On Leakage of Code Generation Evaluation Datasets

Anonymous EMNLP submission

Abstract

 In this paper we consider contamination by code generation test sets, in particular in their use in modern large language models. We dis- cuss three possible sources of such contami- nation and show findings supporting each of 006 them: (i) direct data leakage, (ii) indirect data leakage through the use of synthetic data and (iii) overfitting to evaluation sets during model selection.

 Key to our findings is a new dataset of 161 prompts with their associated python solutions, dataset which we plan to release with this paper under a research license.

⁰¹⁴ 1 Introduction

 Code generation has emerged as an important skill for large language models to master. Measuring re- cent progress in code generation has relied on few, critical benchmarks to judge performance between model families and checkpoints. While many re- cent sophisticated evaluation datasets have been proposed [\(Jain et al.,](#page-4-0) [2024;](#page-4-0) [Jimenez et al.,](#page-4-1) [2024\)](#page-4-1), [t](#page-4-2)he community largely relies on HumanEval [\(Chen](#page-4-2) [et al.,](#page-4-2) [2021\)](#page-4-2) and MBPP [\(Austin et al.,](#page-4-3) [2021\)](#page-4-3) to judge a new model's code capability. In fact, all major announcements in 2023-2024 claiming advanced code capabilities—from academic and industry labs—use at least one of these two datasets. Practi- cally, reporting HumanEval and MBPP is mandatory for a model to report competitive code generation.

 However, the importance of these benchmarks has led to a conflict between popularity and utility. On one side, obtaining competitive numbers comes with significant scientific and economic reward— made increasingly easy with the proliferation of public replicas of these datasets. However, this prevalence has led to data leakage beyond the orig- inal evaluation scope, i.e., *data contamination*, and once this evaluation data *contaminates* model train- ing, the validity of the metrics as a measure of generalization capability becomes unreliable. If a

model has been trained on the same data we use **041** for out-of-distribution generalization (or is selected **042** based on its performance on that data), we break an **043** implicit tenet of how model capability can be mea- **044** sured. We argue that understanding the effect of $\qquad \qquad 045$ contamination is critical to accurately interpreting **046** scores on these benchmarks. 047

In this paper, we review the evidence that these **048** two benchmarks have contaminated most large **049** LLMs, which we define as any procedure that **050** leaked those datasets *during* model training. The **051** most obvious method of contamination is presence **052** inside training data, and we provide evidence that **053** it is highly probably that this occurs at a scale too **054** large to be avoidable. A second possibility is that **055** contamination happens indirectly through the use **056** of synthetic data—a widespread paradigm used in **057** particular to increase code capabilities by gener- **058** ating additional code training tokens. Finally, we **059** argue that final model selection might have been **060** overly influenced by their performance on these **061** datasets, overfitting to performance on these met- **062** rics over general-purpose code-oriented skills. **063**

To measure this contamination, we propose Less **064** Basic Python Problems (LBPP), a code generation **065** benchmark similar to HumanEval and MBPP in style **066** and scale, but more difficult. LBPP is similarly **067** portable, but is produced in a manner to reduce **068** any likelihood of leakage into present code training **069** data. We contribute LBPP to act as a genuinely **070** held-out test set to measure *current* code generation **071** capability, and potential overfitting to HumanEval **072** and MBPP. **073**

2 Related Work **⁰⁷⁴**

[H](#page-4-3)umanEval [\(Chen et al.,](#page-4-2) [2021\)](#page-4-2) and MBPP [\(Austin](#page-4-3) **075** [et al.,](#page-4-3) [2021\)](#page-4-3) remain the most reported results on **076** public leaderboards, but others similar datasets ex- **077** ist [\(Hendrycks et al.,](#page-4-4) [2021;](#page-4-4) [Li et al.,](#page-4-5) [2022\)](#page-4-5). They **078** consist of short and mostly simple (not program- **079** ming competition level) instructions with comple- **080**

090

 tions in Python. Translation into other program- [m](#page-4-6)ing languages exist for those datasets [\(Muen-](#page-4-6) [nighoff et al.,](#page-4-6) [2023;](#page-4-6) [Cassano et al.,](#page-4-7) [2022\)](#page-4-7), as well as versions with additional tests [\(Liu et al.,](#page-4-8) [2024\)](#page-4-8).

