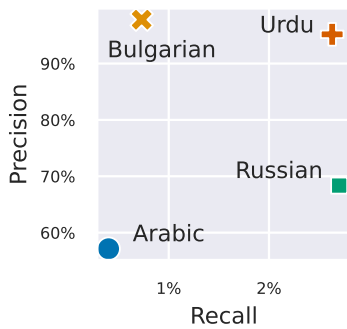


Figure 6. *Binoculars* operates at high precision in Bulgarian and Urdu, but with low recall in all four languages.

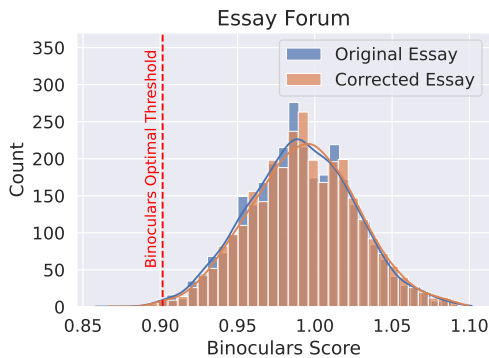


Figure 7. The distribution of *Binoculars* scores remains unchanged when the English grammar is corrected in essays composed by non-native speakers. Both original and corrected essays are unambiguously classified as human-written.

quest to write in Carl Sagan’s voice or without any mechanical or robotic sounding words or like a pirate.

In general, we find that these stylistic changes do not significantly impact the accuracy of *Binoculars*. The biggest impact we observe arises when asking for pirate-sounding output, and this only decreases the sensitivity (increases the false negative rate) by 1%; see Figure 8. Table 6 records

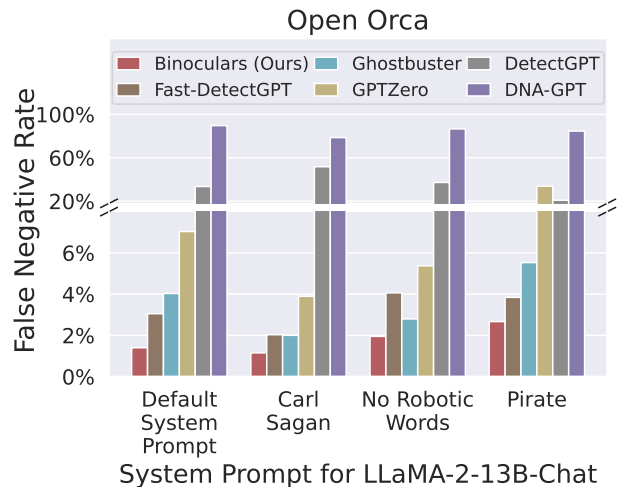


Figure 8. Detection with modified system prompts.

generations based on a sample prompt employing the specified prompting strategies.

Next, we also want to test whether arbitrary mistakes, hash-codes, or other kinds of random (and random seeming) strings bias our model towards false positives. To test the impact of randomness, we generate random sequences of tokens from the Falcon tokenizer, and score them with *Binoculars* as usual. We plot a histogram of this distribution in Figure 14. We find that *Binoculars* confidently scores this as human, with a mean score around 1.35 for Falcon (humans have a mean of around 1). This is expected, as trained LLMs are strong models of language and exceedingly unlikely to ever generate these completely random sequences. In particular, the generation of these random sequences is even less likely than the generation of perfect human-written text by chance.

6. Discussion and Limitations

We present *Binoculars*, a method for detecting LLM output in the zero-shot case in which no data is available from the generation model. We speculate that this transferability arises from the similarity between modern LLMs, as they all use nearly identical transformer components and are likely trained in large part on Common Crawl (commoncrawl.org) data from similar time periods. As the number of open source LLMs rapidly increases, the ability to detect multiple LLMs with a single detector is a major advantage of *Binoculars*, for example when used for platform moderation. Our study has a number of limitations. Due to limited GPU memory, we do not perform broader studies with larger (30B+) open-source models. Further, we focus on the problem setting of detecting machine-generated text in normal use, and we do not consider explicit efforts to by-

pass detection. Finally, there are other non-conversational text domains, such as source code, which we do not investigate in this study.

Impact Statement

Language model detection may be a key technology to reduce harm, whether to monitor machine-generated text on internet platforms and social media, filter training data, or identify responses in chat applications. Nevertheless, care has to be taken so that detection mechanisms actually reduce harm, instead of proliferating or increasing it. We provide an extensive reliability investigation of the proposed *Binoculars* mechanisms in Section 5, and believe that this is a significant step forward in terms of reliability, for example when considering domains such as text written by non-native speakers. Yet, we note that this analysis is only a first step in the process of deploying LLM detection strategies and does not absolve developers of such applications from carefully verifying the impact on their systems. We especially caution that the existence of LLM detectors does not imply that using them is worthwhile in all scenarios.

Also, we explicitly highlight that we consider the task of detecting “naturally” occurring machine-generated text, as generated by LLMs in common use cases. We understand that no detector is perfect and we do not guarantee any performance in settings where a motivated adversary tries to fool our system. We also note that our detector does not provide an explanation or interpretation of its predictions for any given sample and thus is black-box in nature. We present a thorough evaluation across a wide variety of test sources, but we maintain that directed attempts to bypass our classifier might be possible, as is often the case for systems that rely on neural networks.

Acknowledgments

This work was made possible by the ONR MURI program and the AFOSR MURI program. Commercial support was provided by Capital One Bank, the Amazon Research Award program, and Open Philanthropy. Further support was provided by the National Science Foundation (IIS-2212182), and by the NSF TRAILS Institute (2229885). Jonas Geiping was supported by the Tübingen AI Center.

