Can Go AIs be adversarially robust?

Tom Tseng [1] **Euan McLean** [1] **Tony T. Wang** [*2] **Kellin Pelrine** [*3] **Adam Gleave** [*1]

Abstract

Prior work found that superhuman Go AIs such as KataGo are vulnerable to opponents playing simple adversarial strategies. This shows that superhuman average-case capabilities may not translate to satisfactory worst-case robustness. However, Go AIs were never designed with security in mind, raising the question: can simple defenses make KataGo robust? In this paper, we test three natural defenses: adversarial training on hand-constructed positions, iterated adversarial training, and changing the network architecture. We find these defenses protect against previously discovered attacks, but we uncover several qualitatively distinct adversarial strategies that beat our defended agents. Our results suggest that achieving robustness is challenging, even in narrow domains such as Go. Our code is available at `https://github.com/AlignmentResearch/go_attack`.[†]

1. Introduction

It is essential that AI systems work robustly, especially when deployed at a societal scale or used in safety-critical systems. While *average-case* performance of AI systems is rapidly improving, building systems with good *worst-case* performance remains unsolved. Superhuman Go systems (Wang et al., 2023a) fail severely under adversarial inputs, as do state-of-the-art image classifiers (Liu et al., 2023; Croce et al., 2021) and language models (Zou et al., 2023). This shows that strong average-case capabilities may not lead to robustness: building robust AIs requires a concerted effort.

In this paper, we aim to make KataGo (Wu, 2021c), a state-of-the-art Go AI, robust. Wang et al. (2023a) previously found a "cyclic attack" that beat a superhuman KataGo version 97% of the time, yet loses to human amateurs. Since game-playing AIs like KataGo were not designed with security in mind, we investigate three natural defenses (Figure 1.1). We find these defenses protect KataGo against Wang et al.'s adversary but can be overcome by new attacks.

We first consider a **positional adversarial training** defense (deferred to Appendix E): augmenting KataGo's training data with examples of Wang et al. (2023a)'s cyclic attack. This intervention hardens KataGo against Wang et al. (2023a)'s adversary, yet further training enables that adversary to beat the adversarially trained version of KataGo 91% of the time; we also discover a qualitatively new "gift attack" by training from an earlier adversary checkpoint.

Nonetheless, this first approach shows that training against a known adversary can be effective in defeating a specific, fixed attack. This leads us to our second approach of **iterated adversarial training** (Section 3) that simulates an "arms race" of an adversary continuously searching for new attacks to overcome the victim's defenses and a victim continuously building defenses against new attacks. The resulting victim is robust to Wang et al. (2023a)'s adversary. However, we were still able to train a new attack that defeats this victim 81% of the time using just 5% of the compute used for training the victim.

Systematically exploring all possible adversarial strategies is intractable. Instead, we must rely on the AI learning generalizable representations. The limited generalization observed might suggest a fundamental limitation of the convolutional neural network (CNN) architecture used by KataGo and other leading Go AIs. To test this hypothesis and to try to build a more robust system, we train a new professional-level Go AI using a **vision transformer** (ViT) instead of a CNN (deferred to Appendix G.1). We find the ViT-based agent is less vulnerable to Wang et al.'s original adversary. However, after fine-tuning the original adversary against the ViT agent, the adversary defeats a superhuman version of the ViT agent 78% of the time.

We view building a robust Go AI as a natural starting point for designing robust AI systems more broadly. Go

[*]Equal advising contribution. [1]FAR AI [2]MIT [3]Mila. Correspondence to: Adam Gleave <adam@far.ai>.

Proceedings of the 41st International Conference on Machine Learning, Vienna, Austria. PMLR 235, 2024.

[†]This paper is a shortened, preliminary version of our full paper (Tseng et al., 2024).

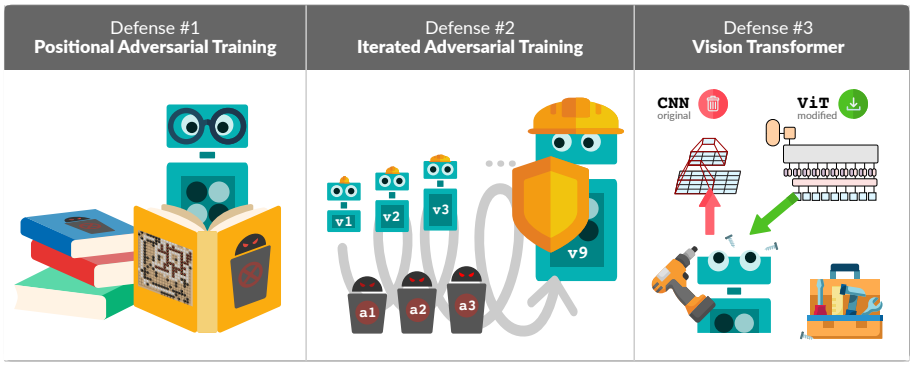


Figure 1.1: The interventions we study to defend Go AIs against adversarial attacks. **Left**: Positional adversarial training involves self-play initialized from adversarial positions for the agent to "study". **Middle**: Iterated adversarial training involves multiple rounds of an adversary finding attacks and a victim building defenses. **Right**: We replace the convolutional neural network (CNN) model with a vision transformer (ViT) to test the hypothesis that the adversarial vulnerability of Go AIs are due to CNNs' inductive biases.

has long driven AI development, with insights from AlphaGo (Silver et al., 2016) being generalized to a wide variety of tasks through algorithms like MuZero (Schrittwieser et al., 2020). At the same time, we expect the narrow domain of Go makes achieving robustness easier than in more open-ended tasks. Furthermore, as Go is a zero-sum or adversarial game with solution concepts like Nash equilibria that minimize exploitability, it should theoretically be possible to be fully robust while maintaining average-case performance. By contrast, in domains like image classification there are fundamental trade-offs between clean and robust accuracy (Tsipras et al., 2019).

Unfortunately, our results suggest that building robust AI systems will be quite challenging. None of our defenses provide a complete solution, even in the narrow domain of Go, and several of the attacks can even be executed by a human (Appendix I). A more extensive redesign is likely needed to build robust AI systems, both in Go and more complex domains. However, our defenses do make attacks more computationally demanding and less effective with higher victim search depth. This suggests that a concerted research effort could develop robust AI that can be relied on in many contexts. The path to this, however, may be orthogonal to that required for impressive average-case capabilities.

2. Background

We follow the threat model of Wang et al. (2023a) set in a two-player zero-sum Markov game (Shapley, 1953). A threat actor trains one of the agents, the "*adversary*," and seeks to win against a "*victim*" agent. The threat actor has *grey-box access* to the victim: they can query the victim's policy network on arbitrary inputs any number of times. However, the adversary does not have direct access to the victim's weights and cannot take gradients through the victim.

We aim to make the victim robust. Though the victim will always be exploitable by *some* adversary since optimal play in Go is intractable, it may be possible to make finding such an adversarial strategy computationally impractical. Accordingly, our threat model restricts itself to *compute-limited* adversaries. We use a small, fixed inference budget and report the amount of compute used to train the adversary. We are also concerned with AI systems that fail dramatically in cases humans do not, framed more precisely in Appendix C. We find these non-human failure modes in all of the following vulnerabilities.

We use Wang et al. (2023a)'s state-of-the-art attack method to produce adversaries for adversarial training and to test our defenses. Wang et al. train an adversary with *victim-play* where the adversary plays games against a frozen copy of the victim, and training data is saved only from the adversary's moves. The adversary selects moves using Adversarial MCTS (A-MCTS), a modification of MCTS that queries the victim's policy network when traversing MCTS nodes corresponding to the opponent's move. The adversary is pitted against increasingly stronger victims as part of a training curriculum, switching to a stronger victim once the adversary's win rate exceeds a certain threshold. We follow Wang et al. by evaluating adversaries with 600 A-MCTS visits per move.

Wang et al. (2023a) trained `base-adversary` against a 2022 KataGo network `base-victim`.*We typi-

*Wang et al. refer to `base-adversary` as

cally train our adversaries by warm-starting from `base-adversary`, which achieved a 97% win rate against `base-victim` at 4096 victim visits. To find diverse attacks, in some experiments we warm-start from `base-adv-early`, which is the first `base-adversary` checkpoint that beats `base-victim` at 1 victim visit after just 7% of `base-adversary`'s compute. See Appendices B and D for details on these networks and training parameters.

3. Iterated adversarial training

Appendix E, examining positional adversarial training, shows that an adversarially trained agent can still be vulnerable to new attacks. Can we create a robust agent by repeatedly defending against new attacks until the space of possible attacks is exhausted? In this section, we design an iterated adversarial training procedure that alternately trains a victim and an adversary. Our procedure produced a victim that was largely robust to the attacks it observed, losing only a low single-digit percentage of games. However, the victim did not gain robustness to new attacks, as we were able to train a new adversary to exploit the final victim.

3.1. Methodology

Our approach differs from KataGo's adversarial training (Appendix E.1) in three key ways. First, we perform *iterated* adversarial training, with multiple rounds of attack and defense to train against a broader range of attacks. Second, we include a higher proportion of adversarial games in the training data: since our priority is robustness, we are more willing to take a hit in average-case capabilities than the KataGo developers. Third, we play games directly against the adversary: this method is less sample-efficient than starting from hand-curated positions, but more scalable and does not require domain-specific knowledge.

We label the adversary and victim at iteration n of adversarial training as "$\mathtt{a}_n$" and "$\mathtt{v}_n$". The initial victim is $\mathtt{v}_0$ = `base-victim`, and the initial adversary is $\mathtt{a}_0$ = `base-adversary`, which Wang et al. trained to defeat `base-victim`. Each subsequent iteration involves training the victim to be robust against the latest adversary, then training an adversary to attack this hardened victim. We repeat this process for 9 iterations.

$\mathtt{v}_n$ is fine-tuned from $\mathtt{v}_{n-1}$ with 18% of games played against a frozen copy of $\mathtt{a}_{n-1}$, and 82% of self-play games against itself. This mixture teaches the victim to be robust to the attack while maintaining its Go capabilities. We stop the training when the victim's win rate plateaus. $\mathtt{a}_n$ is fine-tuned from $\mathtt{a}_{n-1}$ using victim-play with a curriculum of checkpoints from the previous $\mathtt{v}_n$ step. We stop the training after either the victim reaches a threshold visit count or a set maximum compute budget is reached. See Appendix F for details.

`cyclic-adversary` and `base-victim` as `Latest`.

3.2. Results

Each defender $\mathtt{v}_n$ learned an effective defense against the simulated adversary $\mathtt{a}_{n-1}$ but rarely reached a 100% win rate despite $\mathtt{a}_{n-1}$ following a weak, degenerate strategy. We tested the final victim $\mathtt{v}_9$ by pitting it against the final simulated attacker $\mathtt{a}_9$ as well as a validation adversary trained separately from the simulated adversaries $\mathtt{a}_1$, …, $\mathtt{a}_9$. We found the victim was still vulnerable to both attacks but is somewhat less so at high visit counts, indicating that iterated adversarial training offers partial protection against attacks.

3.2.1. Robustness against the iterated adversaries

Each victim $\mathtt{v}_n$ achieves a high win rate against the adversary $\mathtt{a}_{n-1}$ it was trained against when $\mathtt{v}_n$ uses at least 16 visits of search (Fig. 3.2, middle). $\mathtt{v}_n$ quickly learns to beat $\mathtt{a}_{n-1} > 95\%$ of the time (Fig. M.1; 256 visits). However, our defense runs rarely reached a 100% win rate, and the victims were persistently vulnerable at extremely low visits (Fig. 3.2, left).

Both victims and adversaries are able to beat opponents from all previous iterations. This is clearly shown by the adversary win rate in Fig. 3.2 being much higher *below* the diagonal (adversary playing against older victim) than *above* the diagonal (victim playing against older adversary). In the victim case, this can be explained by the training window being large enough to contain data from all previous iterations. By contrast, since adversary training takes many more time steps, all data from one iteration exits the training window during the next iteration. This suggests that the adversary strategy transfers well to previous victims.

The final victim $\mathtt{v}_9$ is still vulnerable even at high visits. Our final simulated adversary $\mathtt{a}_9$ wins 42% of the time against $\mathtt{v}_9$ even at 65,536 visits. We trained $\mathtt{a}_9$ for longer than preceding adversaries, but its total training compute was still only 26% of $\mathtt{v}_9$'s.

