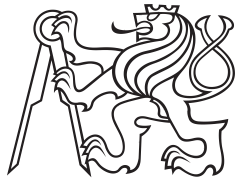


Bachelor Project



**Czech
Technical
University
in Prague**

F3

**Faculty of Electrical Engineering
Artificial Intelligence Center**

Meta-prompts for LLM Prompt Optimization

abcd

Vojtěch Klouda

**Supervisor: Ing. Jan Drchal PhD.
Field of study: Artificial Intelligence
Subfield: Natural Language Processing
May 2025**

Acknowledgements

=)))

Declaration

Prohlašuji, že jsem předloženou práci vypracoval samostatně, a že jsem uvedl veškerou použitou literaturu.

V Praze, 10. May 2025

Abstract

TODO

Keywords: language model,
optimization

Supervisor: Ing. Jan Drchal PhD.
Řesslova 307/9 Praha, E-322

Abstrakt

TODO

Klíčová slova: jazykový model,
optimalizace

Překlad názvu: abcd — abcd

Contents

1 Introduction	1	3 Methodology	27
1.1 Background	2	3.1 Datasets	28
1.2 Objectives	2	3.1.1 External dataset	28
		3.1.2 Custom dataset design	28
2 Literature	5	3.2 Optimization methods	28
2.1 Large Language Models	6	3.2.1 Optimization operators	28
2.1.1 Brief history of NLP approaches	6	3.3 Experimental setup	29
2.2 Prompting techniques	8	4 Experiments	31
2.2.1 Prompt engineering	8	4.1 Comparative analysis of optimization operators	32
2.2.2 Prompting techniques	9	A Bibliography	33
2.3 Optimization methods	13		
2.3.1 Basics	13		
2.3.2 Continuous optimization methods	13		
2.3.3 Discrete optimization methods	13		
2.4 Prompt optimization	14		
2.4.1 Soft prompt tuning	14		
2.4.2 Discrete prompt tuning	14		

Figures

Tables

2.1 Comparison of Zero-shot, One-shot, and Few-shot Prompting	8
--	---



Chapter 1

Introduction

1.1 Background

In recent years large language models (LLMs) emerged as a revolutionary force not only in the field natural language processing (NLP) but in everyday life of the general population [cite smth](#). The fundamental way to interact with these models is via text instructions or **prompts**. These prompts can be standalone or act as templates into which additional information, like a specific task or context, like from a database search, is inserted. This introduces the problem of **prompt engineering**, or finding the optimal prompt for a given situation. Prompt engineering emerges as a largely empirical field, with even experts experienced in the inner workings of LLMs relying on extensive trial-and-error bouts before finding a suitable prompt. With even experts struggling, it is significantly harder for non-experts to design an effective prompt. This motivates the recent research into automated prompt engineering. Several research directions have emerged, such as soft prompt tuning and discrete prompt optimization. Soft prompt tuning is effective but relies on access to inner states of the LLMs which are unavailable when using current state-of-the-art APIs such as the OpenAI API. Furthermore, prompts resulting from soft prompt tuning are often unreadable. In this work we focus on methods of discrete prompt optimization. This problem is very challenging because of the high dimensionality of the language space in which we conduct the search and non-differentiability as there are no gradients in the text space.

1.2 Objectives

The goal of this thesis is to compare several prompt optimization methods utilizing LLMs as the optimizing actors. That means, given a prompt p_t , where t denotes a step in the optimization process, the next prompt can be formulated as $p_{t+1} = \mathcal{L}_{iter}(p_t)$, where \mathcal{L}_{iter} denotes an LLM initialized with specific instructions to facilitate the optimization mapping. The function \mathcal{L}_{iter} is an instance of a general LLM \mathcal{L} and

$$\mathcal{L}_{iter}(p_t) = \mathcal{L}(p_t|m), \quad (1.1)$$

where m denotes the set of instructions, or a prompt, for optimizing p_t . In context of prompt optimization when we are talking about a prompt for optimizing another prompts, we call it a **meta-prompt**. In this case, we can imagine m as

$$m \approx \text{Improve the following prompt \{insert_prompt\}}.$$

By changing the metaprompt, one can easily change the nature of the optimization operator. In the following chapters, we will examine options for designing such operators and compare their performance and effectivity on industry-standard datasets, as well as on a brand new custom dataset.