 [\(Jain et al.,](#page-4-0) [2024\)](#page-4-0) proposed a continuously up- dated set of leetcode to improve dataset challenge by including harder and novel (unseen) prompts. [\(Jimenez et al.,](#page-4-1) [2024\)](#page-4-1) aims for challenging software engineering problems, that require understanding of full repositories. In a similar vein, RepoQA^1 RepoQA^1 **and Bug In The Code Stack^{[2](#page-1-1)} focus on understand-** ing long contexts within code tasks. One proposed [s](#page-4-9)olution is to use hidden evaluation sets [\(Zhang](#page-4-9) [et al.,](#page-4-9) [2024\)](#page-4-9), however, these do not allow inspec- tion of failure cases and requires trusting the quality and correctness of an opaque 'black-box' evalua- tion setup. Recently, [Riddell et al.](#page-4-10) [\(2024\)](#page-4-10) ana- lyzed data contamination in popular pretraining 099 datasets: reporting that 12.2% of HumanEval sam- ples are present in The Pile [\(Gao et al.,](#page-4-11) [2020\)](#page-4-11), and 18.9% in The Stack [\(Kocetkov et al.,](#page-4-12) [2022\)](#page-4-12). Differ- ent from our analysis however, they conclude: "we do not find the performance rankings of the models to change with decontaminated results".

¹⁰⁵ 3 Possible sources of contamination

106 We provide three hypotheses—with evidence for **107** each one—on why existing models might be over-**108** optimized towards existing leaked benchmarks.

109 3.1 Direct data leakage

 The most obvious reason is the simplest: many of the test datasets are of widespread use and the simplest answer might be that modern LLMs are just trained on this evaluation data. We note that intentional (i.e., to *cheat*) or unintentional contam- ination has the same net effect: training on evalu- ation data limits the confidence and utility of the benchmark results. For code tasks, it is very ex- pensive to curate datasets of natural language to code instructions (one example generally costing several dozen US dollars). For any group aiming to minimize data cost to improve coding performance, the dollar value of creating new datasets can be very high. This leads to a common practice of web scraping code-oriented resources (e.g., GitHub or Stackoverflow) for data. However, these resources are also likely sources of contamination. Since

[bug-in-the-code-stack](https://github.com/HammingHQ/bug-in-the-code-stack)

the release of HumanEval and MBPP in 2021 these **127** datasets have been branched, re-used and copied all **128** across the Internet. The small data size and porta- **129** bility of such benchmarks encourages replication **130** within code repositories. For example, searching 131 for the prompts from HumanEval on GitHub returns **132** a hit in all cases—the median hits is 99 and the min- **133** imum 43 (see Fig. [2\)](#page-2-0). In many cases, these hits are **134** exact duplicates and indications of a fork of the **135** original dataset. **136**

While decontamination of training sets is becom- **137** ing more common, present decontamination filters **138** designed for natural text adapts poorly to code. **139** To operate efficiently at scale, most filters rely on **140** generic deduplication algorithms e.g., such as n- **141** gram matching or hashing functions [\(Lee et al.,](#page-4-13) **142** [2022\)](#page-4-13). Such surface-level matching does not ad- **143** equately capture code similarity where a simple **144** variable name change leaves program semantics un- **145** changed, but changing a single keyword can have **146** profound changes.[3](#page-1-2) The same shortcomings of de- **¹⁴⁷** contamination efforts apply to the creation of large- **148** scale synthetic datasets: for example the model- **149** generated dataset of Starcoder [\(Li et al.,](#page-4-14) [2023\)](#page-4-14) is **150** decontaminated only by removing exact docstrings **151** or solutions that match HumanEval or MBPP. **152**