All adversaries $\mathtt{a}_n$ exploit a cyclic group, but there are qualitative variations in the size and location of that group, other stones, and especially the group inside the cyclic one (elaborated in Appendix F.2.1). For example, $\mathtt{a}_9$ favors a small, nearly minimal inside shape (Fig. E.1c). To humans, the differences are subtle, and the difficulty of defending against them does not

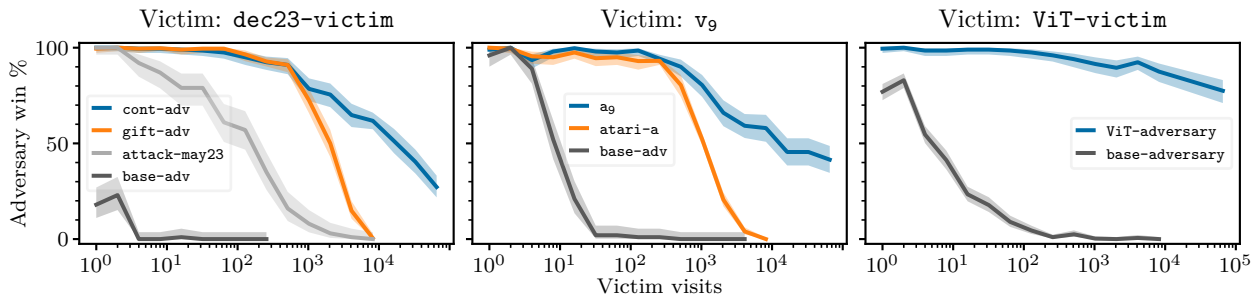


Figure 3.1: Win rate (y-axis) of adversaries (legend) for varying amounts of search (x-axis) given to victims (plot title). `dec23-victim` is a KataGo network that had substantial positional adversarial training. The adversary win rate declines with victim visit counts; however, some adversaries generalize better to higher victim visit counts than others. All the victims are vulnerable even at 65,536 visits. Shaded regions are 95% Clopper-Pearson confidence intervals in this and following figures.

vary significantly. But to the KataGo victims $\texttt{v}_n$, the representations learned do not appear to generalize smoothly between these variations.

3.2.2. Robustness against a new adversary

Though the final iterated victim $\texttt{v}_9$ bests all previous adversaries $\texttt{a}_1$ to $\texttt{a}_8$, the ultimate judge of a defense is whether it works against real attacks. To evaluate this, we train a new adversary `atari-adversary` (initialized to `base-adv-early`) against $\texttt{v}_9$ (Fig. 3.3). This is analogous to a randomly initialized adversary trained to first beat the publicly available KataGo checkpoint `base-victim` at 1 visit and then—without access to any intermediate adversarial training checkpoints $\texttt{v}_1,\ldots,\texttt{v}_8$—trained to attack $\texttt{v}_9$.

`atari-adversary` wins 81% of the time against $\texttt{v}_9$ playing with 512 visits despite being trained with less than 5% of $\texttt{v}_9$'s compute. The attack quickly learns to exploit $\texttt{v}_9$ at low visits, winning over 60% of the time against $\texttt{v}_9$ at 256 visits after just 500 V100 GPU days (Fig. 3.3), sooner than our original `base-adversary` adversary learned to exploit `base-victim`.

However, $\texttt{v}_9$ proves harder to attack at high visits than `base-victim`. Quadrupling to 1024 visits takes slightly more than 4× the compute, largely due to the increased cost of playing training games at higher visits. `atari-adversary` plateaus after 1401 GPU days (♦) with a meager 4% win rate at 4096 visits. By contrast, `base-adversary` generalized rapidly to beat `base-victim` at higher visits. See Appendix F.3 for more information.

`atari-adversary`'s attack is still cyclic, but with a characteristic tendency to leave many stones and groups in "atari", i.e. that could be captured on the next move by $\texttt{v}_9$. Moreover, it sets up "bamboo joints" (Fig. F.3a): shapes where a player has two pairs of two stones with a one-space gap between them. They are common in normal play, and often advantageous: the two sides cannot be separated, as playing in the gap still allows connection through the remaining space. `atari-adversary` induces the victim to form a large cyclic group including these bamboo joints (Fig. F.3b). The attack culminates by surrounding the cyclic group and threatening to split one of the bamboo joints. The correct play for $\texttt{v}_9$ is to capture one of the numerous `atari-adversary` stones in atari, but $\texttt{v}_9$ misses the danger and connects the bamboo joint, leading to the entire cyclic group being captured.

4. Discussion

We explored three natural approaches for defending against adversarial attacks in Go: adversarial training with hand-constructed positions (Appendix E), iterated adversarial training (Section 3), and swapping the CNN backbone for a ViT (Appendix G.1). Each defense made attacks harder—but never impossible, with the attack algorithm finding successful attacks in a fraction of the compute used to train the victims. Moreover, none of the defenses achieve the robustness of a human (Appendix C), and humans are even able to execute several attacks (Appendix I). Our results highlight the challenge of defending against all possible attacks, or even all possible cyclic attacks, suggesting an offense-defense balance (Jervis, 1978) favoring attackers.

We do, however, find it cheap to defend against a specific attack. Perhaps we could fully defend a Go AI by training it against each possible attack? This

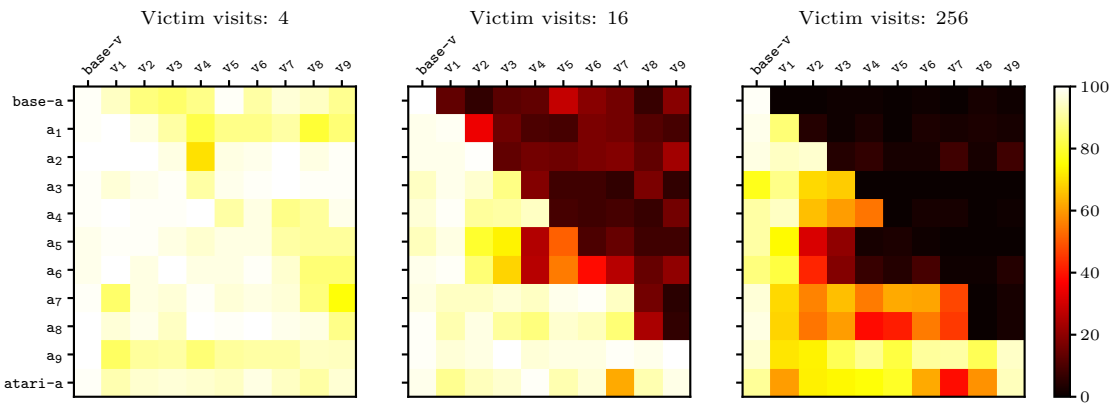


Figure 3.2: Win rate of all adversaries (y-axis) against all victims (x-axis) throughout iterated adversarial training for varying victim visits (plot title). The adversary $\texttt{a}_n$ is typically able to beat the victim $\texttt{v}_n$ it is trained to exploit (top-left-to-bottom-right diagonal), especially at 16 visits or less (middle and left plots). However, given at least 16 visits (middle and right) the victim $\texttt{v}_n$ is typically able to beat the adversary $\texttt{a}_{n-1}$ it trained against (elements immediately above main diagonal) along with all previous iterations $\texttt{a}_{n-2}$, $\texttt{a}_{n-3}$, $\cdots$. See Fig. J.1 for an extended version including other adversaries, victims and visit counts.

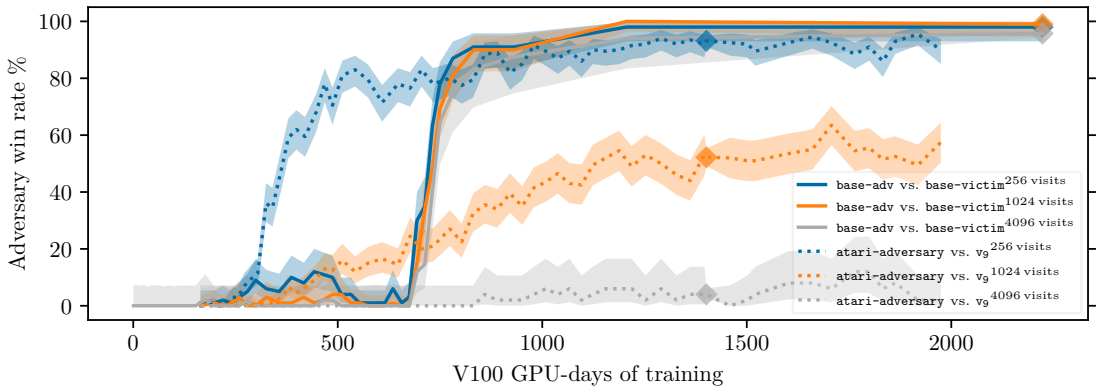


Figure 3.3: Win rate (y-axis) of `base-adversary` vs `base-victim` (—) and `atari-adversary` vs $\texttt{v}_9$ ($\cdots$) by training compute (x-axis), including the 164 GPU days training `atari-adversary`'s initialization checkpoint `base-adv-early`. The checkpoint marked ♦ is used for evaluation.

poses two key challenges. First, the space of adversarial strategies may be large. Second, finding new strong attacks to generate high-quality adversarial training data is computationally expensive.

In order for adversarial training to be an effective defense, it therefore seems necessary for the victim to generalize from a limited number of adversarial strategies. Unfortunately, our results show that current Go AIs do not generalize in this way: $\texttt{v}_9$ and KataGo's adversarially trained networks remain vulnerable to cyclic attacks even after being trained against many cyclic attack variants. Algorithmic improvements are likely needed for effective generalization.

Promising defenses to explore in future work include latent adversarial training (Casper et al., 2024) and more sophisticated multi-agent reinforcement learning algorithms like PSRO (Lanctot et al., 2017) or DeepNash (Perolat et al., 2022). We are also eager to see explorations of attacks in domains other than Go where AI has surpassed human performance. Finally, we recommend a systematic study of whether increases in capabilities lead to increased robustness.

Our results highlight the obstacles to building robust AI systems. If we are unable to achieve robustness in the well-defined and self-contained domain of Go, achieving robustness in more open-ended real-world applications will be even more challenging. To build AI safely, future advanced systems must have intrinsic robustness at the heart of their design.

Acknowledgments

Thanks to David Wu for discussing KataGo and its adversarial training with us and helping us qualitatively describe the two attacks we found in Appendix E. Thanks to Adrià Garriga-Alonso for infrastructure support when running experiments. Thanks to ChengCheng Tan for helping create Fig. 1.1. Thanks to ChengCheng Tan, Derik Kauffmann, Siao Si Looi, David Wu, Micah Carroll, and Daniel Filan for feedback on early drafts. Thanks to Yilun Yang (7 dan professional) and Ryan Li (4 dan professional) for playing `ViT-victim` to evaluate its strength, and to Matthew Harwit and Eric Wainwright for helping connect the authors with professional Go players.

Author contributions

Tom Tseng was the primary technical individual contributor, implementing the majority of the code and running the majority of the experiments. Euan McLean was responsible for writing, preparing an initial draft from high-level comments provided by technical contributors, editing the resulting paper, and project managing the write-up. Tony Wang, Kellin Pelrine and Adam Gleave were joint co-advisors throughout the project. In addition, Tony Wang set up the KGS bot and wrote up sections related to Vision Transformers. Kellin Pelrine analysed the Go games and replicated attacks by hand. Adam Gleave managed the project and edited the paper.

References

Bai, Y., Mei, J., Yuille, A. L., and Xie, C. Are transformers more robust than CNNs? *Advances in Neural Information Processing Systems*, 34:26831–26843, 2021.

Bansal, T., Pachocki, J., Sidor, S., Sutskever, I., and Mordatch, I. Emergent complexity via multi-agent competition. In *International Conference on Learning Representations*, 2018.

北京深客科技有限公司. Golaxy（星阵围棋）, 2018. URL `https://www.19x19.com/`.

Benz, P., Ham, S., Zhang, C., Karjauv, A., and Kweon, I. S. Adversarial robustness comparison of vision transformer and mlp-mixer to CNNs. In *British Machine Vision Conference*, pp. 25. BMVA Press, 2021. URL `https://www.bmvc2021-virtualconference.com/assets/papers/0255.pdf`.

Bhojanapalli, S., Chakrabarti, A., Glasner, D., Li, D., Unterthiner, T., and Veit, A. Understanding robustness of transformers for image classification. In *IEEE/CVF International Conference on Computer Vision*, pp. 10231–10241, 2021.

Brown, N. and Sandholm, T. Superhuman AI for heads-up no-limit poker: Libratus beats top professionals. *Science*, 359(6374):418–424, 2018.

Casper, S., Schulze, L., Patel, O., and Hadfield-Menell, D. Defending against unforeseen failure modes with latent adversarial training. arXiv preprint arXiv:2403.05030, 2024.