Chapter 2

Literature

■ 2.1 Large Language Models

■ 2.1.1 Brief history of NLP approaches

The goal of this section is to familiarize the reader with the progress in the Natural Language Processing (NLP) field in the recent decade.

■ Pre-transformer era

Statistical NLP. Data-driven methods such as Hidden Markov models, Conditional Random Fields and Max Entropy models are being used for part-of-speech tagging, named entity recognition, machine translation and speech recognition.

Word embeddings. Algorithms that encode meaning of words in high-dimensional vectors allow models to understand words and relationships between them.

Istm, seq2seq, attention. Attention allows models to connect key parts of input.

■ Transformer era

Attention is all you need. Discovers that simplifying the architecture and focusing on the attention mechanisms allows for much better efficiency in training and paves way for a new era in NLP.

Pre-training+fine-tuning. New paradigm where the language model is first pre-trained on an enormous corpus of data and later fine-tuned for specific tasks, like instruction-tuning for assistants.

multimodality. Visual embedders allow LLMs to understand images. Embeddings are conserved under different modalities ("dog" and a picture of a dog have the same embedding).

Mixture-of-experts (MoE). More efficient architecture that allows for delegating of work to several "expert" submodels, resulting in sparse computation as only a fraction of the model parameters is activated.

Reinforcement learning. Supervised Fine-tuning (SFT) has been combined or sometimes replaced altogether by various forms of Reinforcement learning (RL). Proximal policy optimization based on human or AI feedback is the basis for assistant chat bots such as ChatGPT. Novel RL approaches (GRPO) used to promote reasoning.

Inference-time compute. Development of reasoning models is converging on the idea that letting the model spend more compute time on each answer leads to better results. Using SFT and/or RL the model is taught to "think" or show its "inner monologue" as a part of the answer inside a designated "<think>" tag. When leaving the thought chain, the "</think>" tag can be substituted by an introspective question like "Wait, did I forget something?" resulting in a prolonged thinking chain. potentially catching errors.

Overview of best current models. Current models, with sizes around 1 trillion parameters, match or surpass average human performance on many benchmarks including math and coding.

2.2 Prompting techniques

Prompting techniques encode human priors, making it difficult to assess a language model's intrinsic reasoning abilities [1]

2.2.1 Prompt engineering

In many modern LLM applications, prompts have become programs themselves. [2] Motivation for prompt engineering is to improve the model's capabilities not by changing the underlying weights with training on data but by crafting an optimal instruction string, or a prompt. This can be done by providing examples of the task as a part of the prompt or by instructing the model how to solve the task. In its essence, the model is a left-to-right text completion engine. We can make the analogy with human thinking modes, where it is said that humans have a fast automatic "System 1" mode and a slow and deliberate "System 2" mode [3]. With a good prompt we can shift the model from "System 1" to "System 2".

In-context learning

Prompts are distinguished based on the number of included examples. Research[4]

Prompting Type	Description
Zero-shot Prompting	Prompt has no examples, model relies on its pre-trained knowledge.
One-shot Prompting	Prompt has one example to guide the model.
Few-shot Prompting	Prompt includes a few examples (typically 2 to 5).

Table 2.1: Comparison of Zero-shot, One-shot, and Few-shot Prompting

has shown that with growing model size the knowledge-generalizing ability of the model increases. Instead of expensive fine-tuning models can reuse knowledge from pre-training and solve many tasks when provided just by a few examples.

Few-shot prompting highlights that LLMs can be seen as powerful pattern-completion engines. [5]

Providing a prompt of examples from a distribution can condition the LLM to generate further high-probability examples from that distribution [5]

■ 2.2.2 Prompting techniques

■ Chain-of-thought (CoT)

Principles

Chain of thought = coherent series of intermediate reasoning steps that lead to the final answer for a problem [6]

CoT allows models to allocate additional computation to problems with more reasoning steps (inference-time scaling) [6]

Examples of CoT reasoning in the prompt in a one/few-shot setting to facilitate a reasoning chain response. [6]

CoT prompting is an emergent ability of model scale, does not positively impact performance for small models [6]

CoT can be elicited by prompting techniques - few-shot with steps demonstrations or zero-shot with specific instructions [1]

Few-shot-CoT requires human engineering of multi-step reasoning prompts and their performance deteriorates if prompt example and task question types are unmatched, suggesting high sensitivity to prompt design. [7]