References

- Almazrouei, E., Alobeidli, H., Alshamsi, A., Cappelli, A., Cojocaru, R., Debbah, M., Goffinet, E., Heslow, D., Launay, J., Malartic, Q., Noune, B., Pannier, B., and Penedo, G. Falcon-40B: An open large language model with state-of-the-art performance, 2023. URL <https://falconllm.tii.ae/>.
- Bail, C., Pinheiro, L., and Royer, J. Difficulty Of Detecting AI Content Poses Legal Challenges. *Law360*, April 2023.
- Bao, G., Zhao, Y., Teng, Z., Yang, L., and Zhang, Y. Fast-detectgpt: Efficient zero-shot detection of machine-generated text via conditional probability curvature. In *The Twelfth International Conference on Learning Representations*, 2023.
- Bhat, M. M. and Parthasarathy, S. How Effectively Can Machines Defend Against Machine-Generated Fake News? An Empirical Study. In *Proceedings of the First Workshop on Insights from Negative Results in NLP*, pp. 48–53, Online, November 2020. Association for Computational Linguistics. doi: 10.18653/v1/2020.insights-1.7. URL <https://aclanthology.org/2020.insights-1.7>.
- Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D. M., Wu, J., Winter, C., Hesse, C., Chen, M., Sigler, E., Litwin, M., Gray, S., Chess, B., Clark, J., Berner, C., McCandlish, S., Radford, A., Sutskever, I., and Amodei, D. Language Models are Few-Shot Learners. In *34th Conference on Neural Information Processing Systems (NeurIPS 2020)*, December 2020. URL <https://papers.nips.cc/paper/2020/hash/1457c0d6bfbcb4967418bfb8ac142f64a-Abstract.html>.
- Chakraborty, S., Bedi, A. S., Zhu, S., An, B., Manocha, D., and Huang, F. On the Possibilities of AI-Generated Text Detection. *arxiv:2304.04736[cs]*, April 2023. doi: 10.48550/arXiv.2304.04736. URL <http://arxiv.org/abs/2304.04736>.
- Chen, C., Borgeaud, S., Irving, G., Lespiau, J.-B., Sifre, L., and Jumper, J. Accelerating Large Language Model Decoding with Speculative Sampling. *arxiv:2302.01318[cs]*, February 2023. doi: 10.48550/arXiv.2302.01318. URL <http://arxiv.org/abs/2302.01318>.
- Chowdhery, A., Narang, S., Devlin, J., Bosma, M., Mishra, G., Roberts, A., Barham, P., Chung, H. W., Sutton, C., Gehrmann, S., Schuh, P., Shi, K., Tsvyashchenko, S., Maynez, J., Rao, A., Barnes, P., Tay, Y., Shazeer, N., Prabhakaran, V., Reif, E., Du, N., Hutchinson, B., Pope, R., Bradbury, J., Austin, J., Isard, M., Gur-Ari, G., Yin, P., Duke, T., Levskaya, A., Ghemawat, S., Dev, S., Michalewski, H., Garcia, X., Misra, V., Robinson, K., Fedus, L., Zhou, D., Ippolito, D., Luan, D., Lim, H., Zoph, B., Spiridonov, A., Sepassi, R., Dohan, D.,

- Agrawal, S., Omernick, M., Dai, A. M., Pillai, T. S., Pel-lat, M., Lewkowycz, A., Moreira, E., Child, R., Polozov, O., Lee, K., Zhou, Z., Wang, X., Saeta, B., Diaz, M., Firat, O., Catasta, M., Wei, J., Meier-Hellstern, K., Eck, D., Dean, J., Petrov, S., and Fiedel, N. PaLM: Scaling Language Modeling with Pathways. *arXiv:2204.02311 [cs]*, April 2022. URL <http://arxiv.org/abs/2204.02311>.
- Crothers, E., Japkowicz, N., and Viktor, H. Machine Generated Text: A Comprehensive Survey of Threat Models and Detection Methods. *arxiv:2210.07321[cs]*, November 2022. doi: 10.48550/arXiv.2210.07321. URL <http://arxiv.org/abs/2210.07321>.
- Dhaini, M., Poelman, W., and Erdogan, E. Detecting ChatGPT: A Survey of the State of Detecting ChatGPT-Generated Text. *arxiv:2309.07689[cs]*, September 2023. doi: 10.48550/arXiv.2309.07689. URL <http://arxiv.org/abs/2309.07689>.
- EssayForum. Nid989/EssayFroum-Dataset · Datasets at Hugging Face, September 2022. URL <https://huggingface.co/datasets/nid989/EssayFroum-Dataset>.
- Gehrmann, S., Strobelt, H., and Rush, A. GLTR: Statistical detection and visualization of generated text. In Costajussà, M. R. and Alfonseca, E. (eds.), *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics: System Demonstrations*, pp. 111–116, Florence, Italy, July 2019. Association for Computational Linguistics. doi: 10.18653/v1/P19-3019. URL <https://aclanthology.org/P19-3019>.
- Ghosal, S. S., Chakraborty, S., Geiping, J., Huang, F., Manocha, D., and Bedi, A. S. Towards possibilities & impossibilities of ai-generated text detection: A survey. *arXiv preprint arXiv:2310.15264*, 2023.
- Guo, B., Zhang, X., Wang, Z., Jiang, M., Nie, J., Ding, Y., Yue, J., and Wu, Y. How Close is ChatGPT to Human Experts? Comparison Corpus, Evaluation, and Detection. *arxiv:2301.07597[cs]*, January 2023. doi: 10.48550/arXiv.2301.07597. URL <http://arxiv.org/abs/2301.07597>.
- Hamborg, F., Meuschke, N., Breiteringer, C., and Gipp, B. news-please: A generic news crawler and extractor. In *Proceedings of the 15th International Symposium of Information Science*, pp. 218–223, March 2017. doi: 10.5281/zenodo.4120316.
- Helm, H., Priebe, C. E., and Yang, W. A Statistical Turing Test for Generative Models. *arxiv:2309.08913[cs]*, September 2023. doi: 10.48550/arXiv.2309.08913. URL <http://arxiv.org/abs/2309.08913>.
- Hermann, K. M., Kočíský, T., Grefenstette, E., Espeholt, L., Kay, W., Suleyman, M., and Blunsom, P. Teaching machines to read and comprehend. In *Proceedings of the 28th International Conference on Neural Information Processing Systems - Volume 1*, NIPS’15, pp. 1693–1701, Cambridge, MA, USA, December 2015. MIT Press.
- Horne, B. D., Nørregaard, J., and Adali, S. Robust fake news detection over time and attack. *ACM Trans. Intell. Syst. Technol.*, 11(1), dec 2019. ISSN 2157-6904. doi: 10.1145/3363818. URL <https://doi.org/10.1145/3363818>.
- Hu, X., Chen, P.-Y., and Ho, T.-Y. RADAR: Robust AI-Text Detection via Adversarial Learning. *arxiv:2307.03838[cs]*, July 2023. doi: 10.48550/arXiv.2307.03838. URL <http://arxiv.org/abs/2307.03838>.
- Kirchenbauer, J., Geiping, J., Wen, Y., Katz, J., Miers, I., and Goldstein, T. A Watermark for Large Language Models. In *Proceedings of the 40th International Conference on Machine Learning*, pp. 17061–17084. PMLR, July 2023. URL <https://proceedings.mlr.press/v202/kirchenbauer23a.html>.
- Krishna, K., Song, Y., Karpinska, M., Wieting, J., and Iyyer, M. Paraphrasing evades detectors of AI-generated text, but retrieval is an effective defense. *arxiv:2303.13408[cs]*, March 2023. doi: 10.48550/arXiv.2303.13408. URL <http://arxiv.org/abs/2303.13408>.
- Leviathan, Y., Kalman, M., and Matias, Y. Fast Inference from Transformers via Speculative Decoding. In *Proceedings of the 40th International Conference on Machine Learning*, pp. 19274–19286. PMLR, July 2023. URL <https://proceedings.mlr.press/v202/leviathan23a.html>.
- Li, J. S., Monaco, J. V., Chen, L.-C., and Tappert, C. C. Authorship authentication using short messages from social networking sites. In *2014 IEEE 11th International Conference on e-Business Engineering*, pp. 314–319, 2014. doi: 10.1109/ICEBE.2014.61.
- Li, X. L., Holtzman, A., Fried, D., Liang, P., Eisner, J., Hashimoto, T., Zettlemoyer, L., and Lewis, M. Contrastive Decoding: Open-ended Text Generation as Optimization. In *Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pp. 12286–12312, Toronto, Canada, July 2023. Association for Computational Linguistics. doi: 10.18653/v1/2023.acl-long.687. URL <https://aclanthology.org/2023.acl-long.687>.