Croce, F., Andriushchenko, M., Sehwag, V., Debenedetti, E., Flammarion, N., Chiang, M., Mittal, P., and Hein, M. Robustbench: a standardized adversarial robustness benchmark. In *Advances in Neural Information Processing Systems*, 2021.

Czech, J., Blüml, J., and Kersting, K. Representation matters: The game of chess poses a challenge to vision transformers. arXiv preprint arXiv:2304.14918, 2023.

Czempin, P. and Gleave, A. Reducing exploitability with population based training. In *International Conference on Machine Learning Workshop on New Frontiers in Adversarial Machine Learning*, 2022.

Fu, Y., Zhang, S., Wu, S., Wan, C., and Lin, Y. PatchFool: are vision transformers always robust against adversarial perturbations? In *International Conference on Learning Representations*, 2022.

Gleave, A. Comment on even superhuman go ais have surprising failure modes, 2023. URL `https://www.lesswrong.com/posts/DCL3MmMiPsuMxP45a/even-superhuman-go-ais-have-surprising-failure-modes?commentId=zztDTZmNGsSmhpbZ8`.

Gleave, A., Dennis, M., Wild, C., Kant, N., Levine, S., and Russell, S. Adversarial policies: Attacking deep reinforcement learning. In *International Conference on Learning Representations*, 2020.

He, K., Zhang, X., Ren, S., and Sun, J. Deep residual learning for image recognition. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 770–778, 2016.

Jervis, R. E. Cooperation under the security dilemma. *World Politics*, 30:167 – 214, 1978. URL `https://api.semanticscholar.org/CorpusID:154923423`.

KGS. Top 100 KGS players, 2022. URL `https://archive.is/J4Fjz`. Retrieved from `https://www.gokgs.com/top100.jsp`.

Lanctot, M., Zambaldi, V., Gruslys, A., Lazaridou, A., Tuyls, K., Perolat, J., Silver, D., and Graepel, T. A unified game-theoretic approach to multiagent reinforcement learning. In *Advances in Neural Information Processing Systems*, volume 30, pp. 4190–4203, 2017.

Li, Y., Yuan, G., Wen, Y., Hu, J., Evangelidis, G., Tulyakov, S., Wang, Y., and Ren, J. EfficientFormer: Vision transformers at MobileNet speed. *Advances in Neural Information Processing Systems*, 35:12934–12949, 2022.

Liu, C., Dong, Y., Xiang, W., Yang, X., Su, H., Zhu, J., Chen, Y., He, Y., Xue, H., and Zheng, S. A comprehensive study on robustness of image classification models: Benchmarking and rethinking, 2023.

Mahmood, K., Mahmood, R., and van Dijk, M. On the robustness of vision transformers to adversarial examples. In *IEEE/CVF International Conference on Computer Vision*, pp. 7838–7847, 10 2021.

Monroe, D. Leela Chess Zero training README, 2023. URL https://github.com/Ergodice/lczero-training/blob/0c10d4e19fbfd28abb167f9134fee74c983ef6db/README.md.

Morandin, F., Amato, G., Gini, R., Metta, C., Parton, M., and Pascutto, G.-C. Sai a sensible artificial intelligence that plays go. In *International Joint Conference on Neural Networks*. IEEE, July 2019. doi: 10.1109/ijcnn.2019.8852266. URL http://dx.doi.org/10.1109/IJCNN.2019.8852266.

Pascutto, G.-C. Leela Zero, 2019a. URL https://zero.sjeng.org/.

Pascutto, G.-C. Leela Zero, 2019b. URL https://github.com/leela-zero/leela-zero/.

Pascutto, G.-C. and Linscott, G. Leela Chess Zero, 2019. URL https://lczero.org/.

Paul, S. and Chen, P.-Y. Vision transformers are robust learners. In *AAAI Conference on Artificial Intelligence*, volume 36, pp. 2071–2081, 2022.

Perolat, J., Munos, R., Lespiau, J.-B., Omidshafiei, S., Rowland, M., Ortega, P., Burch, N., Anthony, T., Balduzzi, D., De Vylder, B., Piliouras, G., Lanctot, M., and Tuyls, K. From Poincaré recurrence to convergence in imperfect information games: Finding equilibrium via regularization. In *International Conference on Machine Learning*, volume 139, pp. 8525–8535, 2021.

Perolat, J., De Vylder, B., Hennes, D., Tarassov, E., Strub, F., de Boer, V., Muller, P., Connor, J. T., Burch, N., Anthony, T., et al. Mastering the game of Stratego with model-free multiagent reinforcement learning. *Science*, 378(6623):990–996, 2022.

Pinto, F., Torr, P. H., and K. Dokania, P. An impartial take to the CNN vs transformer robustness contest. In *European Conference on Computer Vision*, pp. 466–480. Springer, 2022.

polytope. Comment on there are (probably) no superhuman go ais: strong human players beat the strongest ais, 2023. URL https://www.lesswrong.com/posts/Es6cinTyuTq3YAcoK/there-are-probably-no-superhuman-go-ais-strong-human-players?commentId=gAEovdd5iGsfZ48H3.

Sagri, A., Cazenave, T., Arjonilla, J., and Saffidine, A. Vision transformers for computer go. In *International Conference on the Applications of Evolutionary Computation (Part of EvoStar)*, pp. 376–388. Springer, 2024.

Schrittwieser, J., Antonoglou, I., Hubert, T., Simonyan, K., Sifre, L., Schmitt, S., Guez, A., Lockhart, E., Hassabis, D., Graepel, T., Lillicrap, T., and Silver, D. Mastering Atari, Go, chess and shogi by planning with a learned model. *Nature*, 588(7839):604–609, 2020.

Shao, R., Shi, Z., Yi, J., Chen, P.-Y., and Hsieh, C.-J. On the adversarial robustness of vision transformers. *Transactions on Machine Learning Research*, 2022. ISSN 2835-8856. URL https://openreview.net/forum?id=lE7K4n1Esk.

Shapley, L. S. Stochastic games. *PNAS*, 39(10):1095–1100, 1953.

Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., Van Den Driessche, G., Schrittwieser, J., Antonoglou, I., Panneershelvam, V., Lanctot, M., et al. Mastering the game of Go with deep neural networks and tree search. *Nature*, 529(7587):484–489, 2016.

Silver, D., Hubert, T., Schrittwieser, J., Antonoglou, I., Lai, M., Guez, A., Lanctot, M., Sifre, L., Kumaran, D., Graepel, T., Lillicrap, T., Simonyan, K., and Hassabis, D. A general reinforcement learning algorithm that masters chess, shogi, and Go through self-play. *Science*, 362(6419):1140–1144, 2018.

Tang, S., Gong, R., Wang, Y., Liu, A., Wang, J., Chen, X., Yu, F., Liu, X., Song, D., Yuille, A., Torr, P. H. S., and Tao, D. RobustART: Benchmarking robustness

on architecture design and training techniques. arXiv preprint arXiv:2109.05211, 2022.

TCEC. Lczero 0.30-dag-dcb4ece9-bt2-3250000 vs stockfish dev16_202301021914 - tcec - archived game, 2023. URL https://tcec-chess.com/#game=1&round=fl&season=cup11.

Tencent. Fineart, 2017. URL https://en.wikipedia.org/wiki/Fine_Art_(software).

Tian, Y., Ma, J., Gong, Q., Sengupta, S., Chen, Z., Pinkerton, J., and Zitnick, L. ELF OpenGo: an analysis and open reimplementation of AlphaZero. In *International Conference on Machine Learning*, 2019.

Timbers, F., Bard, N., Lockhart, E., Lanctot, M., Schmid, M., Burch, N., Schrittwieser, J., Hubert, T., and Bowling, M. Approximate exploitability: Learning a best response in large games. 2022.

Tseng, T., McLean, E., Pelrine, K., Wang, T. T., and Gleave, A. Can go AIs be adversarially robust?, 2024.

Tsipras, D., Santurkar, S., Engstrom, L., Turner, A., and Madry, A. Robustness may be at odds with accuracy. In *International Conference on Learning Representations*, 2019.

Vinyals, O., Babuschkin, I., Czarnecki, W. M., Mathieu, M., Dudzik, A., Chung, J., Choi, D. H., Powell, R., Ewalds, T., Georgiev, P., et al. Grandmaster level in StarCraft II using multi-agent reinforcement learning. *Nature*, 575(7782):350–354, 2019.

Wang, T. T., Gleave, A., Tseng, T., Pelrine, K., Belrose, N., Miller, J., Dennis, M. D., Duan, Y., Pogrebniak, V., Levine, S., and Russell, S. Adversarial policies beat superhuman Go AIs. In *International Conference on Machine Learning*, pp. 35655–35739. PMLR, 2023a.

Wang, Z., Bai, Y., Zhou, Y., and Xie, C. Can CNNs be more robust than transformers? In *The Eleventh International Conference on Learning Representations*, 2023b. URL https://openreview.net/forum?id=TKIFuQHHECj.

Wu, D. Discord comment on the initial hyperparameters of the distributed training run, 12 2020a. URL https://discord.com/channels/417022162348802048/583775968804732928/786408459662917643.

Wu, D. Discord comment on the purpose of custom seeded self-play games, 3 2021a. URL https://discord.com/channels/417022162348802048/583775968804732928/820047133104537600.

Wu, D. Discord comment on the initial katago adversarial training, 12 2022a. URL https://discord.com/channels/417022162348802048/583775968804732928/1052951418685882408.

Wu, D. Discord comment mentioning the last non-adversarially trained network, 12 2022b. URL https://discord.com/channels/417022162348802048/583775968804732928/1056607918545457252.

Wu, D. Katago should be partially resistant to cyclic groups now, 7 2023a. URL https://www.reddit.com/r/baduk/comments/14prv4f/katago_should_be_partially_resistant_to_cyclic/.

Wu, D. Discord comment on katago adversarial training data sources, 7 2023b. URL https://discord.com/channels/417022162348802048/723268423588642948/1131951228495081543.

Wu, D. Discord comment on increasing training visits for the distributed training run, 3 2023c. URL https://discord.com/channels/417022162348802048/583775968804732928/1090737750459814038.

Wu, D. Discord comment on the percentage of custom seeded self-play games, 12 2023d. URL https://discord.com/channels/417022162348802048/583775968804732928/1180306891314839572.

Wu, D. Other methods implemented in KataGo, 2024. URL https://github.com/lightvector/KataGo/blob/cbaa8625571ee6121fd62f7ab8a8ee3ef76bc250/docs/KataGoMethods.md.

Wu, D. J. Accelerating self-play learning in Go. In *AAAI Workshop on Reinforcement Learning in Games*, 2020b.

Wu, D. J. KataGo training history and research, 2021b. URL https://github.com/lightvector/KataGo/blob/master/TrainingHistory.md.

Wu, D. J. KataGo's supported Go rules (version 2), 2021c. URL https://lightvector.github.io/KataGo/rules.html.

Wu, D. J. KataGo - networks for kata1, 2022c. URL https://katagotraining.org/networks/.

Zhang, C., Zhang, M., Zhang, S., Jin, D., Zhou, Q., Cai, Z., Zhao, H., Liu, X., and Liu, Z. Delving deep into the generalization of vision transformers under distribution shifts. In *IEEE/CVF conference*

on Computer Vision and Pattern Recognition, pp. 7277–7286, 2022.

Zinkevich, M., Johanson, M., Bowling, M., and Piccione, C. Regret minimization in games with incomplete information. In *Advances in Neural Information Processing Systems*, volume 20, 2007.

Zou, A., Wang, Z., Kolter, J. Z., and Fredrikson, M. Universal and transferable adversarial attacks on aligned language models. arXiv preprint arXiv:2307.15043, 2023.

A. Related work

We focus on robustness against *adversarial policies*: strategies designed to make an opponent perform poorly. Adversarial policies give an empirical lower bound for an agent's *exploitability*: its worst-case loss relative to Nash equilibria (Timbers et al., 2022). Gleave et al. (2020) previously explored such policies in a zero-sum game between simulated humanoids trained with self-play. The policies (Bansal et al., 2018) attacked by Gleave et al. were below human performance, raising the question: were the agents vulnerable because of their limited capability? To investigate this, Wang et al. (2023a) searched for adversarial policies against the superhuman Go AI KataGo (Wu, 2020b), finding a strategy that beats KataGo in 97% of games.

We focus on KataGo (Wu, 2020b) as it is the most capable open-source Go AI. Moreover, other superhuman open-source Go AIs such as ELF OpenGo (Tian et al., 2019) and Leela OpenZero (Pascutto, 2019a) all follow the same basic AlphaZero-style training architecture. However, alternative multi-agent reinforcement learning methods may be more robust. Approaches that maintain a population of strategies are promising (Vinyals et al., 2019; Czempin & Gleave, 2022; Lanctot et al., 2017). Another alternative, counterfactual regret minimization (Zinkevich et al., 2007), has been used to beat professional human poker players (Brown & Sandholm, 2018). Furthermore, Perolat et al. (2022) found a method for approximating Nash equilibria (Perolat et al., 2021) that scaled to the boardgame Stratego, whose game tree is 10^{175} times larger than Go's.