LLMs are decent zero-shot reasoners by adding a simple "Let's think step-by-step" prompt, which is versatile and task-agnostic. Similar prompts that encourage reasoning also improve performance, which leaves the question of how to design better Zero-shot-CoT templates. [7]

Existing work suggest LLMs falter in direct-QA scenarios. [1] Greedy decoding in a direct-QA scenario often does not contain a CoT path, which

may stem from the model’s skewed perception of problem difficulty as it might have been trained on simpler questions [1]

Direct prediction is inaccurate for some inferences because the relevant variables are rarely seen together in training. [8]

Chain-of-thought reasoning improves estimation by incrementally chaining local statistical dependencies that are observed frequently in training. [8]

CoT without prompting

CoT can be elicited by model training or tuning with significant amount of reasoning data [1]

Exploring top-k, $k > 0$ tokens at the first decoding step and continuing with greedy reveals natural CoT reasoning in many cases with the resulting answer having much higher confidence and the decoding path with the highest answer confidence among the top-10 decoding paths contains a CoT path in 88% of the GSM8k samples. CoT-decoding can be easily combined with CoT-prompting or weighted aggregation similar to self-consistency, yielding even larger reasoning gains over multiple language models [1]

Applicability

More performance gains for more complicated problems. [6]

Zero-shot-CoT outperforms simple Zero-shot on arithmetic tasks but does not provide performance gains on commonsense reasoning tasks. [7]

CoT can impact performance on tasks where verbal thinking and deliberation hurts performance in humans but for some it is less clear if they should generalize to LLMs [9]

Tasks where human limitations generalize to LLMs: Implicit statistical learning - 36% performance decrease from gpt-4o to o1-preview Facial recognition, classifying data with patterns and exceptions - performance drops [9]

Tasks where human limitations do not generalize a significant performance

decrease is not seen or performance increases: explaining a logical inconsistency: assumes a reasonable base rate in recognizing logical inconsistencies spatial intuition: consequence of information encoded in visual and motor representations that are likely not available to models aggregating features for a decision, complex, multi-dimensional tasks that exceed human working memory capacity but can easily fit in the context window of an LLM [9]

More advanced inference-time reasoning techniques like ToT alleviate performance a little but still underperform zero-shot. [9]

Self-consistency

Self-consistency aggregates answers from diverse reasoning chains and selects the best one based on majority voting. [10]

It significantly improves accuracy in a range of arithmetic and commonsense reasoning tasks and is useful for collecting rationales and providing uncertainty estimates. [10]

Works with both few-shot and zero-shot CoT. [10]

One limitation of self-consistency is that it incurs more computation cost. Small number of paths is enough, as in most cases the performance saturates quickly. [10]

Reflexion

Reflexion converts binary or scalar feedback from the environment into verbal feedback in the form of a textual summary, which is then added as additional context for the LLM agent, e.g. CoT or ReAct module, in the next episode. [11]

Reflections go into a long-term memory context limited to a sliding window with maximum capacity. [11]

Improves performance over strong baselines on sequential decision making, reasoning and programming tasks. [11]

■ ReAct

Multi-turn prompting technique that forms the basis of agentic LLMs. The model is given a set of tools, such as a Wikipedia search function or a math expression evaluator. The model can go through several steps of using the tools, which generates "observation". The model uses these observations to generate a final answer and leaves the ReAct chain when ready using a "finish" function.

■ Tree-of-thought

Similar to CoT with self-consistency but the reasoning chain is split up into steps creating a tree. This reasoning tree can then be explored using a graph search algorithm such as DFS.

■ 2.3 Optimization methods

■ 2.3.1 Basics

Optimization is the search for the optimum (maximum or minimum) of an arbitrary function. We can divide optimization into two categories based on the nature of the decision variables:

1. continuous
2. discrete.

■ 2.3.2 Continuous optimization methods

Gradient descent, Newton's method, EAs

■ 2.3.3 Discrete optimization methods

Hill-climber, search methods, GAs

■ 2.4 Prompt optimization

Prompt engineering is a language generation task requiring complex reasoning to identify model error's and remedy them by modifying the prompt [12] Creating effective prompts often requires substantial trial-and-error experimentation and deep task-specific knowledge [13] Compile-time optimization is carried out only once before deployment thus amortizing the optimization cost over multiple uses of the prompt program. [2]

■ 2.4.1 Soft prompt tuning

Prompts for models which allow access to gradients, which is not the case for proprietary models accessed via APIs, can be optimized in the high-dimensional embedding space.