- Lian, W., Goodson, B., Pentland, E., Cook, A., Vong, C., and "Teknium". Openorca: An open dataset of gpt augmented flan reasoning traces. <https://https://huggingface.co/Open-Orca/OpenOrca>, 2023.
- Liang, W., Yuksekgonul, M., Mao, Y., Wu, E., and Zou, J. GPT detectors are biased against non-native English writers. *arxiv:2304.02819[cs]*, April 2023. doi: 10.48550/arXiv.2304.02819. URL <http://arxiv.org/abs/2304.02819>.
- Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., Levy, O., Lewis, M., Zettlemoyer, L., and Stoyanov, V. Roberta: A robustly optimized bert pretraining approach, 2019.
- Liyanage, V. and Buscaldi, D. Detecting Artificially Generated Academic Text: The Importance of Mimicking Human Utilization of Large Language Models. In Métais, E., Meziane, F., Sugumaran, V., Manning, W., and Reiff-Marganec, S. (eds.), *Natural Language Processing and Information Systems*, Lecture Notes in Computer Science, pp. 558–565, Cham, 2023. Springer Nature Switzerland. ISBN 978-3-031-35320-8. doi: 10.1007/978-3-031-35320-8_42.
- Mitchell, E., Lee, Y., Khazatsky, A., Manning, C. D., and Finn, C. DetectGPT: Zero-Shot Machine-Generated Text Detection using Probability Curvature. In *Proceedings of the 40th International Conference on Machine Learning*, pp. 24950–24962. PMLR, July 2023. URL <https://proceedings.mlr.press/v202/mitchell123a.html>.
- Pu, J., Huang, Z., Xi, Y., Chen, G., Chen, W., and Zhang, R. Unraveling the Mystery of Artifacts in Machine Generated Text. In *Proceedings of the Thirteenth Language Resources and Evaluation Conference*, pp. 6889–6898, Marseille, France, June 2022. European Language Resources Association. URL <https://aclanthology.org/2022.lrec-1.744>.
- Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., and Sutskever, I. Language Models are Unsupervised Multi-task Learners. *OpenAI*, pp. 24, 2019.
- Raffel, C., Shazeer, N., Roberts, A., Lee, K., Narang, S., Matena, M., Zhou, Y., Li, W., and Liu, P. J. Exploring the limits of transfer learning with a unified text-to-text transformer, 2023.
- Sadasivan, V. S., Kumar, A., Balasubramanian, S., Wang, W., and Feizi, S. Can AI-Generated Text be Reliably Detected? *arxiv:2303.11156[cs]*, March 2023. doi: 10.48550/arXiv.2303.11156. URL <http://arxiv.org/abs/2303.11156>.
- Sen, P., Namata, G., Bilgic, M., Getoor, L., Galligher, B., and Eliassi-Rad, T. Collective Classification in Network Data. *AI Magazine*, 29 (3):93–93, September 2008. ISSN 2371-9621. doi: 10.1609/aimag.v29i3.2157. URL <https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/2157>.
- Solaiman, I., Brundage, M., Clark, J., Askell, A., Herbert-Voss, A., Wu, J., Radford, A., Krueger, G., Kim, J. W., Kreps, S., McCain, M., Newhouse, A., Blazakis, J., McGuffie, K., and Wang, J. Release Strategies and the Social Impacts of Language Models. *arxiv:1908.09203[cs]*, November 2019. doi: 10.48550/arXiv.1908.09203. URL <http://arxiv.org/abs/1908.09203>.
- Su, J., Zhuo, T. Y., Wang, D., and Nakov, P. DetectLLM: Leveraging Log Rank Information for Zero-Shot Detection of Machine-Generated Text. *arxiv:2306.05540[cs]*, May 2023. doi: 10.48550/arXiv.2306.05540. URL <http://arxiv.org/abs/2306.05540>.
- Tang, R., Chuang, Y.-N., and Hu, X. The Science of Detecting LLM-Generated Texts. *arxiv:2303.07205[cs]*, March 2023. doi: 10.48550/arXiv.2303.07205. URL <http://arxiv.org/abs/2303.07205>.
- Tian, E. Gptzero update v1, January 2023a. URL <https://gptzero.substack.com/p/gptzero-update-v1>.
- Tian, E. New year, new features, new model, January 2023b. URL <https://gptzero.substack.com/p/new-year-new-features-new-model>.
- Tian, Y., Chen, H., Wang, X., Bai, Z., Zhang, Q., Li, R., Xu, C., and Wang, Y. Multiscale Positive-Unlabeled Detection of AI-Generated Texts. *arxiv:2305.18149[cs]*, June 2023. doi: 10.48550/arXiv.2305.18149. URL <http://arxiv.org/abs/2305.18149>.
- Touvron, H., Martin, L., Stone, K., Albert, P., Almahairi, A., Babaei, Y., Bashlykov, N., Batra, S., Bhargava, P., Bhosale, S., Bikel, D., Blecher, L., Ferrer, C. C., Chen, M., Cucurull, G., Esiobu, D., Fernandes, J., Fu, J., Fu, W., Fuller, B., Gao, C., Goswami, V., Goyal, N., Hartshorn, A., Hosseini, S., Hou, R., Inan, H., Kardas, M., Kerkez, V., Khabsa, M., Kloumann, I., Korenev, A., Koura, P. S., Lachaux, M.-A., Lavril, T., Lee, J., Liskovich, D., Lu, Y., Mao, Y., Martinet, X., Mihaylov, T., Mishra, P., Molybog, I., Nie, Y., Poulton, A., Reizenstein, J., Rungta, R., Saladi, K., Schelten, A., Silva, R., Smith, E. M., Subramanian, R., Tan, X. E., Tang, B., Taylor, R., Williams, A., Kuan, J. X., Xu, P., Yan, Z., Zarov, I., Zhang, Y., Fan, A., Kambadur,

