A Roadmap to Life-long Personalized AI

Yuchen Eleanor Jiang   Wangchunshu Zhou

AIWaves Inc.

Abstract

With artificial general intelligence (AGI) approaching rapidly, one of the most important technical problems of our time is building AI systems to serve *all*, i.e., people with diverse backgrounds, values, needs, and perspectives. We believe this is the key to getting the most out of AGI in a *correct* way, and it would require AI systems to continuously adapt to the diverse and ever-changing characteristics of every user. In this paper, we propose a roadmap to building life-long personalized AI systems, specifically using large language models (LLMs) and language agents as a test bed. We identify and formalize three key technical challenges towards Life-long Personalized AI (LPA): (1) LPA should be able to provide personalized assistance according to the traits of *all* users with diverse characteristics; (2) LPA should be able to continuously adapt to the ever-changing personalities, needs, values, and perspectives of distinct users; and (3) LPA technologies and services should be able to be deployed in an *efficient* way so that the cost of LPA is tractable and worthwhile compared to generic AI systems. We argue that the current efforts in the industry to pursue AGI, including scaling and generic alignment are fundamentally insufficient for building life-long personalized AI systems. We then introduce AI PERSONA, our vision towards lifelong personalized AI. We present the basic ideas of AI PERSONA and the associated infrastructures, as well as a few future directions for lifelong personalization. Finally, we discuss how LPA can help the commercialization and productization of LLMs and AGI systems.

*Corresponding authors: {eleanor,chunshu}@aiwaves.cn

1. Introduction

With the success of scaling large language models (LLMs) (Brown et al., 2020; OpenAI, 2023; Ouyang et al., 2022; Radford et al., 2018, 2019; Touvron et al., 2023a,b), the AI community is able to build models and systems much stronger than ever before. A lot of people believe that artificial general intelligence (AGI) is around the corner (some even believe AGI is already achieved). An important question is: *Are we all good by simply continuing scaling and building stronger models?* We believe the answer is no and there remain at least two fundamental research questions: *safety* and *personalization*. The former, *AI Safety* focuses on the problem of how we can ensure super-powerful AI systems (superintelligence) follow generic human values and intents (Burns et al., 2023; Ganguli et al., 2022), which is often called "superalignment[1]" and is actively studied by research institutes and tech companies including OpenAI, Anthropic, and SSI. On the other hand, *AI Personalization* focuses on ensuring AI systems follow diverse values, intents, and personalities of *every distinct* user from different backgrounds, which is our mission at AIWaves. As illustrated in Figure, scaling compute and data will make AI systems more capable and achieve AGI or superintelligence, AI safety research will make AGI "for good", and efforts on AI personalization will make AGI do good "for everyone". We believe that by combining them together, our community will be able to build AGI for everyone's good.

Currently, scaling has become the common objective of numerous tech companies and research institutes and AI safety is the top priority of a few top AI companies. We argue that AI personalization is a critical next step towards building AGI for everyone's good, however, only a few researchers or companies are focusing on this direction. Through our prior efforts and investigations, we find that AI personalization has become increasingly tractable with the advances on the capabilities and generalization abilities of LLMs. This opens up a new possibility that may make AI personalization even more useful and important than ever before: we can build AI systems that can continuously adapt to the ever-changing intents, characteristics, and values of every user during the interaction with them. We call this new paradigm of AI personalization "**L**ife-long **P**ersonalized **AI**" (LPA).

In this paper, we will formalize the problem definition of life-long personalized AI and identify three key technical challenges of building LPA:

- LPA should be able to provide personalized assistance according to the traits of *all* users with diverse characteristics;
- LPA should be able to continuously adapt to the ever-changing personalities, needs, values, and perspectives of distinct users;
- LPA technologies and services should be able to be deployed in an *efficient* way so that the cost of LPA is tractable and worthwhile compared to generic AI systems.