We replace the CNN backbone of KataGo with a vision transformer (ViT) and train the ViT agent to a superhuman level, finding it to be slower to train than a CNN agent and weaker at the same inference budget. By contrast, Sagri et al. (2024) found the transformer-based EfficientFormer architecture (Li et al., 2022) performed similarly to CNNs for Go—however, their models were trained only with supervised learning, not self-play. Transformers have been investigated more thoroughly in chess. Our results are consistent with Czech et al. (2023) who found that CNNs are stronger at chess than both ViTs and a ViT-CNN hybrid at a given inference budget. Yet transformers have shown strong performance, with the transformer-based Leela Chess Zero (Pascutto & Linscott, 2019; Monroe, 2023) winning the Top Chess Engine Championship Cup 11 (TCEC, 2023).

Although we find ViTs are weaker than CNNs in average-case capabilities, our primary metric is *robustness*. Past research in image classification indicates ViTs are modestly more robust than CNNs against adversarial perturbations and other out-of-distribution inputs (Benz et al., 2021; Shao et al., 2022; Bhojanapalli et al., 2021; Zhang et al., 2022; Paul & Chen, 2022), although some research contests this (Bai et al., 2021; Mahmood et al., 2021; Tang et al., 2022; Pinto et al., 2022; Wang et al., 2023b). Even if ViTs are not overall more robust, their differing inductive biases might cause them to fail in *different* ways to CNNs, with prior work finding ViTs are more vulnerable to patch perturbations (Fu et al., 2022). Surprisingly, we find that not only are ViT-based Go agents exploitable by new attacks, but the attack of Wang et al. (2023a) transfers zero-shot to our ViT agent.

B. KataGo networks reference

We build on top of KataGo (Wu, 2020b), the strongest open-source Go AI system. KataGo learns via self-play using an AlphaZero-style training procedure (Silver et al., 2018). The agent selects moves with Monte-Carlo Tree Search (MCTS), using a neural network to propose and evaluate moves. The neural network contains a policy head that outputs a probability distribution over the next move and a value head that estimates the win rate from the current state. KataGo trains its policy head to mimic the outcome of tree search and its value head to predict whether the agent wins the self-play game.

We evaluate and fine-tune a variety of KataGo models. We refer to each model's architecture as `b`B`c`C where B is the number of *blocks* in the convolutional residual network and C is the number of channels. We refer to each model by `b`B`c`C`-s`S`m` where S is the number of million time steps for which the model has been trained. We may omit the channel term `c`C when there is no ambiguity. All of our adversaries have 6 blocks and 96 channels, abbreviated to `b6c96` or just `b6`.

The victims we attack are either `b40c256` networks or `b18c384`. The `b18c384` networks use a new convolution-based architecture with modified bottleneck blocks (He et al., 2016; Wu, 2024). They were introduced into KataGo's official training run in 2023, becoming the strongest networks by the end of the year. The inference cost of these `b18` networks is similar to that of standard b40 networks. Given the same inference compute budget per move to perform search, they outperform the best standard `b40` and `b60c320` networks.

In Table B.1 we enumerate all victims used in this work, comprising official KataGo networks, those developed by Wang et al. (2023a) and those developed in this work. In Table B.2 we enumerate all adversaries used in this work, including our own and those developed by Wang et al..

Name	Params		Training		Date	Description
	B	C	Steps (M)	GPU-days		
`base-victim`	40	256	11841	21681	2022-06	Original target KataGo network for Wang et al. (2023a)'s adversarial attack. "kata1-b40c256-s11840935168-d2898845681" at `https://katagotraining.org/networks/`.
`may23-victim`	60	320	7702	25888	2023-05	KataGo network that had received 5 months worth of adversarial training against cyclic positions. "kata1-b60c320-s7701878528-d3323518127" at `https://katagotraining.org/networks/`.
`dec23-victim`	18	384	8527	33482	2023-12	KataGo network that had received 1 year worth of adversarial training against cyclic positions. "kata1-b18c384nbt-s8526915840-d3929217702" at `https://katagotraining.org/networks/`.
$\texttt{v}_n$	40	256	–	–	–	The victim at iteration n of our iterated adversarial training (see Section 3). $\texttt{v}_0$ is warm-started from `base-victim`. See Appendix F for breakdown.
$\texttt{v}_9$	40	256	12097	28296	2024-01	Our final iterated adversarially trained victim (see Section 3), warm-started from `base-victim`.
`ViT-victim`	16	384	650	537	2024-01	A network we trained from scratch using the same approach as KataGo but with the CNN backbone replaced with a vision transformer.

Table B.1: All victim networks used in this work with **B**locks, **C**hannels, training steps (in millions), and estimated compute cost (in V100 GPU days). The estimate of `base-victim`'s compute cost is from Wang et al. (2023a). The training cost for $\texttt{v}_9$ includes both the training cost of all iterated victims and all iterated adversaries up to and including $\texttt{a}_8$.

Name	Training		Attack	Description
	Steps (M)	GPU-days	Style	
`base-adversary`	545	2223	cyclic	Original attack trained by Wang et al. (2023a) from scratch to defeat the KataGo network `base-victim`.
`base-adv-early`	227	164	non-cyclic	The first checkpoint able to defeat `base-victim` at one victim visit from the `base-adversary` training run.
`attack-may23`	713	3378	cyclic	`base-adversary` fine-tuned by Wang et al. (2023a) to defeat KataGo's adversarially trained network `may23-victim`.
`cont-adv`	1343	4476	cyclic	A network we trained using victim-play to defeat `dec23-victim`, using a fine-grained curriculum and fine-tuned from `attack-may23`.
`gift-adversary`	878	1865	gift	A network we trained using victim-play to defeat `dec23-victim`, using a coarse-grained curriculum and fine-tuned from `base-adv-early`.
$\mathtt{a}_n$	–	–	cyclic	The adversary at iteration n of our iterated adversarial training (see Section 3). $\mathtt{a}_0$ is fine-tuned from `base-adversary`. See Appendix F for breakdown.
$\mathtt{a}_9$	4132	7337	cyclic	The final adversary resulting from our iterated adversarial training (see Section 3).
`atari-adversary`	791	1401	complex cyclic	A network we trained using victim-play to defeat $\mathtt{v}_9$ fine-tuned from `base-adv-early`, to test the general robustness of iterated adversarial training.
`ViT-adversary`	871	2632	cyclic	A network we trained using victim-play to defeat `ViT-victim`, fine-tuned from `base-adversary`.

Table B.2: All adversary networks used in this work with training steps (in millions) and estimated compute cost (in V100 GPU days). The adversaries use a 6 block, 96 channel KataGo CNN architecture `b6c96`. The training cost for $\mathtt{a}_9$ includes both the training cost of all iterated adversaries.

Victim		Opponent		Opponent vs Victim	
Name	**Visits**	**Name**	**Visits**	**Compute (%)**	**Win rate (%)**
`base-victim`	4096	`base-adversary`	600	10	97
`base-victim`	10^7	`base-adversary`	600	10	72
`may23-victim`	4096	`attack-may23`	600	13	47
`dec23-victim`	4096	`continuous-adversary`	600	13	65
`dec23-victim`	65536	`continuous-adversary`	600	13	27
`dec23-victim`	512	`gift-adversary`	600	6	75
v_9	4096	`base-victim`	4096	77	66
v_9	512	`atari-adversary`	600	5	81
v_9	4096	a_9	600	26	59
v_9	65536	a_9	600	26	42
`ViT-victim`	512	`base-adversary`	600	414	2.5
`ViT-victim`	65536	`ViT-adversary`	600	490	78

Table B.3: The adversary win rate and fraction of opponent's compute used to train the opponent (right) for various victims (left) and opponents (middle). In most cases the victim was trained with much more compute than the opponent; the exception is `ViT-victim` which was trained for a relatively brief period, 4× less than `base-adversary`, although the additional fine-tuning compute used to train `ViT-adversary` was still less than that of `ViT-victim`. We standardize on 600 visits for adversary evaluation. The non-adversarial opponent, `base-victim`, is evaluated at the same number of visits as the victim. The first two rows show evaluations performed by Wang et al. (2023a).

C. Human-robustness standard

We are concerned with whether AI systems may fail dramatically in cases where humans succeed. Broadly, we seek an operationalizable definition such that if a system were human-robust, its worst-case performance would not be worse than human average-case performance. That is, a human-robust system is not just sometimes but consistently superhuman.

More formally, we say a system is **human-robust** if there are no points at which an omniscient observer could ask a human having ordinary skill in the art to make a decision or sequence of decisions, and the human making the decisions—without the benefit of hindsight— would consistently and intentionally produce a substantially better outcome than if the system were making them. In the context of Go, this means the system must not lose from a board state where a human could take over temporarily and consistently produce a win. None of the defense strategies studied in this work meet even weak versions of this human-robust standard.

We note that the concept of a "human having ordinary skill in the art" is derived from patent law,[†] referring to a person with "normal skills and knowledge" of a particular field "without being a genius". We can also define related concepts like lay- or expert-human-robustness, or amateur- or professional- or world-champion-human-robustness, in the natural way by specifying a different group of humans.

The decisions for a human to control are chosen by an omniscient observer so that the human does not need hindsight. If the human themselves were choosing when to intervene without hindsight, they would have to anticipate the robustness failures of the system or perform better than the system in all cases. The former would be unrealistic in most cases, while the latter would be defining a standard that cannot apply to systems that are sometimes superhuman. On the other hand, if the human had hindsight, they would be able to choose where to intervene themselves, but they would also have knowledge of how to intervene that a human with ordinary skill in the art would not, leading to a more stringent standard than just cases where the system would not fail where a human would succeed.

Besides adding hindsight, we could also define a stronger form of robustness by removing "intentionally." This would allows for humans making correct decisions without legitimate reasons for them, and reflects situations where humans might be more robust but in an unstable equilibrium where a change to a different but equally valid decision-making process could destroy that robustness.

We note that an even stronger form could be defined by relaxing "consistently". There are plenty of decisions where a human would randomly make the right decision. However, flipping a coin could too. We suggest that depending on the application, the definition of human-robustness might be strengthened by specifying a particular chance below 100% that a human would make the right decision.

The meaning of "substantially" should depend on the context and level of robustness needed. In the context of Go, the clearest standard is winning or losing the game. This could be made more stringent by considering even some amount of points lost "substantial," but that is currently unnecessary since we find none of the Go AIs meet even the weaker standard.

We note that this standard is not meant to be a mathematically rigorous definition. There could be pathological examples where a system's robustness might be unsatisfactory despite meeting this standard. For example, one could imagine adversaries that detect if a human is playing and adjust their own play (e.g., resigning when they believe they're playing against a human) to break this standard in a contrived way.

Nonetheless, we propose it as one useful lens to think about robustness. On the one hand, if a system met this standard in a non-pathological way, that would suggest that it is robust in a practical way where it will only fail in ways humans would too, and will not create new, potentially dangerous vulnerabilities. On the other hand, it is sufficiently concrete to be falsifiable in real-world scenarios.

In our case in particular, we note that the Go AIs in our experiments do not even achieve the weakest version of these criteria, given that a human would make correct decisions to defend against our attacks virtually 100% of the time. Specifically, for all the cyclic attacks in Fig. E.1, the human could simply capture the adversary's group inside the cyclic group, before the cyclic group itself is captured. This is trivial since the inside groups have few

[†] `https://en.wikipedia.org/wiki/Person_having_ordinary_skill_in_the_art`

liberties and no options to defend against that. Meanwhile, to defend against `gift-adversary`, a human would simply not offer the gift, for example, connecting at the location marked with △ in Fig. E.1b. Similarly, to defend against `atari-adversary`, a human just needs to avoid filling in their own last liberty, i.e., playing anywhere else such as one of the numerous captures available, instead of the location marked with △ in Fig. F.3b.

D. Training parameters

D.1. Training window

KataGo generates training data from self-play games. The model then trains on a sample from a sliding window of the most recent training data. The default starting window size is $m_0 = 250,000$ samples or "rows," and when there are N total training rows, the window size m scales as a power law in N:[‡]

$$m = \frac{.4m_0^{.35}}{.65} \cdot \left(N^{.65} - m_0^{.65}\right) + m_0. \tag{1}$$

Each training "epoch" consumes approximately 250,000 data rows and performs 1 million training steps.