The recent exploration of [Riddell et al.](#page-4-10) [\(2024\)](#page-4-10) **153** aims to quantify the proportion of this data leakage **154** in existing datasets using plagiarism tools specifi- **155** cally designed for code. Even when static training **156** datasets are cleaned, contamination may persist. **157** Entities who serve models through an API may **158** encounter these benchmark tasks when evaluated **159** by third party users. When a sample of real model **160** usage is annotated for future training data, sam- **161** ples from benchmark evaluation can leak into fu- **162** ture training corpora. Furthermore, these samples **163** may include subtle phrasing variations and format **164** changes that further complicate heuristic dedupli- **165** cation. In this scenario, a model may easily mem- **166** orize completions to purportedly novel prompts. **167** As evidence of this phenomena, we prompted one **168** popular commercial system with partial prompts **169** from HumanEval that were designed to keep the in- **170** struction under-specified. Table [2](#page-6-0) in the Appendix **171** shows the outcome and evidence that—despite the **172** ambiguity of the prompt—the resulting completion **173** matches exactly the gold solution from the test set **174** of HumanEval. **175**

¹ <https://github.com/evalplus/repoqa>

² [https://github.com/HammingHQ/](https://github.com/HammingHQ/bug-in-the-code-stack)

 ${}^{3}E.g.,$ compare the instruction "return true if the string is a float" with "return true if the string is a verb".

Figure 1: Pass@1 rate of popular datasets and the 161 prompts in LBPP.

Figure 2: Histogram (excluding outliers) of occurrences for HumanEval prompts in public GitHub repositories. Every prompt occurs at least 43 times.

176 3.2 Data leakage through synthetic data

177 The most capable of code language models rely **178** [h](#page-4-15)eavily on the use of synthetic training data [\(Xu](#page-4-15) **179** [et al.,](#page-4-15) [2023;](#page-4-15) [Wei et al.,](#page-4-16) [2023,](#page-4-16) [2024\)](#page-4-17).

 A typical pipeline generally consists of: curat- ing prompts related to code generation, inferring completions with a previously trained LLM, and synthesizing unit tests for relevant prompts using LLMs. Completions that pass the respective unit tests are considered valid code solutions and can be used as future training examples. Alternatively, if a sufficiently powerful model is used, completions might be used as-is.

 evol-instruct for example comprises 110k complex query prompts coupled with completions from numerous closed and open-source models.[4](#page-2-1) It is widely used by many code LLMs such as Wiz- ardCoder [\(Xu et al.,](#page-4-15) [2023\)](#page-4-15). Prior reports [\(Yu et al.,](#page-4-18) [2023,](#page-4-18) page 8), [\(Wei et al.,](#page-4-16) [2023,](#page-4-16) page 4) discuss an apparent high similarity between some of those

191

Figure 3: Histogram of cosine similarities for prompts in HumanEval, MBPP and LBPP relative to two popular synthetic code training datasets. We note the high similarity between most HumanEval prompts to *evolinstruct*, and how LBPP has reduced overall similarity to either training dataset.

examples in evol-instruct and HumanEval. We **196** extend this analysis by studying the similarity be- **197** tween embedded representations of the *prompts*^{[5](#page-2-2)} of 198 HumanEval and MBPP with nearest neighbors from **199** *evol-instruct* and *Starcoder-Instruct*. Fig [3](#page-2-3) high- **200** lights widespread similarity between evaluation **201** data and synthetic training datasets 'Starcoder V2 **202** OSS Instruct' and 'evol instruct'. Even if unin- **203** tentional, this contamination further damages the **204** utility of these benchmarks as a held-out test of **205** code generation capability. **206**

Strikingly, we saw that training on this dataset **207** can increase performance of one of our models **208** by 14 absolute points on HumanEval (from 0.52 **209** $pass@1$ to 0.66), while only by 1 point on MBPP 210 (from 0.52 to 0.53). Inspecting closest neighbours **211** for almost all examples in HumanEval (see exam- **212** ples in Table [3](#page-7-0) in the Appendix)—we identify a se- **213**

⁴Per downloads, the most popular version is a 'lightly decontaminated' version [on HuggingFace here.](https://huggingface.co/datasets/ise-uiuc/Magicoder-Evol-Instruct-110K)

⁵Embedded using Cohere embed $\sqrt{3}$ [\(Team,](#page-4-19) [2024\)](#page-4-19).

214 mantically equivalent version in evol-instruct.