We discuss the limitations of the current practices for building LLM applications to achieve life-long personalization. We then propose a number of technical solutions from different perspectives including strategies for training, inference, and deployment for building life-long personalized AI systems. By combining these methods, we introduce AI Persona, a framework to efficiently enable life-long personalized AI in real-world applications, as well as the associated training/inference infrastructures. We then discuss a few possible applications of LPA in commercialized products.

[1]https://openai.com/index/introducing-superalignment/

2. Background

The concept of lifelong personalized AI is closely related to two research topics: AI personalization and lifelong learning. We provide a brief overview of these fields as follows:

2.1. AI Personalization

The goal of AI personalization is to adapt machine learning models or systems to the intent and characteristics of distinct users by taking user profiles into consideration. As summarized by Tseng et al. (2024), AI personalization techniques have been widely used in various applications, including recommendation, search, education, healthcare, and dialogue. Traditional methods mostly require training distinct models or features for each user for personalization. This paradigm has achieved great commercial success. However, it is not straightforward to combine traditional AI personalization approaches with the advances in LLMs, which have shown great potential in various applications. Therefore, LLM personalization has become an important research topic. Current practices for LLM personalization can be summarized into two categories: *prompt-based* and *training-based*. Prompt-based methods (Castricato et al., 2024; Wu et al., 2024) leverage the generalization and instruction following ability of LLMs and provide user profiles in the prompts for personalized functions. Training-based methods (Clarke et al., 2024; Jang et al., 2023) instead train different models, or add-on modules such as LoRAs (Hu et al., 2022), for different users.

Despite the effectiveness of current LLM personalization methods in a few use cases, they are still far from ready for achieving lifelong personalization in large-scale real-world production scenarios due to various factors including generality and efficiency. Specifically, existing prompt-based methods rely on hand-crafted prompt templates for different scenarios and thus are not general enough for diverse user intents. They are also incapable of dynamically adjusting user profiles with incoming human-AI interactions. Training-based methods, on the other hand, are mostly incapable of scaling to a large number of users while keeping their personalization ability.

2.2. Lifelong Learning

Lifelong learning is a long-standing goal in the field of AI. It requires an AI system to be continuously updated to new domains or reinforced with new knowledge or experience. Traditional methods for lifelong learning are mostly built upon continual training with regularization methods, memory-augmented methods, or data rehearsal methods. These approaches are mostly incompatible with LLM personalization since most powerful LLMs are closed-sourced and it is impractical to fine-tune separate models for each user in large-scale production scenarios.

3. Towards Life-long Personalized AI

To address the aforementioned limitations, we introduce AI Persona, a framework for practical and scalable lifelong personalized AI. We first introduce the core components in the framework and then describe the infrastructure advances for AI Persona.

3.1. AI Persona

The proposed AI Persona framework unifies the *prompt-based* and *training-based* methods and makes them suitable for lifelong personalization, more general to diverse applications, and more scalable for large-scale production. AI Persona is implemented with a config file consisting of both prompt/agent components and model/module components. AI Persona allows us to define each user's distinct user profile using lightweight YAML or JSON documents, which can be applied in various edge scenarios or as extensions or plugins for other applications.

3.1.1. Prompt/Agent Components

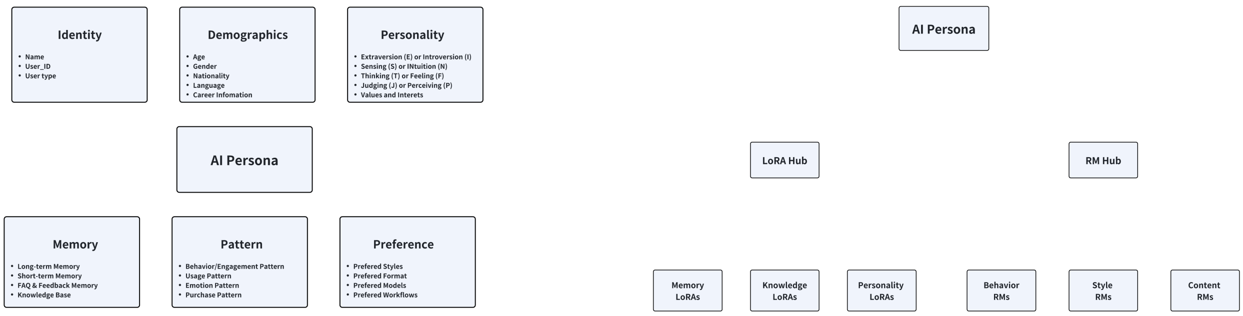

Figure 1 | Illustrations of the AI Persona framework.