All of our models, besides our self-play ViT models, involve *warm-starting* from KataGo models or models trained by Wang et al. (2023a). Warm-starting from a model, or fine-tuning a model, means we initialize our training from that model and pre-seed the training data with that model's training history. The pre-seeding increases the window size by increasing N in Eq. (1), and it populates the training window with the pre-existing training data. Without pre-seeding the data, the default starting window size would be small and cause over-fitting. We could also increase the training window size by increasing m without pre-seeding, but then there is a high initial cost to generate enough new data to populate the starting window.

D.2. Configuration parameters

The board size varies randomly between training games, allowing KataGo to learn to play Go on various board sizes. Because we focus on 19x19 games in our evaluations, we train our adversaries primarily on 19x19 games: 53.6% to be precise, matching the distribution used in recent KataGo training. This contrasts with the attack of Wang et al. (2023a) who set only 35% of games to be 19x19, following a distribution of board sizes matching those used for early KataGo training of small 6-block and 10-block models.

When training our adversaries, we disable the variance time loss (`vtimeloss` in the KataGo code), an auxiliary loss on a model output predicting uncertainty in the game's outcome. We disabled it following Wang et al.'s finding that this stabilized their early training runs, although we did not confirm its impact on our training.

Like Wang et al., our adversary training uses curricula in which the adversary plays against increasingly strong victims, switching to a stronger victim once the adversary win rate exceeds a certain threshold. We usually set the threshold to 75%. However, we increased the threshold to 90% for higher visit count victims (typically 512 or more) since at that point higher victim visit counts substantially increase the cost of generating games, making it more computationally efficient to train at a slightly lower sample efficiency but with cheaper samples.

When training adversaries against a victim using fewer than 100 victim visits, we enable Wang et al.'s pass-alive defense to prevent the adversary from learning the degenerate "pass attack" that they encountered in low-visit victims.

We change several training configuration parameters listed below compared to Wang et al., usually tweaking these parameters partway into training runs since we only identified or began experimenting with them after launching the runs.

Enabling selecting moves by the lower-confidence bound (LCB) on their utility. Selecting moves by LCB is the default in evaluation but is disabled in training because the creator of KataGo found that enabling LCB reduced self-play training progress despite making evaluation stronger.[§]. We found that having LCB disabled led to a large strength gap between training and evaluation. We preferred to keep train and evaluation similar so that we could be more confident that training progress correlated with evaluation strength.

Adjusting other victim configuration parameters to more closely match the settings used during evaluation. For example, parameters that govern exploration vs. exploration trade-offs (like temperature), or

[‡]The sliding window is implemented by the script at `https://github.com/lightvector/KataGo/blob/eaaddd82339750d9defc70f566e6c59d7068b7b3/python/shuffle.py`, and the `--help` documentation string for the script gives this equation.

[§]The creator of KataGo details their LCB experiments at `https://github.com/leela-zero/leela-zero/issues/2411`.

the KataGo "optimism" feature[¶].

In some training runs, we only changed a subset of these parameters because we had not yet discovered all of these parameters disparities. The full list of parameters we change in the final runs is:

```
antiMirror = true
chosenMoveTemperature = 0.10
chosenMoveTemperatureEarly = 0.50
conservativePass = true
cpuctExploration = 1.0
cpuctExplorationLog = 0.45
cpuctUtilityStdevScale = 0.85
dynamicScoreCenterScale = 0.75
dynamicScoreCenterZeroWeight = 0.2
dynamicScoreUtilityFactor = 0.3
enablePassingHacks = true
fillDameBeforePass = true
policyOptimism = 1.0
rootDesiredPerChildVisitsCoeff = 0
rootFpuReductionMax = 0.1
rootNoiseEnabled = false
rootNumSymmetriesToSample = 1
rootPolicyOptimism = 0.2
rootPolicyTemperature = 1.0
rootPolicyTemperatureEarly = 1.0
staticScoreUtilityFactor = 0.1
subtreeValueBiasFactor = 0.45
subtreeValueBiasWeightExponent = 0.85
useNoisePruning = true
useNonBuggyLcb = true
useUncertainty = true
valueWeightExponent = 0.25
```

Adjust adversary configuration parameters to more closely match the settings used in the latest KataGo training runs. This involves slight adjustments in exploration and utility computation, as well as a small bugfix related to LCB. We made these changes under the assumption that later KataGo configurations are superior to early ones our initial parameter settings were based on, although we did not check if this made a major difference in our training. The full list of parameters we change is:

```
cpuctExploration = 1.05
cpuctExplorationLog = 0.28
dynamicScoreCenterScale = 0.75
dynamicScoreUtilityFactor = 0.30
rootPolicyTemperatureEarly = 1.5
staticScoreUtilityFactor = 0.05
subtreeValueBiasFactor = 0.30
useNonBuggyLcb = true
```

[¶]Policy optimism is described at `https://github.com/lightvector/KataGo/blob/828f1bc27617f9a7dc881d11a7296856ef7c4fc0/docs/KataGoMethods.md#optimistic-policy`. Wang et al. used a version of KataGo that had not yet introduced this feature.

E. Positional adversarial training

E.1. Defense methodology

We target models from KataGo's main training run, which began to include adversarial training against cyclic positions soon after their discovery. Since December 2022, 0.08% of KataGo's self-play games have been initialized from a set of hand-written positions based on `base-adversary`'s strategy (Wu, 2022a; 2023a). Other positions were added as online Go players found different configurations of cyclic positions, growing the fraction of seeded self-play games to a few tenths of a percent (Wu, 2023b). The resulting models defended well against `base-adversary`.

Despite this positive result, Wang et al. (2023a) were able to fine-tune `base-adversary` to produce `attack-may23` achieving a 47% win rate against an adversarially trained KataGo checkpoint `may23-victim` at 4096 visits. Building on Wang et al.'s evaluation, we test `dec23-victim` which has had over twice as much adversarial training as `may23-victim`.

KataGo's official training run performed adversarial training on board positions exhibiting the cyclic attack. Despite this, we show that KataGo's adversarially trained network remains exploitable by training two new adversaries that beat the strongest KataGo network from the end of 2023, which we call `dec23-victim`. The first adversary, `continuous-adversary`, wins 65% of games against `dec23-victim` (4096 victim visits) using a cyclic strategy. The second adversary, `gift-adversary`, defeats `dec23-victim` in 75% of games (512 victim visits) using a qualitatively different exploit where the victim repeatedly gifts the adversary two stones (though it does not scale to high victim visits as well as `continuous-adversary`). Both attacks can be replicated by a human expert (Appendix I).

E.2. The continuous adversary

`continuous-adversary` was initialized from `attack-may23` and fine-tuned using victim-play (Wang et al., 2023a) against `dec23-victim`. `continuous-adversary`'s curriculum involved increasing the victim search budget along with periodically or "continuously" updating the victim to the latest KataGo checkpoint over several months. See Appendix E.2.1 for more details.

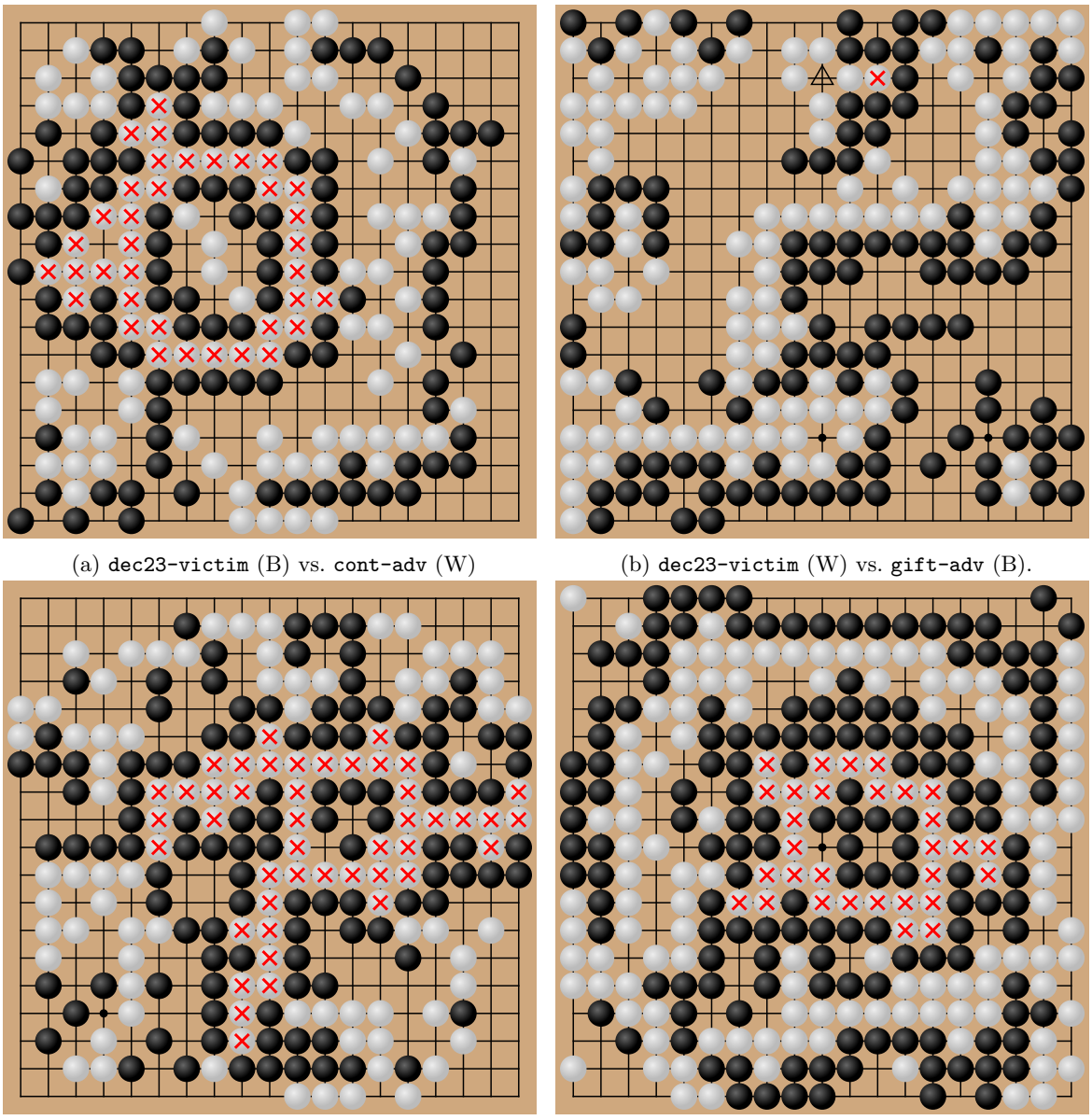
The final `continuous-adversary` achieves a win rate of 91% against `dec23-victim` (at 512 victim visits—above the superhuman threshold of 64 visits, see Appendix H). The attack can exploit even high-visit victims, attaining a win rate of 65% against 4096 visits (Fig. 3.1). Although still cyclic, unlike Wang et al.'s original cyclic attack the `continuous-adversary` always forms nearly the same shape in the interior of the cycle (an example is shown in Fig. E.1a and is also visible in Fig. L.3). Moreover, `continuous-adversary` did not achieve as high win rates as Wang et al. achieved against the non-adversarially trained `base-victim`. This suggests that while adversarial training complicates attacks and may narrow the range of feasible attacks, it does not comprehensively eliminate the cyclic vulnerability.

E.2.1. Extra details

We warm-started from `attack-may23` since Wang et al. found it to be effective against KataGo's `b18` networks. `attack-may23` was trained to attack an adversarially trained KataGo network `may23-victim` (`b60c320-s7702m`) released on May 17, 2023 (see Table B.1). We trained the adversary for a further 1098 V100 GPU-days and 630 million training steps, for a total of 4476 GPU days and 1343 million training steps (Table B.2).

We started the curriculum at 1 victim visit, doubling the visits when a win rate threshold was reached. We set the threshold to 75% up to 256 visits, and 90% after that due to the increased cost of generating training games against high visit-count victims. We periodically updated the KataGo `b18` checkpoint used.

Figure E.2 shows `continuous-adversary`'s win rate against `dec23-victim` throughout adversary training. Figure E.3 shows `continuous-adversary`'s win rate against several `b18` KataGo networks. We see that `continuous-adversary` successfully attacks all `b18` networks up until `b18-s9432m` when `continuous-adversary` positions were introduced into KataGo's training data, at which point `continuous-adversary`'s win rate drops quickly. This decline was faster than when KataGo initially introduced positions from `base-adversary` into KataGo's training data—at that time, it took several hundred million training steps to make `base-adversary`'s



(a) `dec23-victim` (B) vs. `cont-adv` (W)

(b) `dec23-victim` (W) vs. `gift-adv` (B).