 Even when the original evaluation datasets were not used as inspiration for the creation of the synthetic datasets the simple nature of the eval- uation datasets might make duplication unavoid- able. There are only so many short natural lan- guage prompts describing typical interview-style programming questions that can be used. While synthetically generated prompts may not be ex- plicitly based on provided examples from a given test set in the prompt context, the massive scale of these datasets (238k instances for StarCoder- Instruct prior to deduplication) runs the risk of exhausting the possible number of variations on questions. Table [1](#page-5-0) shows examples where gener- ated prompts are extremely similar to questions in the MBPP test set. Note that despite that similarity training on this dataset did not improve substan-tially performance on MBPP.

233 3.3 Overfitting to test sets

 The exaggerated importance of these benchmarks encourages an incentive structure where model se- lection prioritizes gain on a narrow suite of metrics. While it may be tempting to use such benchmarks as a deciding factor between similar checkpoints, there is weak evidence for these benchmarks cor- relating with 'solving code generation'. While the meaning and measurement of this unscientific ob- jective is subject to constant revision, selecting for optimal HumanEval performance may be akin to p-hacking in other fields. This practice can be justi- fied by assuming that these benchmarks are the new dev sets, while the true test is the usage of users over time. The risk remains however that some models overfit to those test sets more than others, distorting perception on relative performance.

 In order to measure this, we created Less Basic Python Problems (LBPP), a dataset of 161 code completion problems in the style of HumanEval. Human annotators were instructed to create totally fresh problems, which were not solvable by an in-255 ternal model^{[6](#page-3-0)} they had access to. Annotators had competitive programming experience and could use programming books as inspiration, but were in- structed not to copy existing solutions on the Inter- net and not to use any LLMs. All annotators were paid above minimum wage in their respective coun-tries, and all final prompt-completion pairs were

manually reviewed by the authors. This adversarial **262** collection resulted in more difficult problems, with **263** most models solving less than 50% of the dataset. **264** Results on a selection of models are in Table [4](#page-8-0) in **265** the Appendix. **266**

Using this dataset we can correlate the perfor- **267** mances of existing models on them against perfor- **268** mance of the well-known benchmarks. The two 269 plots comparing them to HumanEval and MBPP can **270** be seen in Fig. [1.](#page-2-4) There is a clear correlation on **271** both data-sets, indicating that the public bench- **272** marks are still a valuable target signal. However, **273** when zooming in — in particular for models from **274** the same family — the correlation often becomes **275** negative, which might indicate that the selected **276** checkpoint to release performs better on those pub- **277** lic datasets while under-performing on new data- **278** points. Note in particular in Fig. [1a](#page-2-4) the crowded **279** space between 0.75 and 0.8 of the x-axis (pass $@1$ 280 of HumanEval). Despite very similar performance **281** on that public evaluation set, the numbers of LBPP **282** vary wildly. On the other side, in Fig. [1b](#page-2-4) a verti- **283** cal line can be traced at around 0.38 of LBPP that **284** crosses various points – indicating maybe an overfit **285** to MBPP. **286**

4 Conclusion **²⁸⁷**

We study the cause and effect of data contamina- **288** tion by two popular code generation benchmarks. **289** Our analysis highlights that contamination is likely **290** unavoidable at the LLM scale given the difficulty **291** of filtering every potential permutation of a bench- **292** mark dataset. This insight motivates our contri- **293** bution of a novel code generation benchmark to **294** evaluate contemporary LLMs in a contamination- **295** free setting. We are well aware that our decision to **296** release this dataset will make future leakage impos- **297** sible to control. However, with the context of the **298** fast-paced model development cycles that LLMs **299** are currently undergoing we believe that releasing **300** this increases trustworthiness and usefulness of this **301** dataset. It is conveniently designed to serve as drop- **302** in replacement (or addition) of current evaluation **303** sets. On top of its newness, the more challenging 304 nature of this dataset also allows it to provide more **305** signal for model comparison. **306**

5 Limitations **³⁰⁷**

All the model analysis was done *black-box*, without 308 inspecting the model weights or the training set **309** (excepting the work on synthetic data). There is no **310**

⁶We will update references to internal models in future revisions.

 reason why this dataset will not follow the same path than the two studied here. As mentioned in the Conclusion we believe there is more value in that than in an alternative solution (not releasing or keeping it behind an API access).