As illustrated in the left-hand side of Figure 1, the prompt and agent components in AI Persona consists of 6 fields including identity, demographics, personality, memory, pattern, and preference components. The combination of these components enables AI Persona to *holistically* capture the unique profile of each individual. We provide detailed explanations of each field as follows:

- Identity: critical identity information of users, including their names, user ids, user types, etc.
- Demographics: demographic information of users including the user's gender, age, nationality, native language, location, etc.
- Personality: personality traits of users including their MBTI types, values, interests, and other descriptions for the personality of a user.
- Memory: long-short term memory storing the usage/interaction history of the user. Long-term memory is typically stored in a vector database and the link for the database is stored in AI Persona. In some applications, frequently asked questions or frequently used functions, as well as some feedback or reflections can also be stored in this field.
- Pattern: frequently encountered behavioral and engagement patterns of the user, which helps the AI system to anticipate to possible user reactions and future intents and prepare/plan beforehand.
- Preference: styles, content, formats, and reasoning patterns preferred by the user. In products where a mixture of different LLMs and agents is available, the user's preference for different models and agents can also be provided in this field.

Some possible extensions can also be flexibly defined and added according to actual product requirements by simply adding the keywords in the config files and modifying the prompt templates accordingly.

During inference, the prompt components will be dynamically assembled into a paragraph of user information by a carefully designed prompt template. Other agentic components involving tool usage, e.g., knowledge base search, are annotated with corresponding tools and critical information required for tool usage, e.g., the address or link for the knowledge base. We then combine the assembled user information and the tool usage results with the function-specific prompts for different functionalities in the application with a carefully curated template. The final input will then be fed into an LLM to provide a personalized experience.

3.1.2. Model/Module Components

In addition to prompt and agentic components, AI Persona also integrates training-based personalization approaches. We include both LoRA-based LLM personalization and test-time alignment methods and make a few adaptations for scalable personalization. Specifically, for the LoRA-based method, we pre-train a set of LoRA modules corresponding to different types of knowledge, personalities, and memories and retrieve a mixture of LoRA models using the method described in Zhao et al. (2024) according to the corresponding descriptions in AI Persona. We then merge the retrieved LoRAs according to the weights calculated in the retrieval phrase and use the merged LoRA for personalized inference. Similarly, we pre-train a number of preference models, or reward models, corresponding to behavioral preference, style preference, content preference, etc. Similar to the case in LoRA-based personalization, we retrieve different preference models according to the user profile and perform minimum Bayes-risk (MBR) decoding using the weighted combination of rewards to model the risk. Specifically, the sampling process will be biased towards the direction where the output sequence maximizes the weighted sum of the scores from the preference models.

It is noteworthy that the prompt-based methods and training-based methods are orthogonal to each other and can be applied either separately or combined together. In practice, it is often more practical to start with the prompt-based personalization method for cold start, accumulate enough user data for training a hub of LoRAs and preference models, and then combine with model-based personalization.

3.1.3. Training and Inference Infrastructure

We then describe the training and inference infrastructure we build for lifelong personalized AI and the AI Persona framework. First, to enable lifelong personalization with prompt-based components, we need to be able to constantly update the prompts and tools in the persona of a user with a new usage/interaction history. We adopt the agent symbolic learning framework (Zhou et al., 2024) to update the prompt/agent components in an AI Persona. As for model-based methods, we design a fast-slow adaptation scheme: fast adaption relies on the update in the textual user profile in the prompt components, which leads to different retrieval results of LoRAs and preference models. Slow adaptation, on the other hand, refers to periodical updates of the models.