This makes the optimization problem continuous. Soft prompts however pose the problem of interpretability and are non-transferable across different LLMs [14].

Continuous prompt-optimization techniques, although effective, require parameters of LLMs inaccessible to black-box APIs and often fall short of interpretability. [15]

■ 2.4.2 Discrete prompt tuning

The area of optimizing prompts discretely while utilizing language models as optimization operators has attracted significant research interest in recent years.

Natural language prompt engineering is particularly interesting because it is a natural interface for humans to communicate with machines, but plain language prompts do not always produce the desired result. [16]

Natural language program synthesis search space is infinitely large. [16]

Discrete tokens are not amenable to gradient-based optimization and brute-force search has an exponential complexity. [14]

Unlike perturbing e.g. network weights continuously which predictably generates small changes in functionality, perturbing code requires discrete changes which often dramatically change functionality. [17] **Reinforcement learning**

Heuristics based on “enumeration (e.g., paraphrasing)-then-selection” do not explore the prompt space systematically [14]

RLPrompt trains a policy network which is inserted as a MLP layer into a frozen compact model. [14]

Agent chooses the next token at each step using the previous tokens according to a learned policy. When the prompt is completed, the agent receives the task reward. [14]

The policy network can also take another inputs, leading to input-specific prompts. [14]

Meta-prompts are flexible but studies lack principled guidelines about their design. [18]

Reproduces key model parameter learning factors - update direction and update method - in LLMs to seek theoretical foundations. [18]

OPRO[19] and APO[20] introduced analogical "gradient" forms. [18]

Analogical momentum forms inspired by the momentum method involve including the optimization trajectory in the meta-prompt. To fit into the context limit and reduce noise, trajectory can be summarized or k most recent/relevant/important gradients can be retrieved. [18]

To mimic effects of learning rate, prompt variation can be limited by edit distance (maximum words to be changed). Warm-up and decay strategies can be applied to this constraint. [18]

New prompt can be created by editing a previous prompt or generate a

new one by following a demonstration. [18]

In an experiment on BBH, authors found that optimization without reflection performs better and the best momentum method being relevance. For prompt variation control, the best combination was cosine decay and no warm-up. [18]

Summarization-based trajectory is less helpful because it tends to only capture common elements. [18]

Task input-output examples are beneficial in the meta-prompt to provide additional context to the LLM to understand the task. [18]

GPT-4 can consistently find better task prompts than GPT-3.5-turbo, which suggests the need for a capable model as the prompt optimizer [18]

Trajectory-based methods perform very well possible because trajectory helps the prompt optimizer pay more attention to the important information instead of the noise in the current step. [18]

APE LLMs are used to construct a good set of candidate solutions by inferring the most likely instructions from input/output demonstrations. [16]

Local search around the best candidates by resampling - asking the LLM to paraphrase the candidate prompt - this however only provides marginal improvements over just choosing the best-performing prompt from instruction induction. [16]

APE was used to improve on Zero-Shot-CoT [7] universal "Let's think by step" prompt on GSM8k.[16]

Prompt to the LLM optimizer is called the meta-prompt and includes previous prompts with their training accuracies sorted in ascending order along with the task description and training set samples. [19]

The main advantage of LLMs for optimization is their ability of understanding natural language, which allows people to describe their optimization tasks without formal specifications. [19]

Motivated by linear regression and TSP and on small-scale traveling salesman problems, OPRO performs on par with some hand-crafted heuristic algorithms. [19]

Optimization stability can be improved by generating multiple solutions when relying on random ICL samples. [19]

To balance between exploration and exploitation, LLM sampling temperature can be tuned. Lower temperature encourages exploitation in the local solution space and higher temperature allows more aggressive exploration of different solutions. [19]

Only the top instructions are kept in the meta-prompt to fit in the LLM context limit. [19]

New outstanding solution is usually found only all the prompts are of similar quality: first all the worse prompts are purged and substituted by a prompt similar to the current best. [19]

Semantically similar instructions have vastly different performance on GSM8k: “Let’s think step by step.” achieves accuracy 71.8, “Let’s solve the problem together.” has accuracy 60.5, while the accuracy of “Let’s work together to solve this problem step by step.” is only 49.4. [19]

Symbolic search With increasing complexity of prompt structure, many prompt optimization techniques are no longer applicable. [2] Symbolic prompt programs (SPPs) can be represented as directed acyclic graphs where nodes are functions (subprograms) and edges indicate call dependencies. [2]

Search space can be defined in two ways, as an enumerative search, where a small number of options is known beforehand, and iterative search, where a large search space is explored with iterative search strategies. [2]

■ Textual gradients

Naturally there are no gradients in the text space but some researchers try to emulate them using reflection-based operators.