(c) $\texttt{v}_9$ (W) vs. $\texttt{a}_9$ (B)

(d) `ViT-victim` (W) vs. `ViT-adversary` (B)

Figure E.1: The learned adversarial strategies are qualitatively unique. a, c, d are variants of the cyclic attack with the × groups soon to be captured. The inside shapes are distinctive of each attacker but have little impact on optimal play, and are similarly easy for a human to navigate correctly. The `gift-adversary` in b follows a distinctly different strategy, inducing the victim (white) to play the stone marked × "gifting" the adversary two stones it can capture by playing at △. Each subcaption links to the complete game history on our website.

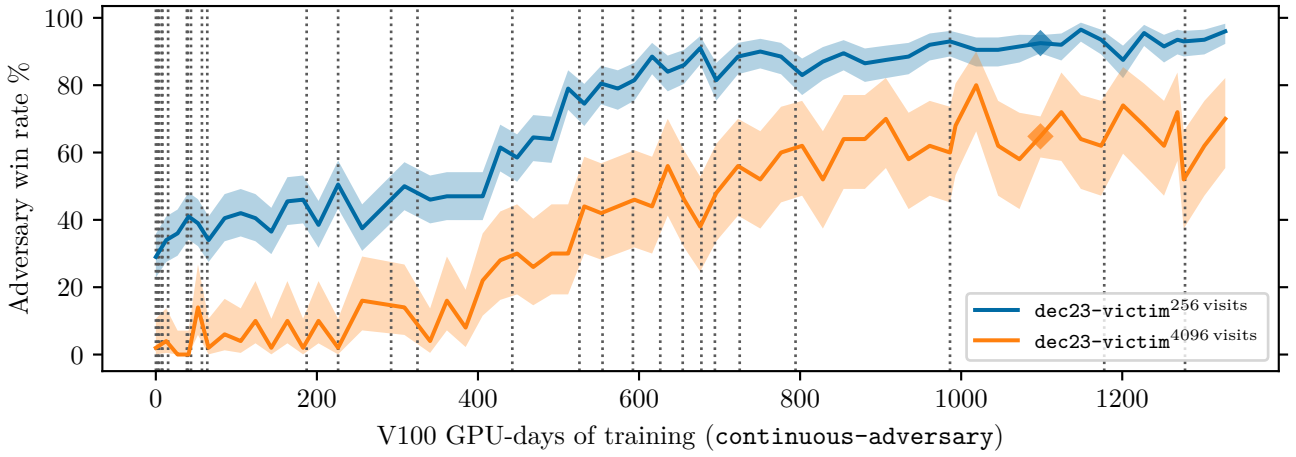


Figure E.2: Win rate (%) of `continuous-adversary` (marked ♦) against `dec23-victim` throughout fine-tuning against `dec23-victim`. The zero of the x-axis represents the win rate of `attack-may23` against `dec23-victim` before the fine-tuning against `dec23-victim` began.

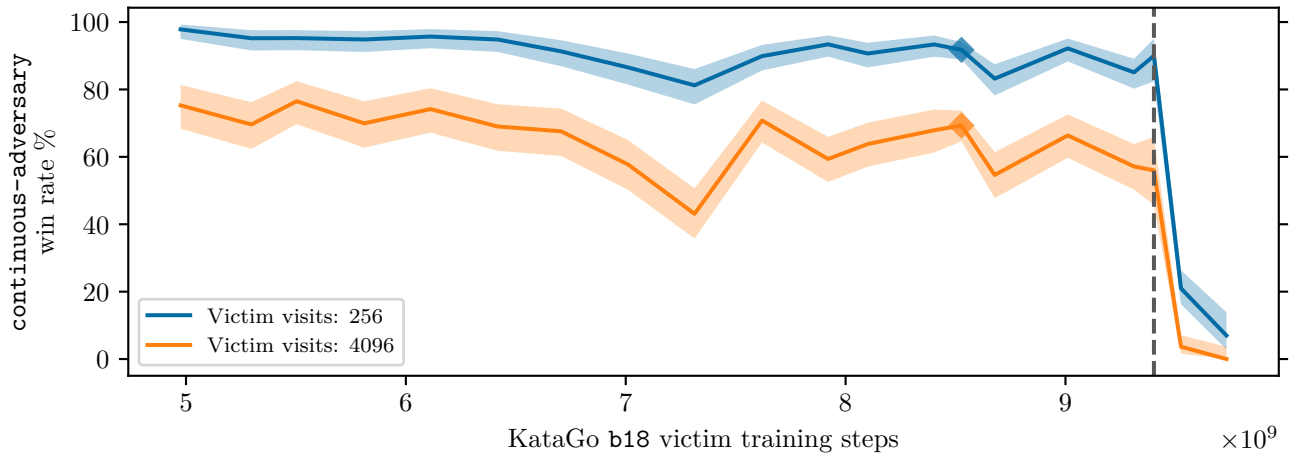


Figure E.3: The win rate (%) of `continuous-adversary` against the main KataGo training run between networks `b18-s4975m` and `b18-s9732m`. The marked point ♦ is `dec23-victim`. At the dashed line, the KataGo developers added positions from `continuous-adversary` and `gift-adversary` into KataGo's adversarial training data, which caused the win rate to drop.

win rate to dramatically drop, see Wang et al. (2023a, Figure L.2).

The full curriculum was:

- `b18-s7283m` (released August 17, 2023), 1–16 visits.
- `b18-s7313m`, 16–32 visits.
- `b18-s7343m`, 32–256 visits.
- `b18-s7373m`, 256 visits.
- `b18-s7500m`, 256–512 visits.
- `b18-s7590m`, 1024 visits.
- `b18-s7620m`, 256 visits. (Here we reverted visits to 256 because earlier visit increases were due to non-representative samples of games skewing our curriculum advancement script into giving inaccurate win rate estimates.)
- `b18-s7680m`, 256 visits.
- `b18-s7740m`, 256 visits.
- `b18-s7830m`, 256 visits.
- `b18-s7890m`, 256 visits.
- `b18-s7950m`, 256 visits.
- `b18-s8010m`, 256 visits.
- `b18-s8071m`, 256–512 visits.
- `b18-s8191m`, 512 visits.
- `b18-s8282m`, 512 visits.
- `b18-s8463m` (released Dec 11 2023), 512 visits. This is the last curriculum checkpoint that our chosen adversary checkpoint `continuous-adversary` at 1098 V100 GPU-days saw. The remaining curriculum checkpoints were seen by adversary checkpoints beyond the one we chose for main evaluations in this paper.
- `b18-s8588m`-v512
- `b18-s8678m`-v512 (released Jan 9 2024)

We initially observed a large win rate gap between training and evaluation. To close this gap, we made only two changes to the training configuration, rather than all the changes listed in Appendix D.2: we enabled LCB move selection and activated optimism for the victim.

E.3. The gift adversary

The `gift-adversary` was initialized from the earlier `base-adv-early` checkpoint, encouraging exploration, and fine-tuned against `dec23-victim` with a curriculum of increasing victim search budgets (Appendix E.3.1). The attack wins 91% of games against `dec23-victim` (at 512 victim visits) after training with just 6% as much compute as the victim. The `gift-adversary` does not scale to high victim visits as well as the `continuous-adversary` (Fig. 3.1). However, the attack reveals a qualitatively new exploit against KataGo (Fig. E.1b).

In particular, the adversary sets up a so-called "sending-two-receiving-one" situation where the victim, for no valid reason, gifts the adversary two stones and needs to capture one back. However, the victim's recapture is

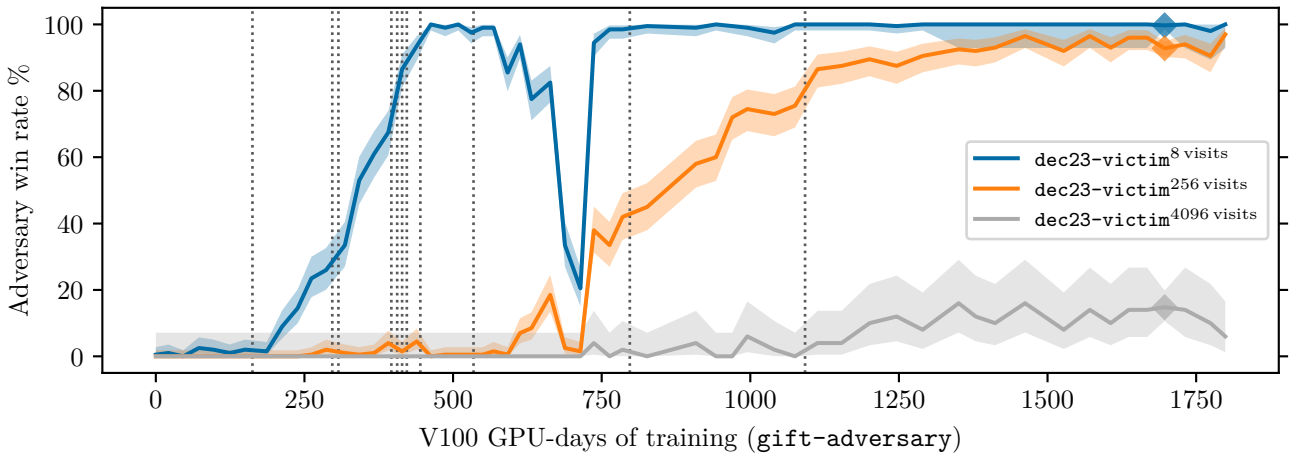


Figure E.4: Win rate (%) of `gift-adversary` (marked ♦) against `dec23-victim` throughout fine-tuning against `dec23-victim`. The zero of the x-axis represents the win rate of `base-adv-early` against `dec23-victim` before the fine-tuning against `dec23-victim` began. The large drop in win rate at 700 GPU-days occurred when the curriculum prematurely increased from 128 visits to 256 visits. The adversary's win rate against `dec23-victim` at 256 visits was poor, and it was not learning well. After we reverted the curriculum back to 128 visits, the win rate surprisingly recovered, seemingly without hindering training progress.

blocked by positional superko rules.[‖] The adversary sets up the position such that the resurrection of one of its dead groups is at stake, leading to a disaster for the victim. This occurs despite no benefit for the victim in initiating the scenario even if superko rules were not in play. Moreover, the victim was trained with superko rules and has an input feature that marks superko moves illegal if they come up in the search.

E.3.1. Extra details

The adversary is warm-started from `base-adv-early`. The curriculum began with `dec23-victim` at 4 visits, increasing up to 8 visits in 1 visit increments, then doubling visits each time until 512 visits. We added the extra victim visits between 4 and 8 because after finding that a direct increase from 4 to 8 visits led to a large win rate drop and minimal training progress. The adversary was trained for a further 1697 V100 GPU-days and 651 million training steps, totalling 1861 GPU-days and 878 million steps (Table B.2).

Figure E.4 shows the win rate of `gift-adversary` throughout training. Figure E.5 shows `gift-adversary`'s win rate against several `b18` KataGo networks. Either `gift-adversary` is highly specialized to setting up the gift attack against `dec23-victim`, or the gift vulnerability only appears in recent KataGo `b18` nets. David Wu, the main developer of KataGo, suggests the former is more likely. After we disclosed this vulnerability, he examined older KataGo nets and found that they also misjudge board positions produced by `gift-adversary`.

At 163 V100 GPU-days (79 million training steps), we adjusted victim configuration parameters to more closely match evaluation as described in Appendix D.2.

At 170 V100 GPU-days (81 million training steps), we reduced the training move limit per game from KataGo's default of 1600 moves to $900 * (\text{board area})/(19^2)$ moves since we noticed several games dragging out to hit the move limit due us enabling the pass-alive defense (Appendix D.2), which lengthens games, on low-visit victims during training. This is before the adversary had discovered the gift attack, and games were not noticeably longer than `atari-adversary`'s games at a similar point in `atari-adversary`'s training. Still, we hypothesized this would increase training efficiency by cutting the duration of lengthy games, which cost compute and generate an excessive amount of end-game policy training data.

At 475 V100 GPU-days (220 million steps), we noticed that the adversary learned to prolong a significant portion

[‖]To prevent an infinite loop, most rule sets include a *superko rule* forbidding repetition of a previous board state ("positional superko") or state and player's turn ("situational superko").

Figure E.5: The win rate (%) of `gift-adversary` against the main KataGo training run between networks `b18-s4975m` and `b18-s9732m`. The marked point ♦ is `dec23-victim`. At the dashed line, the KataGo developers added positions from `continuous-adversary` and `gift-adversary` into KataGo's adversarial training data.

of games using extended ko fights to hit the 900-move limit. Normally during training, such games are scored and assigned a winner based on the final board state. Not only does having lots of games hit the move limit significantly slow down training, but we were also worried that the final board state score does not necessarily reflect what the score would have been had the game been played out to completion. The adversary could reward hack by stalling in a state that is winning if scored prematurely but is losing if played to the end.