- M., Narang, S., Rodriguez, A., Stojnic, R., Edunov, S., and Scialom, T. Llama 2: Open Foundation and Fine-Tuned Chat Models. *arxiv:2307.09288[cs]*, July 2023. doi: 10.48550/arXiv.2307.09288. URL <http://arxiv.org/abs/2307.09288>.
- Tulchinskii, E., Kuznetsov, K., Kushnareva, L., Cherniavskii, D., Barannikov, S., Piontkovskaya, I., Nikolenko, S., and Burnaev, E. Intrinsic Dimension Estimation for Robust Detection of AI-Generated Texts. *arxiv:2306.04723[cs]*, June 2023. doi: 10.48550/arXiv.2306.04723. URL <http://arxiv.org/abs/2306.04723>.
- Turnitin.com. URL <https://www.turnitin.com/>.
- Varshney, L. R., Shirish Keskar, N., and Socher, R. Limits of Detecting Text Generated by Large-Scale Language Models. In *2020 Information Theory and Applications Workshop (ITA)*, pp. 1–5, February 2020. doi: 10.1109/ITA50056.2020.9245012.
- Vasilatos, C., Alam, M., Rahwan, T., Zaki, Y., and Maniatakos, M. HowkGPT: Investigating the Detection of ChatGPT-generated University Student Homework through Context-Aware Perplexity Analysis. *arxiv:2305.18226[cs]*, June 2023. doi: 10.48550/arXiv.2305.18226. URL <http://arxiv.org/abs/2305.18226>.
- Verma, V., Fleisig, E., Tomlin, N., and Klein, D. Ghostbuster: Detecting Text Ghostwritten by Large Language Models. *arxiv:2305.15047[cs]*, May 2023. doi: 10.48550/arXiv.2305.15047. URL <http://arxiv.org/abs/2305.15047>.
- Wang, Y., Mansurov, J., Ivanov, P., Su, J., Shelmanov, A., Tsvigun, A., Whitehouse, C., Afzal, O. M., Mahmoud, T., Aji, A. F., and Nakov, P. M4: Multi-generator, Multi-domain, and Multi-lingual Black-Box Machine-Generated Text Detection. *arxiv:2305.14902[cs]*, May 2023. doi: 10.48550/arXiv.2305.14902. URL <http://arxiv.org/abs/2305.14902>.
- Wolff, M. and Wolff, S. Attacking Neural Text Detectors. *arxiv:2002.11768[cs]*, January 2022. doi: 10.48550/arXiv.2002.11768. URL <http://arxiv.org/abs/2002.11768>.
- Yang, X., Cheng, W., Petzold, L., Wang, W. Y., and Chen, H. DNA-GPT: Divergent N-Gram Analysis for Training-Free Detection of GPT-Generated Text. *arxiv:2305.17359[cs]*, May 2023a. doi: 10.48550/arXiv.2305.17359. URL <http://arxiv.org/abs/2305.17359>.
- Yang, X., Cheng, W., Wu, Y., Petzold, L., Wang, W. Y., and Chen, H. Dna-gpt: Divergent n-gram analysis for training-free detection of gpt-generated text, 2023b.
- Yu, X., Qi, Y., Chen, K., Chen, G., Yang, X., Zhu, P., Zhang, W., and Yu, N. GPT Paternity Test: GPT Generated Text Detection with GPT Genetic Inheritance. *arxiv:2305.12519[cs]*, May 2023. doi: 10.48550/arXiv.2305.12519. URL <http://arxiv.org/abs/2305.12519>.
- Zellers, R., Holtzman, A., Rashkin, H., Bisk, Y., Farhadi, A., Roesner, F., and Choi, Y. Defending Against Neural Fake News. In *Advances in Neural Information Processing Systems*, volume 32. Curran Associates, Inc., 2019. URL <https://proceedings.neurips.cc/paper/2019/hash/3e9f0fc9b2f89e043bc6233994dfcf76-Abstract.html>.
- Zhan, H., He, X., Xu, Q., Wu, Y., and Stenetorp, P. G3Detector: General GPT-Generated Text Detector. *arxiv:2305.12680[cs]*, May 2023. doi: 10.48550/arXiv.2305.12680. URL <http://arxiv.org/abs/2305.12680>.