APO mirrors the steps of gradient descent within a text-based Socratic dialogue substituting differentiation with LLM feedback and backpropagation with LLM editing [20]

Beam search is an iterative optimization process where in current prompt is expanded into many more candidates in each iteration and a selection process decides which will be used in the next iteration. [20]

Expansion first uses gradients to edit the current prompt and then explores the local monte-carlo search space by paraphrasing the editions [20]

To limit the computation used on evaluating prompts, an approach inspired by best arm identification in bandit optimization is utilized. [20]

Applying previous iterative prompt optimization methods, based on prompt+score pairs, to text generation tasks is challenging due to the lack of effective optimization signals. [21]

Critiques and suggestions, written in natural language, are more helpful for prompt improvement than a single score.[21]

CriSPO uses prompt+score+critique triples for next candidate generation. [21] Unlike APE [20] prompt generation is decoupled from suggestions and a history of critiques and suggestions as packed into the optimizer for a more stable optimization. [21]

CoT is applied in optimization by first asking to compare high-score prompts to low-score ones and draft general ideas. [21]

Critique-based optimization explores a larger space, which is indicated by lower similarity of the prompts in lexicons and semantics.[21]

CriSPO outperforms OPRO [19] both on summarization and QA tasks and metaprompt allows for creating ICL and RAG template prompts. [21]

DSPy optimizers

Most prompt optimizer approaches do not apply to multi-stage LLM programs where we lack gold labels or evaluation metrics for individual LLM

calls. [22]

Proposing a few high-quality instructions is essential due to the intractably large search space. [22]

Uses a surrogate Bayesian optimization model, which is updated periodically by evaluating the program on batches, to sample instructions and demonstrations for each stage of the LLM program [22]

Optimizing demonstrations alone usually yields better performance than just optimizing instructions, but optimizing both yield the best performance. [22]

Optimizing instructions is most valuable for tasks with subtle conditional rules not expressible by a few examples. [22]

For LLM programs, it is beneficial to alternate between optimizing weights (fine-tuning) and optimizing prompts. [23]

■ Evolutionary optimization

There is considerable synergy potential between the fields of evolutionary computation and deep learning. [17]

LLM-based variation operator

LLMs trained on code can suggest intelligent mutations and thus sidestep many of the challenges in evolving programs. [17]

Genetic programming still offers an advantage when the programming task is far from the training distribution of the LLM. [17]

Genetic programming can in principle evolve in any space. [17] **this can be connected with the idea that prompts**

Topic of mutation is guided by previously chosen "commit message" **this is like a pseudogradient**. [17]

Evolution with language models can be used as a way of generating domain data for downstream deep learning where it did not previously exist. [17]

The pattern-completion ability of few-shot prompting can be leveraged to create a form of intelligent evolutionary crossover. [5]

Performance at in-context learning improves with model scale, implying that methods relying upon this capability will benefit from continuing progress in LLM training. [5]

Advent of large, pretrained foundation models marked a significant step in the paradigm of evolutionary recombination with deep generative models, where these new models can be directly leveraged without additional training and allow for searching more abstract spaces. [5]

Next-token prediction naturally lends itself to creating an evolutionary variation operator. [5]

LLM variation operator should be capable of generating meaningful variation for any text representation that has moderate support in the training set, meaning it is basically domain-independent. [5]

LLM crossover acts like an EDA in that it builds a probabilistic model of parents from which the children are sampled. [5]

LLM crossover becomes more similar to an EDA as the number of parents increases. [5]

LLM crossover can express any genetic operator even with small parent sets by fine-tuning or through effective prompting schemes. [5]

Simultaneously evolving the solution along with the LLM and the prompting mechanism could be a powerful paradigm for more open-ended systems. [5]

Input arranged in ascending fitness order prompts the model to generate output that follows an ascending fitness trend. [5]

Evolutionary algorithms have been shown to be effective in search spaces

with millions and billions of variables, which are inaccessible to LLM crossover due to the size of the LLM context window. [5]

The level of stochasticity in LMX can be controlled by the softmax temperature parameter, which can be seen as analogous to a mutation rate parameter in a traditional EA [5]

Frameworks Building upon the inherent ability of LLMs to paraphrase (mutation) and combine (crossover) text, an interesting intersection of traditional evolutionary algorithms and modern LLMs has formed.