³¹⁶ References

- **317** Jacob Austin, Augustus Odena, Maxwell I. Nye, **318** Maarten Bosma, Henryk Michalewski, David Dohan, **319** Ellen Jiang, Carrie J. Cai, Michael Terry, Quoc V. Le, **320** and Charles Sutton. 2021. [Program synthesis with](http://arxiv.org/abs/2108.07732) **321** [large language models.](http://arxiv.org/abs/2108.07732) *CoRR*, abs/2108.07732.
- **322** Federico Cassano, John Gouwar, Daniel Nguyen, Syd-**323** ney Nguyen, Luna Phipps-Costin, Donald Pinckney, **324** Ming-Ho Yee, Yangtian Zi, Carolyn Jane Anderson, **325** Molly Q Feldman, et al. 2022. Multipl-e: A scal-**326** able and extensible approach to benchmarking neural **327** code generation. *arXiv preprint arXiv:2208.08227*.
- **328** Mark Chen, Jerry Tworek, Heewoo Jun, Qiming **329** Yuan, Henrique Ponde de Oliveira Pinto, Jared Ka-**330** plan, Harri Edwards, Yuri Burda, Nicholas Joseph, **331** Greg Brockman, et al. 2021. Evaluating large **332** language models trained on code. *arXiv preprint* **333** *arXiv:2107.03374*.
- **334** Leo Gao, Stella Biderman, Sid Black, Laurence Gold-**335** ing, Travis Hoppe, Charles Foster, Jason Phang, Ho-**336** race He, Anish Thite, Noa Nabeshima, et al. 2020. **337** The pile: An 800gb dataset of diverse text for lan-**338** guage modeling. *arXiv preprint arXiv:2101.00027*.
- **339** Dan Hendrycks, Steven Basart, Saurav Kadavath, Man-**340** tas Mazeika, Akul Arora, Ethan Guo, Collin Burns, **341** Samir Puranik, Horace He, Dawn Song, et al. 2021. **342** Measuring coding challenge competence with apps. **343** *arXiv preprint arXiv:2105.09938*.
- **344** Naman Jain, King Han, Alex Gu, Wen-Ding Li, Fanjia **345** Yan, Tianjun Zhang, Sida Wang, Armando Solar-**346** Lezama, Koushik Sen, and Ion Stoica. 2024. Live-**347** codebench: Holistic and contamination free eval-**348** uation of large language models for code. *arXiv* **349** *preprint arXiv:2403.07974*.
- **350** Carlos E Jimenez, John Yang, Alexander Wettig, **351** Shunyu Yao, Kexin Pei, Ofir Press, and Karthik R **352** Narasimhan. 2024. [SWE-bench: Can language mod-](https://openreview.net/forum?id=VTF8yNQM66)**353** [els resolve real-world github issues?](https://openreview.net/forum?id=VTF8yNQM66) In *The Twelfth* **354** *International Conference on Learning Representa-***355** *tions*.
- **356** Denis Kocetkov, Raymond Li, Loubna Ben Allal, Jia Li, **357** Chenghao Mou, Carlos Muñoz Ferrandis, Yacine Jer-**358** nite, Margaret Mitchell, Sean Hughes, Thomas Wolf, **359** et al. 2022. The stack: 3 tb of permissively licensed **360** source code. *arXiv preprint arXiv:2211.15533*.
- **361** Katherine Lee, Daphne Ippolito, Andrew Nystrom, **362** Chiyuan Zhang, Douglas Eck, Chris Callison-Burch, **363** and Nicholas Carlini. 2022. [Deduplicating training](https://doi.org/10.18653/v1/2022.acl-long.577)

[data makes language models better.](https://doi.org/10.18653/v1/2022.acl-long.577) In *Proceedings* **364** *of the 60th Annual Meeting of the Association for* **365** *Computational Linguistics (Volume 1: Long Papers)*, **366** pages 8424–8445, Dublin, Ireland. Association for **367** Computational Linguistics. **368**