A. Appendix

A.1. Experimental Details

A.1.1. DATASET GENERATION

Using human-written samples from CC News, CNN and Pubmed datasets, we prompt LLaMA-2-13B and Falcon-7B to generate corresponding machine text. To do so, we peel off the first 50 tokens of each human sample and use it as a prompt to generate up to 512 tokens of machine output. We then remove the human prompt from the generation and only use the purely machine-generated text in our machine-text datasets.

A.1.2. OUT OF DOMAIN THRESHOLD TUNING

As motivated in section 4.2, we evaluate detectors True-Positive-Rate while operating under ultra-low False-Positive Rate (TRP@ 0.01%FPR). This metric, like AUC, is threshold-agnostic that captures the discrimination power at the desired low False-Positive Rate of the respective method. When presenting F1-Score (fig. 9), Recall and Precision (fig. 4, 5, 6), and False Negative Rate (fig. 8) we use a purely “out-of-domain” tuned threshold to separate machine and human text.

We set the threshold using the combination of training splits from all of our reference datasets: News, Creative Writing, and Student Essay datasets from Verma et al. (2023), which are generated using ChatGPT. We also compare detectors on LLaMA-2-13B and Falcon-7B generated text with prompts from CC News, CNN, and PubMed datasets. All of these datasets have an equal number of human and machine-generated text samples. We optimize using accuracy and fix our threshold globally using these datasets. For all datasets, we use prefix of 512 tokens for each document, unless explicitly mentioned otherwise.

In order to meet the “out-of-domain” claim when evaluating News, Creative Writing, and Student Essay datasets by Ghostbuster paper (Verma et al., 2023) we do not include them in the threshold determination and only use tune threshold on from CC News, CNN, and PubMed (generated via LLaMA and Falcon).

A.1.3. BASELINE DETAILS

As described in the section 1, we choose baselines with emphasis on post-hoc, out-of-domain (zero-shot), and black-box detection scenarios. These open source detector Ghostbuster (Verma et al., 2023), the commercially deployed GPTZero⁵, DetectGPT (Mitchell et al., 2023) and its efficient version Fast-DetectGPT (Bao et al., 2023) and DNA-GPT (Yang et al., 2023b) to compare detection performance across various datasets in Section 4.

We use out-of-domain version of all of these baselines (applicable only for Ghostbuster) for a fair comparison with our method. If a threshold is provided with original work, we use it for hard prediction otherwise we optimize threshold identical to our method on same datasets for fair and identical comparison.

For DetectGPT, we use LLaMA-2-13B for scoring and T5 model (Raffel et al., 2023) for mask filling for all datasets (even ones generated using LLaMA-2-13B). For Fast-DetectGPT, as described in original work, we use GPT-J-6B and GPT-Neo-2.7B for reference and scoring models respectively for all datasets. We use *gpt-3.5-turbo-instruct* API (March 2024) for suffix prediction in DNA-GPT implementation. GPTZero, a closed sourced API, was queried in September 2023 for our experiments.

A.2. Benchmark Performance

ChatGPT Text Detection. F1-scores on ChatGPT dataset released by (Verma et al., 2023). The numbers for Zero-Shot baseline method are taken from the same work.

A.3. Ablation Studies

Comparison to Other Scoring Model Pairs.

String Length. Is there a correlation between *Binoculars* score and sequence length? Such correlations may create a bias towards incorrect results for certain lengths. In Figure 10, we show the joint distribution of token sequence length and *Binocular* score. Sequence length offers little information about class membership.

⁵<https://gptzero.me/>

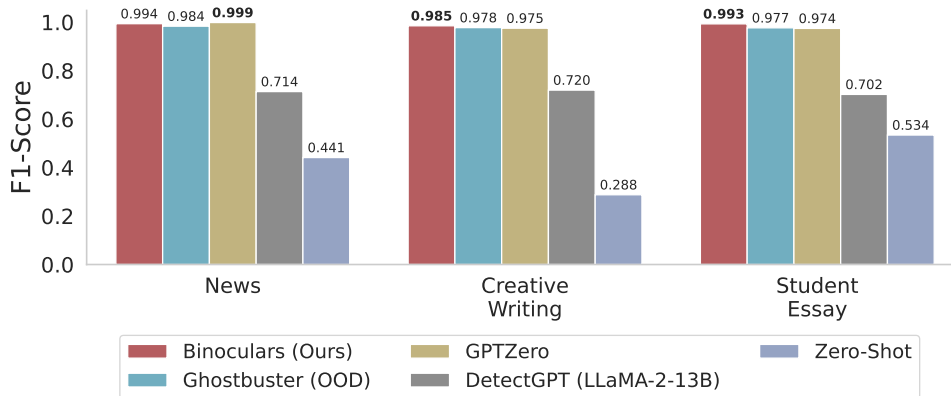


Figure 9. F1 scores for detection of ChatGPT-generated text indicate that several detectors perform similarly. We discuss below how this metric can be a poor indicator of performance at low FPR.

Score Components. Perplexity is used by many detecting formulations in isolation. We show in Figure 11 that both perplexity and cross-perplexity are not effective detectors in isolation. Table 4 show the results where we compute PPL and X-PPL with different model families viz. LLaMA-2 and Falcon.