We therefore at 632 V100 GPU-days (307 million steps) began scoring games that hit the move limit with a score of 0 and marked them as losing for the adversary (-1 utility). This drove the hit-move-limit rate from 59% to 22%. At 836 V100 GPU-days (393 million steps), we reduced the utility of such games even further to -1.6, below the worst typically possible utility -1.35 resulting from losing a game and having the opponent control all territory on the board. This drove the hit-move-limit down to 0%.

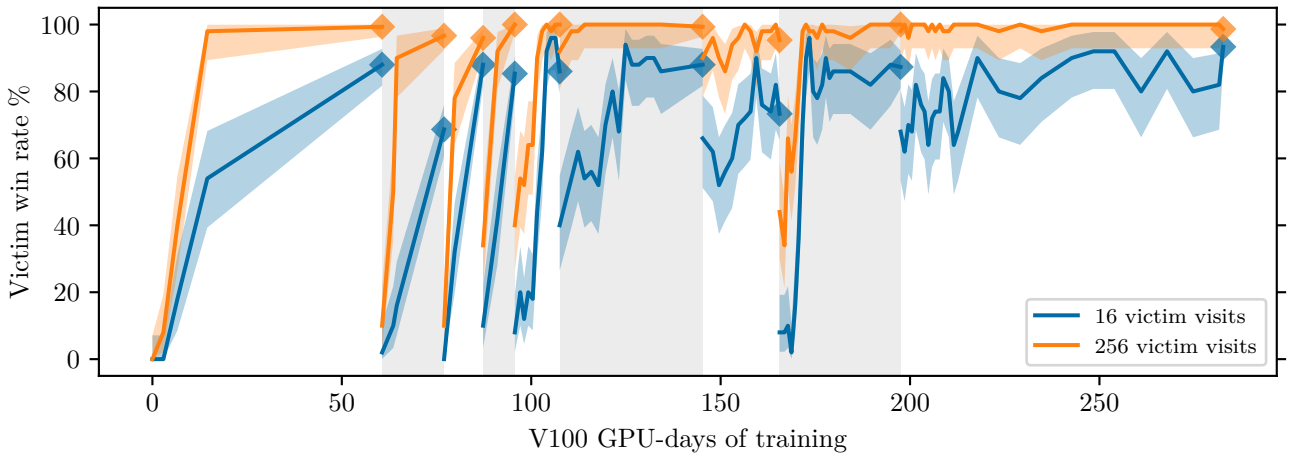


Figure F.1: The victim $\mathtt{v}_n$ win rate (%) against $\mathtt{a}_{n-1}$ throughout iterated adversarial training. Iterations are signified by alternating between a white and grey background. The curves for $\mathtt{v}_1$ to $\mathtt{v}_4$ only have a few data points along the x-axis as intermediate checkpoints were lost.

F. Iterated adversarial training

F.1. Defense

At each iteration, we train a victim $\mathtt{v}_n$ to defend against a fixed adversary $\mathtt{a}_{n-1}$. Figure F.1 shows the training progress of each $\mathtt{v}_n$ against $\mathtt{a}_{n-1}$. Figure M.1 shows the same information but with a separate plot for each iteration. We see that the victim always made rapid progress in defending against the adversary, but continued to lose a significant fraction of the time at 16 victim visits, and still suffered occasional losses at 256 victim visits.

The first $\mathtt{v}_1$ is warm-started from $\mathtt{v}_0$ (`base-victim`) and is trained against `base-adversary`. We do not use a curriculum in victim training. We reduced the learning rate by a factor of 10 from KataGo's default since the base model `base-victim` had been trained with a lower learning rate scale as well. We found that fine-tuning with the default learning rate led to a large initial drop in model strength.

The victim plays with 300 MCTS visits, while the adversary plays with 600 A-MCTS visits. We chose 600 A-MCTS visits for the adversary to follow the default number of visits for adversary training and evaluation used by Wang et al. (2023a). We chose 300 MCTS visits for the victim because it keeps the inference cost of the victim similar to the adversary's—roughly $600/2 = 300$ visits of the adversary's A-MCTS invoke the victim model, with the remaining visits invoking the smaller, cheaper adversary model.

The training window size begins at 68 million rows to match the window size of `base-victim`.** This is large enough that throughout defense training, all games generated in prior defense iterations remain in the training window. Although keeping all the games in the window was not an intentional design choice, it likely contributes to each $\mathtt{v}_n$ defending well against every $\mathtt{a}_m$ with $m < n$.

The victim was trained with a mixture of self-play games and games against the adversary. Self-play games help preserve general Go strength, whereas games against the adversary focus on overcoming specific attacks. We set the game mix to 82% self-play and 18% against the adversary. This proportion was based on preliminary experiments suggesting that training on 90% self-play data and 10% adversary data makes rapid progress in overcoming the adversary without compromising general Go strength (estimated via win rate against `base-victim`). Self-play games generate twice as much policy training data as games against the adversary because the model only trains on its own moves in adversary games. Setting the proportion of selfplay games to 82% makes the generated game data roughly match 90% from self-play.

For simplicity, we only used Tromp-Taylor rules, since the adversaries were also only trained on these rules. We also disabled many KataGo self-play flags (auto-komi, komi randomization, handicap games, game forking, cheap

**The window size was calculated from Eq. (1) using the fact that `base-victim` was trained on 2.9 billion rows of data.

Iteration	Victim		Adversary	
n	GPU-days	Steps (M)	GPU-days	Steps (M)
1	61	61	238	150
2	16	22	439	253
3	10	16	273	213
4	8	11	1195	983
5	12	10	862	535
6	38	20	304	228
7	20	13	491	372
8	32	32	308	230
9	85	71	1005	622
Total	**282**	**256**	**5114**	**3587**

Table F.1: The cost of training the victim $\texttt{v}_n$ and adversary $\texttt{a}_n$ at each iteration n of iterated adversarial training.

search, reduced search when winning, playing initial moves directly from policy) to simplify implementation.

In each iteration, we hand-select the final model for the subsequent iteration based on expected strength. All else equal, we choose the checkpoint with the highest win rate against the adversary. However, as the win rate against the adversary tends to plateau, we additionally favor checkpoints from *stable* periods of training where immediately preceding and succeeding checkpoints also have high win rates. We break ties in favor of earlier checkpoints.

F.1.1. Defense per-iteration

In this section we discuss each individual iteration in more detail. We provide the training cost (in training steps and V100 GPU-days) of each iteration in Table F.1. Additionally, we discuss any configuration changes or notable results that occurred in iterations below.

Defense iteration 1: The win rate at 300 victim visits against the cyclic adversary already plateaued after 14 of the 61 GPU-days (16 of 61 million steps), but we continued training in hopes of achieving a consistent 100% win rate against the adversary.

Defense iteration 4: An error occurred in populating the training history, where extra data from running the previous defense iteration was added for an additional 58 million steps beyond our selected checkpoint $\texttt{v}_3$. We identified this error and removed the extraneous data for subsequent defense rounds.

Defense iteration 6: In iteration 6 and 7 we unintentionally generated games faster than we were training on them, which is why the GPU-days relative to the number of training steps is higher.

Defense iteration 9: We ran this iteration longer than usual because it was our final defense iteration. We also noticed that its win rate at 8 visits increased modestly (from 49% to 74% at the end of training), even though the training win rate at 300 visits against $\texttt{a}_8$ remained around 97% for the entire run.

F.2. Attack

At each iteration, we train an adversary $\texttt{a}_n$ to attack $\texttt{v}_n$ warm-starting from the previous adversary $\texttt{a}_{n-1}$. The very first iteration $\texttt{a}_1$ is warm-started from $\texttt{a}_0 = \texttt{base-adversary}$. Figure F.2 shows the training progress of each $\texttt{a}_n$ against $\texttt{v}_n$. Figure M.2 shows the same information but with a separate plot for each iteration.

As can be seen in Fig. 3.2, the adversaries at iterations 5, 6 and 8 perform especially poorly for victim visits of 16 or above. The main reason for this is that training progress significantly slowed down; the number of victim visits reached by each iteration from $\texttt{a}_5$ onwards was at most 64. Additionally, in iterations 6 and 8, those adversaries were trained for relatively brief periods. The computational expense of training potent attacks is a bottleneck to

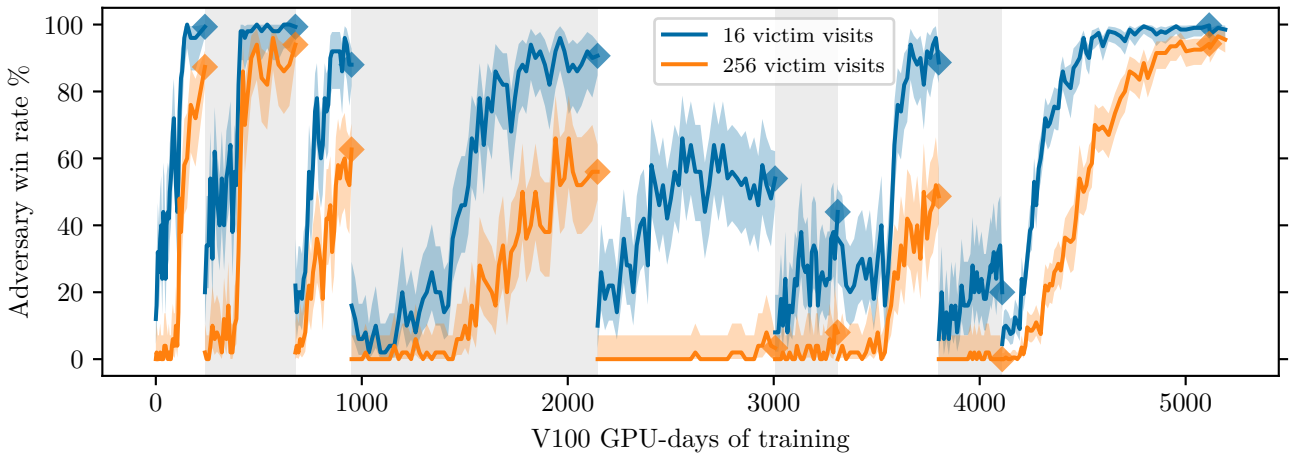


Figure F.2: The adversary $\mathtt{a}_n$ win rate (%) against $\mathtt{v}_n$ throughout iterated adversarial training. Iterations are signified by alternating between a white and grey background.

performing a large number of iterations of adversarial training.

The adversary plays with 600 A-MCTS visits. Initially the curriculum for each adversary $\mathtt{a}_n$ consisted of intermediate checkpoints from $\mathtt{v}_n$'s training run before advancing to $\mathtt{v}_n$ with doubling visit counts. We manually selected intermediate checkpoints by looking at the win rates of $\mathtt{v}_n$'s intermediate checkpoints against $\mathtt{a}_{n-1}$ and sampling checkpoints with varied win rates. Later we found that the victim $\mathtt{v}_n$ at 1 visit was always vulnerable to attack, so we simplified the curriculum by no longer using intermediate checkpoints and instead started the curriculum at the final $\mathtt{v}_n$ checkpoint with very low visit counts.

The final $\mathtt{a}_n$ model we select from a training run is always the latest model checkpoint since win rate increases fairly consistently with more training. We did not have a consistent stopping criterion for each iteration, but we generally targeted either a high win rate at a particular number of visits or restricted the run to a rough training step budget. Unlike in defense training, because the adversary training is longer and the training window is smaller, the data from the previous iteration fully exits the training window (within 132 million training steps) in every iteration.

F.2.1. Attack strategies

All of the adversaries $\mathtt{a}_n$ exploit a cyclic group, but there are still some qualitative differences. In particular, $\mathtt{a}_1$ emphasizes a small alive group inside the victim's cyclic group and coaxes the victim to form a cyclic group with an eye, in contrast to the original cyclic attack of Wang et al. (2023a). $\mathtt{a}_2$ creates a very large group inside the victim's cyclic group. In the middle iterations $\mathtt{a}_4$ to $\mathtt{a}_6$, the inside group is small. In most attacks, the adversary sets up the inside group early and allows the victim stake out territory around it. However, in $\mathtt{a}_4$ to $\mathtt{a}_6$, the adversary instead stakes out its own territory with the destined inside group on the edge. It then allows the victim come into its territory, resulting in it separating off the inside group and forming the cycle.