The aforementioned model-based personalization methods also pose challenges to the LLM inference infrastructure. Specifically, we build LLM inference engines that support associating different LoRAs with different inputs in batched inference and MBR decoding with preference models, and the feature that allows different combinations of preference models for different inputs in a batch.

4. Commercialization of LPA

Finally, we discuss a few potential applications where LPA and AI Persona can be commercialized. We take AI-assisted writing and AI phone OS, two typical cases where LPA has great potential for improving user experience, for case studies.

4.1. Case study: AI-assisted Writing

Conventional AI-assisted writing platforms such as Grammarly and Jasper provide the same services for all users. However, different writers have very different preferences on the style and pattern of AI assistance. To this end, we integrate AI Persona in WawaWriter[2], the creative writing copilot

[2] `https://wawawriter.com/`

developed by AIWaves, which provides personalized writing assistance for professional story writers. AI Persona enables our system to constantly adjust its behavior according to the users' writing history on the platform. For example, our system will automatically infer and update a user's preferences on writing styles and content, which are stored in the AI Persona of the user, according to his/her editing history.

4.2. Case study: AI Phone

Another good testbed of lifelong personalized AI techniques is on smartphones, devices with which people interact the most on a daily basis. The human-phone interaction history and patterns can be effectively captured and used to update AI Persona of users in real-time, resulting in highly informative user profiles. The LPA system will then be able to provide personalized experience for users and shuttle the users according to their intents.

In addition to the two aforementioned case studies, LPA and AI Persona also has great potential for LLM-assisted search, recommendation, education, etc.

5. Discussion

In this paper, we discuss the problem of lifelong personalization of AI systems. We first present a concrete problem definition of lifelong personalized AI and discuss the chances and challenges of achieving lifelong personalization of LLM-based systems. We then present AI Persona, a blueprint towards building lifelong personalized AI systems in large-scale industry-level products. We believe lifelong personalization of AI systems will be an important milestone towards achieving AGI and making human life better.

References

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.

C. Burns, P. Izmailov, J. H. Kirchner, B. Baker, L. Gao, L. Aschenbrenner, Y. Chen, A. Ecoffet, M. Joglekar, J. Leike, I. Sutskever, and J. Wu. Weak-to-strong generalization: Eliciting strong capabilities with weak supervision, 2023.

L. Castricato, N. Lile, R. Rafailov, J.-P. Fränken, and C. Finn. Persona: A reproducible testbed for pluralistic alignment, 2024. URL `https://arxiv.org/abs/2407.17387`.

C. Clarke, Y. Heng, L. Tang, and J. Mars. Peft-u: Parameter-efficient fine-tuning for user personalization, 2024. URL `https://arxiv.org/abs/2407.18078`.

D. Ganguli, L. Lovitt, J. Kernion, A. Askell, Y. Bai, S. Kadavath, B. Mann, E. Perez, N. Schiefer, K. Ndousse, A. Jones, S. Bowman, A. Chen, T. Conerly, N. DasSarma, D. Drain, N. Elhage, S. El-Showk, S. Fort, Z. Hatfield-Dodds, T. Henighan, D. Hernandez, T. Hume, J. Jacobson, S. Johnston, S. Kravec, C. Olsson, S. Ringer, E. Tran-Johnson, D. Amodei, T. Brown, N. Joseph, S. McCandlish, C. Olah, J. Kaplan, and J. Clark. Red teaming language models to reduce harms: Methods, scaling behaviors, and lessons learned, 2022.

E. J. Hu, Y. Shen, P. Wallis, Z. Allen-Zhu, Y. Li, S. Wang, L. Wang, and W. Chen. LoRA: Low-rank adaptation of large language models. In International Conference on Learning Representations, 2022. URL https://openreview.net/forum?id=nZeVKeeFYf9.