A.4. Other famous texts

Two songs by Bob Dylan further demonstrate this behavior. *Blowin’ In The Wind*, a famous Dylan track has a much lower Falcon perplexity than his unreleased song *To Fall In Love With You* (logPPL values are 1.11 and 3.30, respectively.) It might be reasonable for famous songs to get classified as machine text and they are more likely output than less famous songs. *Binoculars*, however, labels both of these samples confidently as human samples (with scores of 0.92, and 1.01, respectively).

A.5. Identical Scoring Model

We inspect Binocular’s performance when we choose to use identical \mathcal{M}_1 and \mathcal{M}_1 models in equation (4). We use Falcon-7B and Falcon-7B-Instruct models and compare the two performances with Binoculars Score over dataset by (Verma et al., 2023) in Figure 13. We observe although the vanilla Binoculars score is best over 3 domains, using Falcon-7B as input models is competitive.

A.6. Modified System Prompts

We test Binoculars’ and comparable baselines’ performances in Section 5.4 on multiple prompting strategies. We prompt LLaMA-2-13B-chat with samples from the Open-Orca dataset. In addition to the default sample-specific prompt, we use 3 different versions in which we append instructions into the system prompt. These include instruction to write in the style of Carl Sagan, in a non-robotic tone, and like a pirate. In Table 6 we mention the exact instruction appended to the default system prompts.

A.7. Random Tokens

Next, we also want to test whether arbitrary mistakes, hashcodes, or other kinds of random (and random-seeming) strings bias our model toward false positives. To test the impact of randomness, we generate random sequences of tokens from the Falcon tokenizer and score them with *Binoculars* as usual. We plot a histogram of this distribution in Figure 14. We find that *Binoculars* confidently scores this as human, with a mean score around 1.35 for Falcon (humans have a mean of around 1). This is expected, as trained LLMs are strong models of language and exceedingly unlikely to ever generate these completely random sequences of tokens in any situation. In particular, the generation of these random sequences is even less likely than the generation of perfect human-written text by chance.



Figure 10. A closer look at the actual distribution of scores in terms of sequence length for the Ghostbuster news dataset.

Table 3. Other combinations of scoring models, evaluated on our reference datasets as described in the main body.

PPL Scorer (\mathcal{M}_1)	X-Cross PPL Scorers ($\mathcal{M}'_1, \mathcal{M}_2$)	TPR at 0.01% FPR	TPR at 0.1% FPR	F1-Score	AUC
Falcon-7B-Instruct	Falcon-7B, Falcon-7B-Instruct	100.0000	100.0000	1.0000	1.0000
Llama-2-13B	Llama-13B, Llama-2-13B	99.6539	99.6539	0.9982	0.9999
Llama-2-7B	Llama-7B, Llama-2-7B	99.3079	99.3079	0.9965	0.9998
Llama-2-13B	Llama-13B, Llama-2-13B	98.3549	98.3549	0.9913	0.9997
Falcon-7B-Instruct	Falcon-7B, Falcon-7B-Instruct	98.7200	99.1600	0.9953	0.9996
Falcon-7B-Instruct	Falcon-7B, Falcon-7B-Instruct	94.9200	99.4000	0.9963	0.9996
Llama-2-7B	Llama-7B, Llama-2-7B	95.8441	97.5757	0.9922	0.9996
Llama-2-13B	Llama-13B, Llama-2-13B	98.6400	99.0400	0.9953	0.9995
Llama-2-7B	Llama-7B, Llama-2-7B	98.8000	99.2800	0.9959	0.9995
Llama-2-7B	Llama-7B, Llama-2-7B	98.1600	98.6000	0.9937	0.9992
Llama-2-13B	Llama-13B, Llama-2-13B	98.4000	98.7200	0.9943	0.9992
Falcon-7B-Instruct	Falcon-7B, Falcon-7B-Instruct	94.1125	97.9220	0.9926	0.9992
Falcon-7B-Instruct	Falcon-7B, Falcon-7B-Instruct	93.5000	93.5000	0.9875	0.9990
Falcon-7B-Instruct	Falcon-7B, Falcon-7B-Instruct	92.0000	92.0000	0.9918	0.9990
Llama-2-7B	Llama-7B, Llama-2-7B	94.0000	94.0000	0.9850	0.9989
Llama-2-7B	Llama-7B, Llama-2-7B	98.0000	98.0000	0.9956	0.9988
Falcon-7B-Instruct	Falcon-7B, Falcon-7B-Instruct	72.6957	72.7857	0.9908	0.9988
Llama-2-13B	Llama-13B, Llama-2-13B	97.8750	97.8750	0.9931	0.9987
Llama-2-13B-Chat	Llama-2-13B, Llama-2-13B-Chat	71.3199	82.6799	0.9846	0.9986
Llama-2-13B	Llama-13B, Llama-2-13B	97.5000	97.5000	0.9875	0.9985
Falcon-7B-Instruct	Falcon-7B, Falcon-7B-Instruct	97.5778	97.5778	0.9930	0.9983
Falcon-7B-Instruct	Falcon-7B, Falcon-7B-Instruct	23.3076	48.3732	0.9842	0.9975
Llama-2-13B	Llama-13B, Llama-2-13B	0.3200	32.0800	0.9840	0.9968
Llama-2-13B-Chat	Llama-2-13B, Llama-2-13B-Chat	20.9172	60.0671	0.9763	0.9968
Llama-2-13B	Llama-13B, Llama-2-13B	47.1476	69.2953	0.9747	0.9964

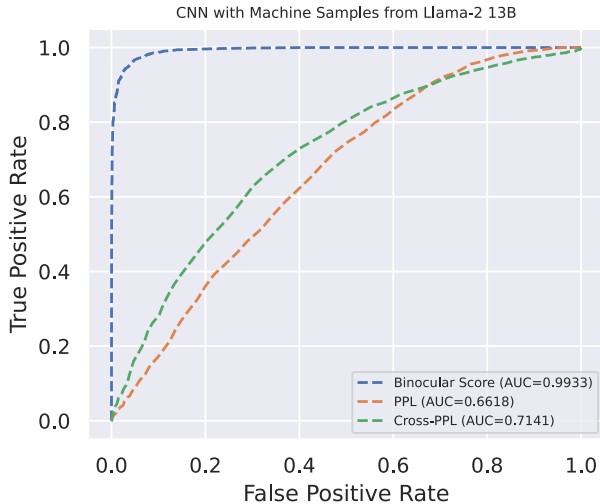


Figure 11. Perplexity and Cross-perplexity are not strong detectors on their own.