Sequences of phrases can be regarded as gene sequences in typical Evolutionary algorithms. [15]

Considers two widely used EAs: Genetic Algorithm and Differential Evolution with DE outperforming GA on most tasks [15]

ELM uses a MAP-elites Quality Diversity algorithm. [17]

Initial population consists of manually-written prompts to leverage human knowledge as well as some prompts generated by LLMs to reflect the fact that EAs start from random solutions to avoid local optima. [15]

DE-inspired approach builds on the idea that the common elements of the current best prompts need to be preserved [15]

Evoprompt performs best with roulette selection when compared with tournament and random selection. [15]

Similar results are achieved when population is initialized with the best and with random prompts, hinting that the crafted design of initial prompts is not essential. [15]

Previous research optimized zero-shot instructions and examples separately, overlooking their interplay and resulting in sub-optimal performance. [24]

There is a prevailing notion that prompt engineering sacrifices efficiency for performance due to the lengthening of prompts, but PhaseEvo actively shortens the prompts [24]

Current EA applications to prompt optimization suffer from extremely high computational cost and slow convergence speed due to the complexity of the high-dimensional search space. [24]

PhaseEvo alternates between two phases: exploration with evolution operators and exploitation using a feedback "gradient". [24]

TABLE 1 **recreate** compares all 5 operators. [24]

4 phases: initialization - lamarck or manual, local feedback mutation, global evolution with EDA and CR operators, local semantic mutation (paraphrasing) [24]

Candidates for evolution operators are selected based on a "performance vector", combining prompts that do not make the same mistakes. [24]

When the performance improvement with an operator stagnates up to some operator-specific tolerance, the current phase is terminated. [24]

Evolution in phases outperforms random operator selection. [24]

PhaseEvo is the most cost-effective but still needs around 12 iterations and 4000 API calls. [24]

APE [16] ran into problems with diminishing returns and abandoning the iterative approach entirely, Promptbreeder aims to solve this with a diversity-maintaining evolutionary algorithm for self-referential self-improvement of prompts [25]

Prompt optimization techniques utilize the fact that LLMs are effective at generating mutations from examples and can encode human notions of interestingness and can be used to quantify novelty. [25]

Self-referential system should improve the way it is improving, thus Promptbreeder used a "hyper-prompt" to optimize its meta-prompt [25]

Uses a binary tournament genetic algorithm. [25]

Uses a random uniformly sampled mutation operators out of 9 total from 5 broad categories for each replication event. [25]

Zero-order mutation (creating a prompt from task description) generates new task prompts more aligned with the task description in the event the evolution diverges. [25]

LLMs tend to be biased to examples found later in EDA mutation lists. Lying to the LLM and telling it that the prompts are sorted by performance in a descending order improves diversity. [25]

Removing any self-referential operator in ablation is harmful under nearly all circumstances [25]

Prior works do not provide sufficient guidance in the meta-prompt. [12]

PE2 improves on APE and APO with a back-tracking search procedure and a more complete metaprompt with a two-step task description, prompt layout specification and a step-by-step reflection template. [12]

Experiments with step size and momentum and also a prompt engineering tutorial in the metaprompt to mixed results. [12]

Optimized prompts do not seem to be generalizable across different models. [12]

Gold-agnostic methods

Current prompt optimization methods often depend heavily on external references for evaluation which are often unavailable or impractical to define in many applications, especially for open-ended tasks [13] Gold-agnostic evaluation is important because we ultimately expect LLMs to solve problems for which answers are not already known [26]

Two primary sources can be used for evaluation: LLM-generated outputs and task-specific truths. These can then be evaluated using either a predefined metric, LLM-as-a-judge or by a human judge to produce an optimization signal based on a numeric score or a textual feedback. [13]

In each iteration, SPO generates new prompts, executes them, and performs pair-wise evaluations of outputs to assess their adherence [13]

