Learning Report

Jiayao Zhang
University of Hong Kong
https://jiayao-zhang.com

Abstract

In this report, the author shared his experience of the research internship (a.k.a. visiting student researcher) at University of California at Berkeley in the Summer of 2018. A particular focus was given to the skills learnt as well as reflections for improvement during the internship throughout the report. We hope this report may not only provide a glimpse to the curious nature of the top schools from another perspective; but of certain help to junior students who wish to participate in activities of similar nature as well. Questions are welcome and should be redirected to the author via <jiayaozhang@{acm,ieee}.org>.

1 Introduction

Located on the northeastern side of the San Francisco Bay Area, the University of California at Berkeley, as the founding university of the University of California system, is widely acknowledged as one of a few top school for computer scientists among the world, and, together with three other top schools, is colloquially referred to as the “Big Four”. In the summer of 2019, the author was fortunate to be a visiting student researcher, jointly funded by HKU’s Undergraduate Research Fellowship Programme (URFP) and Chui’s Students’ Excellence Scheme (CSES), with one of the top faculty members in the EECS department specializing in computer security and privacy, blockchain, and deep learning. Throughout the activity, the author was fortunate to have conversations with rising starts in CS research, to participate in group meetings, to give talk on the work done while visiting UC Berkeley, and to take the chance to explore the Bay Area.

This report is structured as follows. Section 2 discusses work done while visiting UC Berkeley, where we highlight the academic activities participated; Section 3 initiates another thread of inquiry, namely the exploration of the campus culture and the Bay Area in general; finally, we conclude this report by a short discussion on the skills acquired and limitations for improvement during the internship. We also offer a brief outline of suggestions for participating in activities of similar nature, which may be of independent interest.

2 Research Involvements

Paper Collaboration. We first discuss the core of the captioned activities, research, where the main subject of interest is a submissions currently under double-blind review. We do, nonetheless, offer a concise discussion on the background and its formation. We are interested in the evolution of several information-theoretic quantities during deep neural network training. Such quantities are often decent indicators relating to learning-theoretic notions such as the generalization error gap, and sample complexity. Previous work exploring from an information-theoretic perspective often found themselves in a dilemma created by the estimation procedure, which is notoriously hard in high dimensions. Indeed, under practical settings, such quantities might be undefined when one fixes a network as deterministic. We thus propose a novel framework for such maneuver. Although it is true that we rely on certain assumptions, which might be sometimes too good to be true in practice. The theoretical analysis, which leads to a closed-form asymptotic bound on such information-theoretic

Preprint. Work in progress.
quantities, shed light on the endeavours towards a deeper understanding of deep neural nets, a specific point we hope could inspire the community more or less. Of parallel interest, we study the robustness of deep neural networks. Albeit to its unprecedented success in a variety of science and engineering applications such as visual recognition, object localization, natural language processing, etc, deep neural networks are susceptible to adversarial examples, which are input data with well-crafted noises that fool the learning model but are seemingly innocuous to humans. As a vivid, if not ubiquitous, example, first introduced in [GSS15], an image of panda (left, Figure 1), after adding some seemingly random noises (middle, Figure 1), is perceived as the image of the same panda (right, Figure 1) – but fools the network to classify it as a gibbon. The study of robustness of learning models is not only of theoretical interest, but has significant impact into practice. Intuitively, no one wishes the autonomous vehicle thinks a white truck right in front of it as part of the sky and then hits it. Unfortunately, this intuition does not always hold, hence rendering the research on the defence of such adversaries necessary. In our work, we are most interested in an information-theoretic perspective in interpreting those naughty examples.

Reading Group. Unlike paper collaboration, which can be seamlessly implemented in a distant mode, real-time face-to-face discussions, either in the form of formal meetings, less formal reading groups, or informal lunch chats, generally require physical presence. During those meetings, updates from individual researchers, discussions involving recent advances and latest papers, and sharing observations or insights are often involved. The author vividly recall during one of such sessions in which his work was put into strict scrutiny due to lacking of empirical justifications of an overly strong assumption. The process, painful as it might sound at first thought, is a de facto sanity-preserving process that pushes the work into a higher level of precision. At the end of the research internship, the author gave a talk, not short by any standard but hopefully not boring on the other hand, introducing the work done during the visit. The author also wishes to take this chance to thank the audience for their patience for the slides over fifty pages long. During the talk, the author was constantly replying questions from the audience, and found this process to be particularly useful, if not helpful, for both sides: the audience gains a better and possibly in-depth understanding to the work whereas the presenter learns the flaws of the presentation and may improve adaptively.

3 Explorations

Group Hiking. As an integral part of life, exercising regularly keeps one healthy, if done properly, and may possibly relieve stresses generated from a manifold of sources in life continuously. Indeed, hiking to the nearby Berkeley hills is viewed as a convention, if not tradition, of the research group I was with while visiting UC Berkeley. This hike provides a chance for visiting students/scholars, post-docs, doctoral students, and matriculating students to enjoy the bless of nature, the buzz from flying animals of various kinds, and the breeze of intellectual exchange. This occasions was documented in the form of an image, which we present in Figure 2a.

Group Luncheon. To further support the arguments in Section2 we consider a particular instance dining with the group, which we show in Figure 2b. During the luncheon, the author took the opportunity to learn more about the current focus on blockchain research, which is by definition a
sheer new area to the author. This occasion, informal it might be, has indeed deepened the boosting the inter-disciplinary research exchanges, and introduced the author with the exciting area of blockchain.

4 Discussions and Conclusions

In this report, we discussed both the academic and living aspects of the research internship the author had participated in during the Summer of 2018. We gave a brief introduction on the work performed during the internship; the academic activities the author has participated in; and those non-academic activities, which, unsurprisingly, boil down to academic ones. It is hoped that this report would provide the inquisitive audience a short introduction, if not an idiosyncratic stacking of mouthful and sometimes ambiguous vocabularies. As we conclude this report, it might be pedagogical to re-examine the flaws from the captioned activities and offer suggestions for future cohorts, which are summarized into the following list, whose further elaborations are omitted due to conflict of interests.

- Plan early and be proactive.
- Reach faculty members in various schools.
- Be prepared to fail.

Finally, we conclude this writing by recalling a motto from a research scientist, under whom the author has been luckily mentored: have fun, be awesome.

References