A.8. Performer Model Ablation

In this experiment, we aimed to determine the highest-performing model (M_2) to use in the Binoculars setup. In Appendix A.5, we demonstrated that using identical scoring models (Falcon-7B) is not the optimal choice, and Falcon-7B-instruct as performer model yields a better detector. Therefore, we know that instruction tuning does help improve Binoculars’ performance. We fine-tuned Falcon-7B on the Alpaca instruction tuning dataset and used it as the performer model. We benchmark Binoculars’ performance with performers trained at various steps: 0 (identical model case), 1, 10,

Spotting LLMs With Binoculars: Zero-Shot Detection of Machine-Generated Text

Table 4. Over various datasets, we show that perplexity alone or cross-perplexity alone are poor predictors of human versus machine, whereas Binoculars perform well even at low false-positive rates (FPR).

Dataset	Detector	AUC	True Positive Rate			
			@ 0.01% FPR	@ 0.1% FPR	@ 1% FPR	@ 5% FPR
Writing Prompts	Falcon PPL	1.00	0.86	0.86	0.94	0.98
	Falcon X-PPL	0.94	0.56	0.56	0.59	0.79
	LLaMA PPL	0.99	0.86	0.86	0.92	0.98
	LLaMA X-PPL	0.86	0.04	0.04	0.10	0.43
	Binoculars-Falcon	1.00	0.93	0.93	0.96	1.00
	Binoculars-LLaMA	1.00	0.95	0.95	0.98	1.00
News	Falcon PPL	0.99	0.65	0.77	0.90	0.95
	Falcon X-PPL	0.85	0.04	0.12	0.29	0.53
	LLaMA PPL	0.98	0.67	0.71	0.89	0.95
	LLaMA X-PPL	0.26	0.00	0.00	0.00	0.01
	Binoculars-Falcon	1.00	0.95	0.99	1.00	1.00
	Binoculars-LLaMA	1.00	0.99	0.99	1.00	1.00
Essay	Falcon PPL	1.00	0.78	0.78	0.88	0.99
	Falcon X-PPL	0.93	0.25	0.25	0.38	0.70
	LLaMA PPL	0.99	0.42	0.42	0.90	0.98
	LLaMA X-PPL	0.80	0.01	0.01	0.04	0.16
	Binoculars-Falcon	1.00	0.98	0.98	0.99	1.00
	Binoculars-LLaMA	1.00	0.99	0.99	1.00	1.00

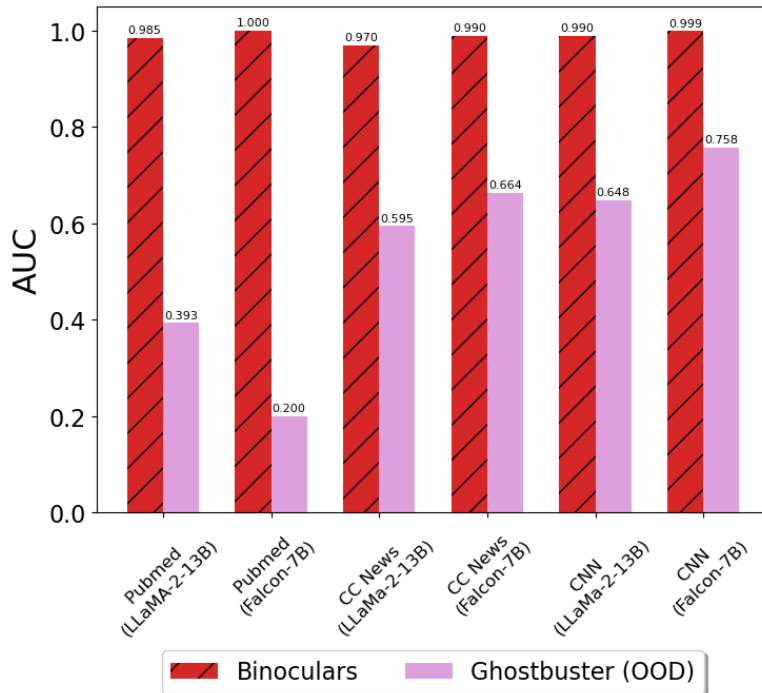


Figure 12. Comparison of Ghostbuster and Binoculars AUC on PubMed, CCNews and CNN datasets.

50, 100, 500, and finally using Falcon-7B-instruct (original formulation). We observed that the fully fine-tuned performer (Falcon-7B-Instruct) achieved the best detection performance, and this performance increase was nearly monotonic with instruction fine-tuning.

Experiment Details. We finetune pretrained Falcon-7B on alpaca instruction dataset with $5e-5$ learning rate and 65K tokens batch size (32 samples * 2048 block size) with cosine annealing ratio of 3% on 4 A5000 GPUs using FSDP distributed training.

Table 5. Case Studies of Text Samples likely to be memorized by LLMs.