J. Jang, S. Kim, B. Y. Lin, Y. Wang, J. Hessel, L. Zettlemoyer, H. Hajishirzi, Y. Choi, and P. Ammanabrolu. Personalized soups: Personalized large language model alignment via post-hoc parameter merging, 2023. URL https://arxiv.org/abs/2310.11564.

OpenAI. GPT4 technical report. arXiv preprint arXiv:2303.08774, 2023.

L. Ouyang, J. Wu, X. Jiang, D. Almeida, C. L. Wainwright, P. Mishkin, C. Zhang, S. Agarwal, K. Slama, A. Ray, J. Schulman, J. Hilton, F. Kelton, L. Miller, M. Simens, A. Askell, P. Welinder, P. Christiano, J. Leike, and R. Lowe. Training language models to follow instructions with human feedback, 2022.

A. Radford, K. Narasimhan, T. Salimans, I. Sutskever, et al. Improving language understanding by generative pre-training. 2018.

A. Radford, J. Wu, R. Child, D. Luan, D. Amodei, I. Sutskever, et al. Language models are unsupervised multitask learners. OpenAI blog, 1(8):9, 2019.

H. Touvron, T. Lavril, G. Izacard, X. Martinet, M.-A. Lachaux, T. Lacroix, B. Rozière, N. Goyal, E. Hambro, F. Azhar, et al. LLaMA: Open and efficient foundation language models. arXiv preprint arXiv:2302.13971, 2023a.

H. Touvron, L. Martin, K. Stone, P. Albert, A. Almahairi, Y. Babaei, N. Bashlykov, S. Batra, P. Bhargava, S. Bhosale, D. Bikel, L. Blecher, C. Canton-Ferrer, M. Chen, G. Cucurull, D. Esiobu, J. Fernandes, J. Fu, W. Fu, B. Fuller, C. Gao, V. Goswami, N. Goyal, A. Hartshorn, S. Hosseini, R. Hou, H. Inan, M. Kardas, V. Kerkez, M. Khabsa, I. Kloumann, A. Korenev, P. S. Koura, M. Lachaux, T. Lavril, J. Lee, D. Liskovich, Y. Lu, Y. Mao, X. Martinet, T. Mihaylov, P. Mishra, I. Molybog, Y. Nie, A. Poulton, J. Reizenstein, R. Rungta, K. Saladi, A. Schelten, R. Silva, E. M. Smith, R. Subramanian, X. E. Tan, B. Tang, R. Taylor, A. Williams, J. X. Kuan, P. Xu, Z. Yan, I. Zarov, Y. Zhang, A. Fan, M. Kambadur, S. Narang, A. Rodriguez, R. Stojnic, S. Edunov, and T. Scialom. Llama 2: Open foundation and fine-tuned chat models. CoRR, abs/2307.09288, 2023b. doi: 10.48550/arXiv.2307.09288. URL https://doi.org/10.48550/arXiv.2307.09288.

Y.-M. Tseng, Y.-C. Huang, T.-Y. Hsiao, W.-L. Chen, C.-W. Huang, Y. Meng, and Y.-N. Chen. Two tales of persona in llms: A survey of role-playing and personalization, 2024. URL https://arxiv.org/abs/2406.01171.

B. Wu, Z. Shi, H. A. Rahmani, V. Ramineni, and E. Yilmaz. Understanding the role of user profile in the personalization of large language models, 2024. URL https://arxiv.org/abs/2406.17803.

Z. Zhao, L. Gan, G. Wang, W. Zhou, H. Yang, K. Kuang, and F. Wu. Loraretriever: Input-aware lora retrieval and composition for mixed tasks in the wild, 2024. URL https://arxiv.org/abs/2402.09997.

W. Zhou, Y. Ou, S. Ding, L. Li, J. Wu, T. Wang, J. Chen, S. Wang, X. Xu, N. Zhang, H. Chen, and Y. E. Jiang. Symbolic learning enables self-evolving agents, 2024. URL https://arxiv.org/abs/2406.18532.