SPO achieves high efficiency, requiring only 8 LLM calls per iteration with three samples, significantly lower than existing methods [13]

Outputs of LLMs inherently contain rich quality information that directly reflects prompt effectiveness [13]

LLMs exhibit human-like task comprehension [13]

With score-based feedback a large sample size is needed to ensure scoring stability, which can be avoided by pairwise comparison of outputs [13]

LLM-as-a-judge biases do not affect the overall optimization trend because eval’s feedback merely serves as a reference for the next round of optimization [13]

While maintaining comparable performance with other ground truth-dependent prompt optimization methods, SPO requires only 1.1% to 5.6% of their optimization costs [13]

Self-consistency can be used as a metric instead of accuracy as correct answers generally exhibit greater self-consistency than incorrect ones. However it can overestimate prompts that produce consistent incorrect answers. [26]

Mutual-consistency refinement refines self-consistency scores based on the self-consistency scores of other prompts [26]

Gold-agnostic evaluation methods like GLaPE are robust metrics akin to accuracy and are able to produce effective prompts similarly to gold-label-based methods like OPRO[19]. [26]

If all prompts produce consistent but incorrect answers it is challenging to discern the error without external resources. This happens in some datasets, leading to diminished correlation between GLaPE and accuracy. [26]

■ Metaprompting

Metaprompting or "prompting to create prompts"

Meta-prompts are task-agnostic, meaning they will return the relevant outputs for an arbitrary task, provided a task description is provided as an input. [27].

It is possible to construct a general-purpose meta-prompt. [27].

Meta-prompts will perform better than standard prompts at executing a wide range of tasks. [27].

In tests meta-generated prompts were ranked as more useful than the baselines as well as producing content that was rated more suitable. [27].



Chapter 3

Methodology

■ 3.1 Datasets

Datasets were chosen according to the following requirements:

1. The task is challenging for modern LLMs using a standard CoT prompt but has non-zero accuracy
2. Complex output (no multiple-choice answers)
3. Easy to check programmatically to avoid human/AI judges

■ 3.1.1 External dataset

We found the Livebench datasets to meet our requirements.

■ 3.1.2 Custom dataset design

Sequences dataset challenges the pattern recognition and algebraic capabilities of the model

■ 3.2 Optimization methods

■ 3.2.1 Optimization operators

Metaprompts that define the transition between optimizer generations.

■ 3.3 Experimental setup

Language model used for solving is gpt-4o-mini. Prompts for the solver model are optimized by the optimized model, for which we use the gpt-4o. To encourage diversity and exploration in the optimization process, a temperature of 0.7 is used for the optimizer model. The solver model uses temperature 0.0 to keep the outputs deterministic.



Chapter 4

Experiments

■ 4.1 Comparative analysis of optimization operators

Appendix A

Bibliography

- [1] X. Wang and D. Zhou, “Chain-of-thought reasoning without prompting,” 2024.
- [2] T. Schnabel and J. Neville, “Symbolic prompt program search: A structure-aware approach to efficient compile-time prompt optimization,” 2024.
- [3] S. Yao, D. Yu, J. Zhao, I. Shafran, T. L. Griffiths, Y. Cao, and K. Narasimhan, “Tree of thoughts: Deliberate problem solving with large language models,” 2023.
- [4] T. B. Brown, B. Mann, N. Ryder, M. Subbiah, J. Kaplan, P. Dhariwal, A. Neelakantan, P. Shyam, G. Sastry, A. Askell, S. Agarwal, A. Herbert-Voss, G. Krueger, T. Henighan, R. Child, A. Ramesh, D. M. Ziegler, J. Wu, C. Winter, C. Hesse, M. Chen, E. Sigler, M. Litwin, S. Gray, B. Chess, J. Clark, C. Berner, S. McCandlish, A. Radford, I. Sutskever, and D. Amodei, “Language models are few-shot learners,” 2020.
- [5] E. Meyerson, M. J. Nelson, H. Bradley, A. Gaier, A. Moradi, A. K. Hoover, and J. Lehman, “Language model crossover: Variation through few-shot prompting,” 2024.
- [6] J. Wei, X. Wang, D. Schuurmans, M. Bosma, B. Ichter, F. Xia, E. Chi, Q. Le, and D. Zhou, “Chain-of-thought prompting elicits reasoning in large language models,” 2023.
- [7] T. Kojima, S. S. Gu, M. Reid, Y. Matsuo, and Y. Iwasawa, “Large language models are zero-shot reasoners,” in *Advances in Neural Information Processing Systems* (S. Koyejo, S. Mohamed, A. Agarwal,