- Raymond Li, Loubna Ben Allal, Yangtian Zi, Niklas **369** Muennighoff, Denis Kocetkov, Chenghao Mou, Marc **370** Marone, Christopher Akiki, Jia Li, Jenny Chim, et al. **371** 2023. Starcoder: may the source be with you! *arXiv* **372** *preprint arXiv:2305.06161*. **373**
- Yujia Li, David Choi, Junyoung Chung, Nate Kushman, **374** Julian Schrittwieser, Rémi Leblond, Tom Eccles, **375** James Keeling, Felix Gimeno, Agustin Dal Lago, **376** et al. 2022. Competition-level code generation with **377** alphacode. *Science*, 378(6624):1092–1097. **378**
- Jiawei Liu, Chunqiu Steven Xia, Yuyao Wang, and Ling- **379** ming Zhang. 2024. Is your code generated by chatgpt **380** really correct? rigorous evaluation of large language **381** models for code generation. *Advances in Neural* **382** *Information Processing Systems*, 36. **383**
- Niklas Muennighoff, Qian Liu, Armel Zebaze, Qinkai **384** Zheng, Binyuan Hui, Terry Yue Zhuo, Swayam **385** Singh, Xiangru Tang, Leandro Von Werra, and **386** Shayne Longpre. 2023. Octopack: Instruction tun- **387** ing code large language models. *arXiv preprint* **388** *arXiv:2308.07124*. **389**
- Martin Riddell, Ansong Ni, and Arman Cohan. 2024. **390** Quantifying contamination in evaluating code gener- **391** ation capabilities of language models. *arXiv preprint* **392** *arXiv:2403.04811*. **393**
- [C](https://huggingface.co/Cohere/Cohere-embed-english-v3.0)ohere Embedding Team. 2024. [Cohere embed-english-](https://huggingface.co/Cohere/Cohere-embed-english-v3.0) **394** [v3.0.](https://huggingface.co/Cohere/Cohere-embed-english-v3.0) **395**
- Yuxiang Wei, Federico Cassano, Yifeng Ding, Naman **396** Jain, Harm de Vries, Leandro von Werra, Arjun Guha, **397** and Lingming Zhang. 2024. [Starcoder2-instruct:](https://huggingface.co/blog/sc2-instruct) **398** [Fully transparent and permissive self-alignment for](https://huggingface.co/blog/sc2-instruct) **399** [code generation.](https://huggingface.co/blog/sc2-instruct) **400**
- Yuxiang Wei, Zhe Wang, Jiawei Liu, Yifeng Ding, and **401** Lingming Zhang. 2023. Magicoder: Source code is **402** all you need. *arXiv preprint arXiv:2312.02120*. **403**
- Can Xu, Qingfeng Sun, Kai Zheng, Xiubo Geng, **404** Pu Zhao, Jiazhan Feng, Chongyang Tao, Qingwei **405** Lin, and Daxin Jiang. 2023. Wizardlm: Empowering **406** large pre-trained language models to follow complex 407 instructions. In *The Twelfth International Conference* **408** *on Learning Representations*. **409**
- Zhaojian Yu, Xin Zhang, Ning Shang, Yangyu Huang, **410** Can Xu, Yishujie Zhao, Wenxiang Hu, and Qiufeng **411** Yin. 2023. Wavecoder: Widespread and versatile **412** enhanced instruction tuning with refined data genera- **413** tion. *arXiv preprint arXiv:2312.14187*. **414**
- Hugh Zhang, Jeff Da, Dean Lee, Vaughn Robinson, **415** Catherine Wu, Will Song, Tiffany Zhao, Pranav Raja, **416** Dylan Slack, Qin Lyu, et al. 2024. A careful exami- **417** nation of large language model performance on grade **418** school arithmetic. *arXiv preprint arXiv:2405.00332*. **419**

⁴²⁰ Appendix

Table 1: Examples of similar prompts from the test set of MBPP found in evol_instruct [\(Xu et al.,](#page-4-15) [2023\)](#page-4-15).

Table 2: Original human evaluation prompts with the completion from a major LLM provider. Table 2: Original human evaluation prompts with the completion from a major LLM provider.

Table 3: Most similar prompt in evol-instruct for a non-handpicked selection of HumanEval prompts. Table 3: Most similar prompt in evol-instruct for a non-handpicked selection of HumanEval prompts.

Table 4: Results of pass@1 rate on the LBPP dataset for a selection of models.