Human Sample	PPL (Falcon 7B Instruct)	Cross PPL (Falcon 7B, Falcon 7B Instruct)	Binoculars Score	Predicted as Human-Written
US Constitution	0.6680	0.8789	0.7600	✗
“I have a dream speech”	1.0000	1.2344	0.8101	✗
Snippet from Cosmos series	2.3906	2.8281	0.8453	✗
Blowin’ In the Wind (song)	1.1172	1.2188	0.9167	✓
Oscar Wilde’s quote	2.9219	3.0781	0.9492	✓
Snippet from White Night	2.6875	2.8125	0.9556	✓
Wish You Were Here	2.5000	2.5938	0.9639	✓
Snippet from Harry Potter book	2.5938	2.6875	0.9651	✓
First chapter of A Tale of Two Cities	2.7188	2.7500	0.9886	✓
Snippet from Crime and Punishment	2.8750	2.9063	0.9892	✓
To Fall In Love With You (song)	3.2969	3.2656	1.0096	✓

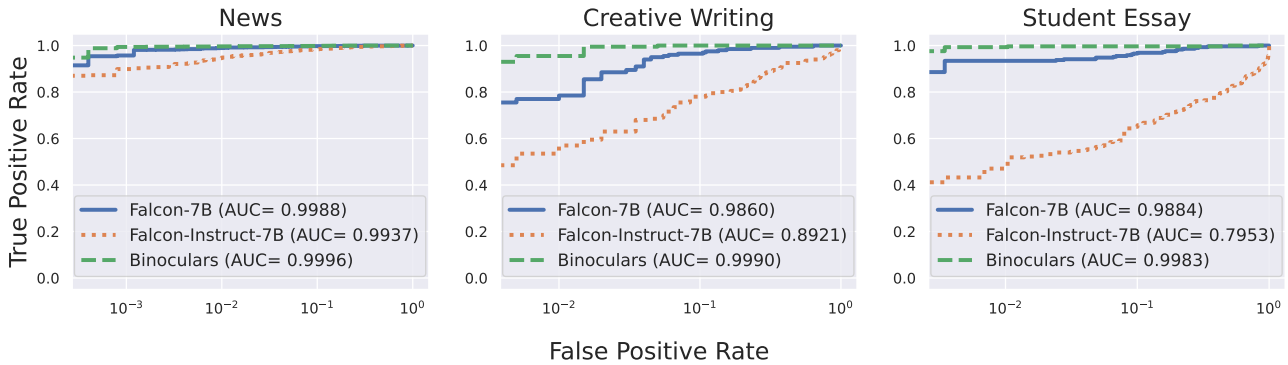


Figure 13. AUC Curve Binoculars score using identical \mathcal{M}_1 and \mathcal{M}_2 models using Falcon-7B and Falcon-7B-Instruct.

Table 6. Instructions appended in system prompts for 3 different strategies.

Prompting Strategy	Instruction appended to the default system prompt
Carl Sagan	Write in the voice of Carl Sagan.
Non-Robotic	Write your response in a way that doesn’t sound pretentious or overly formal. Don’t use robotic-sounding words like ‘logical’ and ‘execute.’ Write in the casual style of a normal person.
Pirate	Write in the voice of a pirate.

A.9. Confidence estimates for Binoculars Performance

We report the standard error on our reported AUC and TPR @ 0.01% FPR in Figure 1 to provide confidence estimates around these figures. We achieve this by creating 20 one-third-sized subsamples from the original set using stratified bootstrapping, ensuring a 50-50 class mix.

A.10. Binoculars Performance on GPT4 and Gemini-Pro

We evaluate Binoculars’ performance on state-of-the-art APIs as of March 2024. We randomly sample instruction and system prompt pairs from the Open Orca dataset and use the GPT-4 and Gemini APIs to generate text. We observe a very low false negative rate for Gemini, while it is considerably high for GPT-4.

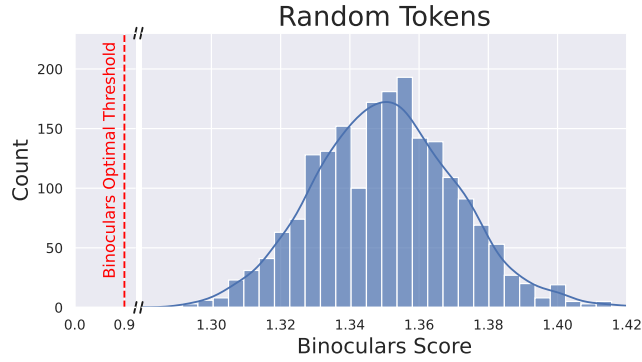


Figure 14. Random token sequences fall strictly on the human side of the Binoculars threshold.

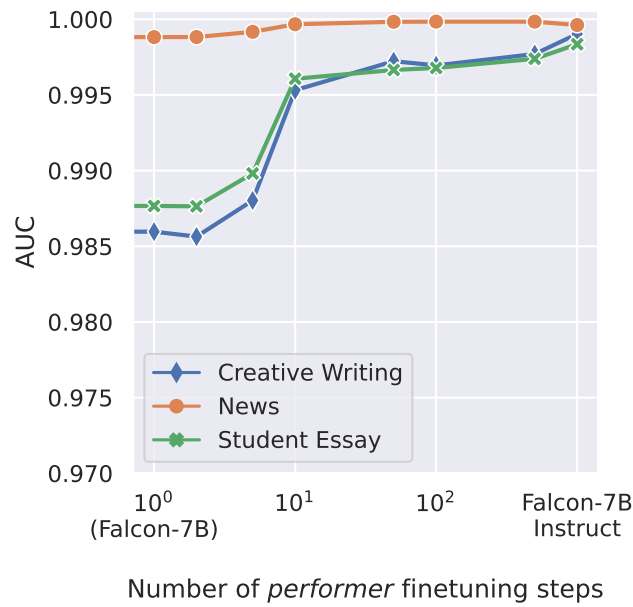


Figure 15. We Find that fully finetuned \mathcal{M}_2 (i.e., Falcon-7B-Instruct) achieves the best performance, while fine-tuning on the instruction dataset (Alpaca) further enhances performance. This experiment complements the findings from Figure 13.

Table 7. Standard error for reported metrics from the main paper.

Dataset Name	AUC	TPR @ 0.01% FPR
News	2.12e-5	2.92e-3
Creative Writing	2.50e-4	2.15e-3
Student Essay	8.99e-5	3.89e-3

Table 8. False negative rate on samples generated by state-of-the-art generation API

API Name	Version	# Correct	# Total	Source	Acc.	False Negative Rate
gemini-1.0-pro-latest	March 2024	125	129	Open Orca	96.89%	3.10%
gpt-4	March 2024	54	129	Open Orca	41.86%	58.13%