- D. Belgrave, K. Cho, and A. Oh, eds.), vol. 35, pp. 22199–22213, Curran Associates, Inc., 2022.
- [8] B. Prystawski, M. Y. Li, and N. D. Goodman, “Why think step by step? reasoning emerges from the locality of experience,” 2023.
 - [9] R. Liu, J. Geng, A. J. Wu, I. Sucholutsky, T. Lombrozo, and T. L. Griffiths, “Mind your step (by step): Chain-of-thought can reduce performance on tasks where thinking makes humans worse,” 2024.
 - [10] X. Wang, J. Wei, D. Schuurmans, Q. Le, E. Chi, S. Narang, A. Chowdhery, and D. Zhou, “Self-consistency improves chain of thought reasoning in language models,” 2023.
 - [11] N. Shinn, F. Cassano, E. Berman, A. Gopinath, K. Narasimhan, and S. Yao, “Reflexion: Language agents with verbal reinforcement learning,” 2023.
 - [12] Q. Ye, M. Axmed, R. Pryzant, and F. Khani, “Prompt engineering a prompt engineer,” 2024.
 - [13] J. Xiang, J. Zhang, Z. Yu, F. Teng, J. Tu, X. Liang, S. Hong, C. Wu, and Y. Luo, “Self-supervised prompt optimization,” 2025.
 - [14] M. Deng, J. Wang, C.-P. Hsieh, Y. Wang, H. Guo, T. Shu, M. Song, E. P. Xing, and Z. Hu, “Rlprompt: Optimizing discrete text prompts with reinforcement learning,” 2022.
 - [15] Q. Guo, R. Wang, J. Guo, B. Li, K. Song, X. Tan, G. Liu, J. Bian, and Y. Yang, “Connecting large language models with evolutionary algorithms yields powerful prompt optimizers,” 2024.
 - [16] Y. Zhou, A. I. Muresanu, Z. Han, K. Paster, S. Pitis, H. Chan, and J. Ba, “Large language models are human-level prompt engineers,” 2023.
 - [17] J. Lehman, J. Gordon, S. Jain, K. Ndousse, C. Yeh, and K. O. Stanley, “Evolution through large models,” 2022.
 - [18] X. Tang, X. Wang, W. X. Zhao, S. Lu, Y. Li, and J.-R. Wen, “Unleashing the potential of large language models as prompt optimizers: An analogical analysis with gradient-based model optimizers,” 2024.
 - [19] C. Yang, X. Wang, Y. Lu, H. Liu, Q. V. Le, D. Zhou, and X. Chen, “Large language models as optimizers,” 2024.
 - [20] R. Pryzant, D. Iter, J. Li, Y. T. Lee, C. Zhu, and M. Zeng, “Automatic prompt optimization with “gradient descent” and beam search,” 2023.
 - [21] H. He, Q. Liu, L. Xu, C. Shivade, Y. Zhang, S. Srinivasan, and K. Kirchhoff, “Crispo: Multi-aspect critique-suggestion-guided automatic prompt optimization for text generation,” 2024.

- [22] K. Opsahl-Ong, M. J. Ryan, J. Purtell, D. Broman, C. Potts, M. Zaharia, and O. Khattab, “Optimizing instructions and demonstrations for multi-stage language model programs,” 2024.
- [23] D. Soylu, C. Potts, and O. Khattab, “Fine-tuning and prompt optimization: Two great steps that work better together,” 2024.
- [24] W. Cui, J. Zhang, Z. Li, H. Sun, D. Lopez, K. Das, B. Malin, and S. Kumar, “Phaseevo: Towards unified in-context prompt optimization for large language models,” 2024.
- [25] C. Fernando, D. Banarse, H. Michalewski, S. Osindero, and T. Rocktäschel, “Promptbreeder: Self-referential self-improvement via prompt evolution,” 2023.
- [26] X. Zhang, Z. Zhang, and H. Zhao, “Glape: Gold label-agnostic prompt evaluation and optimization for large language model,” 2024.
- [27] A. de Wynter, X. Wang, Q. Gu, and S.-Q. Chen, “On meta-prompting,” 2024.