Meanwhile, in iterations 7 through 8, the adversary forms an inside group with kos. For $\mathtt{a}_7$ and $\mathtt{a}_8$ there are between 1 and 3 kos – in small sample analysis, there were most often 2 or 3 kos for $\mathtt{a}_7$ and 1 for $\mathtt{a}_8$, with more variable inside group shape. With $\mathtt{a}_9$, it initially converged to 2 kos and a highly consistent inside group shape, but then abandoned the kos and started making a diamond, "ponnuki"-like inside shape, which the victim surrounds with a square shape. This results in a small, nearly minimal inside group at the time of the final capture. An example of this is shown in Fig. E.1c.

In Appendix L, we plot heatmaps of the inside and cyclic group locations. Paralleling the qualitative analysis above, we observe differences in where they are concentrated and their sizes. We also notice some variations in victim stone concentration. Overall, we find clear but constrained evolution in the attacks. To humans, the differences do not change the difficulty of gameplay—the attacks all fit very well in the same overall type (cyclic

attacks) so knowing how to beat one would almost certainly mean knowing how to beat them all. But to the KataGo victims, the representations learned do not appear to generalize smoothly between these variations.

F.2.2. Attack per-iteration

In this section we discuss each individual iteration in more detail. We provide the training cost (in training steps and V100 GPU-days) of each iteration in Table F.1. Additionally, we discuss any configuration changes or notable results that occurred in the iterations below. We denote an intermediate checkpoint S million training steps into the n-th iteration of defense training as $\texttt{v}_n\texttt{-sSm}$.

Attack iteration 1: The curriculum consisted of $\texttt{v}_1\texttt{-s4m}$ with 128 visits, $\texttt{v}_1\texttt{-s16m}$ with 32–128 visits, and $\texttt{v}_1$ with 32–1024 visits, with a win rate threshold of 75%. We stopped the run due to hitting a large number of victim visits, which slowed the generation of training data.

In this iteration, we made an error when warm-starting from the original cyclic adversary. When we copied the original cyclic adversary's training history, timestamps were erased. Therefore, at the start of the run, the training window contained the original cyclic adversary's After 122 of 238 V100 GPU-days (41 of 150 million training steps), all these data left the window. The most likely effect of this error was hindering early training progress, though it is also possible that it inadvertently helped encourage exploration in early training.

Attack iteration 2: The curriculum consisted of $\texttt{v}_2\texttt{-s4m}$ with 128 visits, $\texttt{v}_2\texttt{-s5m}$ with 64–128 visits, and $\texttt{v}_2$ with 64–1024 visits, with a win rate threshold of 75%. Once again we stopped the run due to hitting a large number of victim visits.

Attack iteration 3: The curriculum consisted of $\texttt{v}_3\texttt{-s5m}$ with 128 visits and $\texttt{v}_3$ with 64–256 visits. Here, we stopped at a 75% training win rate against 256 victim visits because we had used about as much compute as in previous attack iterations and considered 256 visits to be a sufficiently large number of visits that the attack likely transfers, at least somewhat, to high visits.

Attack iteration 4: The curriculum consisted of $\texttt{v}_4\texttt{-s5m}$ with 128 visits and $\texttt{v}_4$ with 4–256 visits. We aimed for a training win rate of 75% against $\texttt{v}_4$ at 256 visits but halted early as we found training progress to be much slower than in previous iterations.

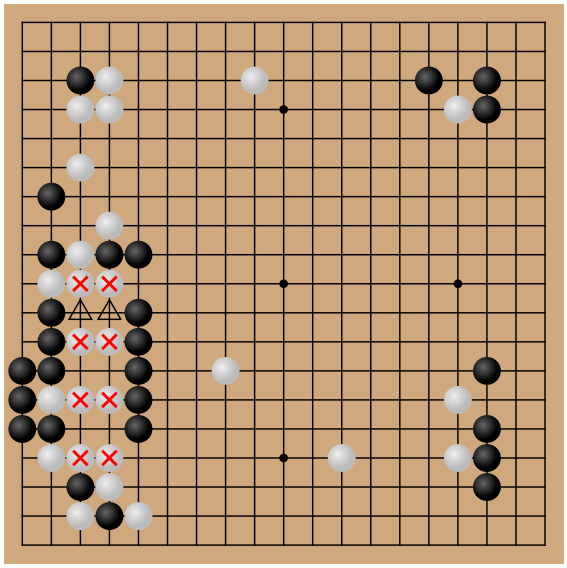
Initially, the curriculum jumped from $\texttt{v}_4\texttt{-s5m}^{128\text{ visits}}$ to $\texttt{v}_4{}^{64\text{ visits}}$ but the win rate against $\texttt{v}_4{}^{64\text{ visits}}$ was very low at 3%, and it did not appear to be trending upwards. After this, we reverted the curriculum back to $\texttt{v}_4\texttt{-s5m}^{128\text{ visits}}$ and enabled LCB move selection, which remained enabled in all subsequent attack iterations as well. The result of enabling LCB move selection was a lower training win rate, presumably due to the victim playing more strongly.

The hope was that training against the earlier checkpoint $\texttt{v}_4\texttt{-s5m}$ for longer would yield stronger performance once the curriculum advanced to $\texttt{v}_4$, but we still had a low win rate of 5% when we reached $\texttt{v}_4{}^{64\text{ visits}}$.

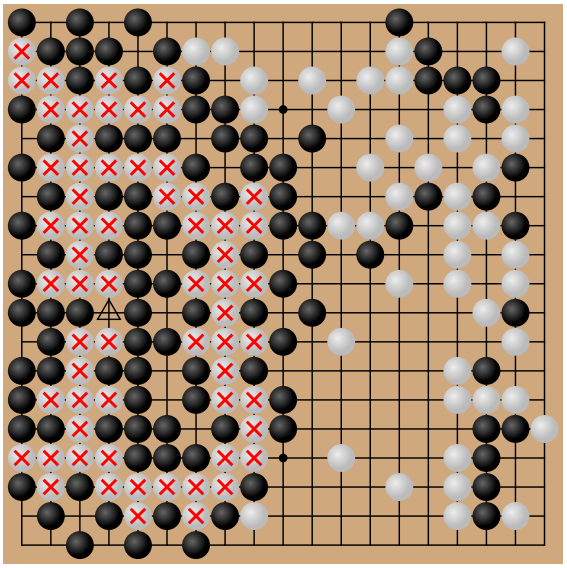
We then changed the curriculum to reduce the starting visit count for $\texttt{v}_4$ from 64 to 4, which worked better. We suspect that we could have skipped the $\texttt{v}_4\texttt{-s5m}$ intermediate checkpoint entirely and immediately initialized the curriculum at $\texttt{v}_4$ with 4 visits, saving 420 V100 GPU-days and 360 million steps of training. We therefore stopped using intermediate curricula checkpoints in subsequent attack iterations and switched to starting the curriculum against the target victim $\texttt{v}_n$ at very low visits.

Attack iteration 5: The curriculum consisted of $\texttt{v}_5$ with 4–32 visits. We halted this run because progress was slow, and it did not look like we would reach higher victim visits within our compute budget.

Attack iteration 6: From this point onward, we did not anticipate reaching high victim visits during training, so we decided to run each attack iteration for around 250 million training steps, although it is not entirely clear that running defense iterations against weak adversaries provides useful training signal on the defense side. We trained $\texttt{a}_6$ against a curriculum of $\texttt{v}_6$ with 4–16 visits.



(a) `atari-adversary` induces the victim to set up several bamboo joints (×). These are normally strong shapes for connecting, e.g., if black plays a triangle-marked location, white can play the other to keep the joints connected.



(b) Ultimately, `atari-adversary` threatens to split one of the bamboo joints, and the victim prevents that by playing at the triangle location. But this is a terrible mistake—on the next move, the entire cyclic group will be captured.

Figure F.3: The cyclic "bamboo joint" strategy learned by `atari-adversary`; explore online.

Attack iteration 7: We trained $\texttt{a}_7$ against a curriculum of $\texttt{v}_7$ with 4–64 visits. We initially intended to train $\texttt{a}_7$ for only 200 million steps, but the win rate in both training and evaluation started increasing noticeably faster at 190 million steps (272 V100 GPU-days), so we extended the training duration.

Attack iteration 8: We trained $\texttt{a}_8$ with a curriculum of $\texttt{v}_8$ with 4–16 visits.

Attack iteration 9: We trained $\texttt{a}_9$ against a curriculum of $\texttt{v}_9$ with 4–512 visits, raising the win rate threshold from 75% to 90% at 256 visits. At 82 GPU-days (74 million steps), we adjusted the victim configuration parameters to match evaluation settings as described in Appendix D.2 due to a large gap between training and evaluation win rates, and because a higher training win rate was not leading to stronger evaluation strength. We also updated adversary configuration parameters as described in Appendix D.2.

No defense iteration trains against $\texttt{a}_9$. We trained $\texttt{a}_9$ to see whether it could successfully attack $\texttt{v}_9$.

F.3. Validation attack

In Section 3.2.2, we found that the final iterated adversarially trained victim $\texttt{v}_9$ can be readily exploited at low visits by the validation attack `atari-adversary`. This attacker was warm-started from `base-adv-early`. We used a curriculum of $\texttt{v}_9$ starting at 1 victim visits and doubling until it reached 512 visits (curriculum changes denoted by dotted lines in Fig. F.4). The curriculum win rate threshold was 75% until reaching 256 visits, at which point the threshold increased to 90%. We modified the bot configurations as described in Appendix D.2 to make the victim configuration closer to evaluation settings and the adversary configuration closer to the latest KataGo training runs.

Although `atari-adversary` beats $\texttt{v}_9$ at low visit counts, we did not find an attack that achieved a high win rate against $\texttt{v}_9$ at high visit counts. However, `atari-adversary` was only trained for 6% as much compute as $\texttt{v}_9$, raising the question: how well would the attack perform were we to continue this training run? More generally, can we predict how much more compute it would take to scale `atari-adversary` to achieve, say, a 10% win rate against $\texttt{v}_9$ at 65,536 visits?

Unfortunately, training dynamics are hard to forecast in advance. For instance, `base-adversary` made little progress for a few hundred GPU-days before abruptly finding a strategy that generalized to attack `base-victim`

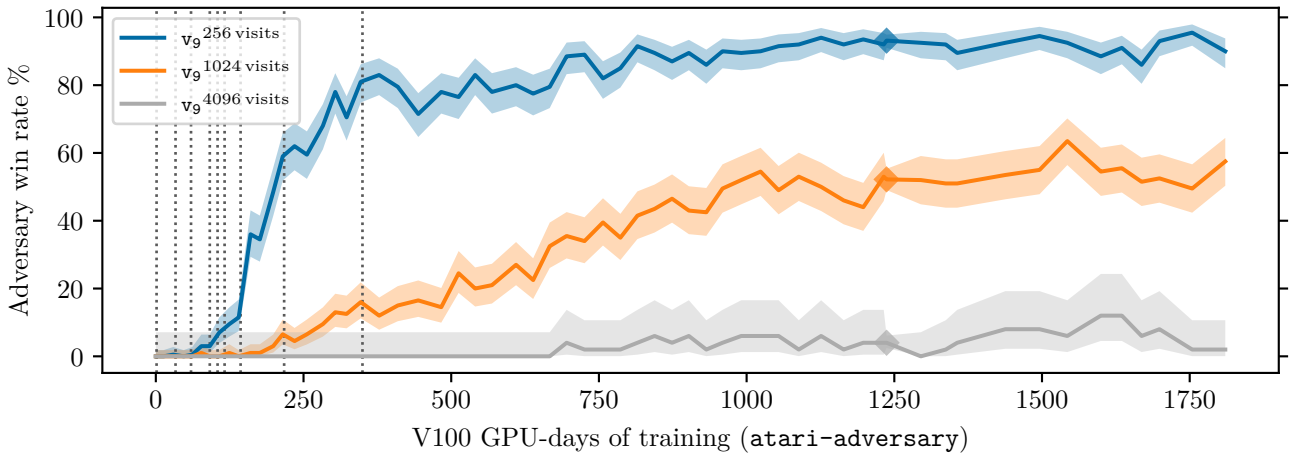


Figure F.4: Win rate of `atari-adversary` (♦) against v_9 throughout `atari-adversary` training, warm-starting (at $x = 0$) from `base-adv-early`. Curriculum changes are denoted by a vertical dotted line.

at high visits (Wang et al., 2023a; Gleave, 2023). Looking at the training progress for `atari-adversary` (Fig. F.4), `atari-adversary` makes fairly consistent progress until it stalls out late in the training run. This training curve is consistent both with it plateauing and never achieving high win rates against high victim visits, or it suddenly hitting a phase change in training like `base-adversary` did and shooting up.

Therefore even with the slowing progress of `atari-adversary` late in its training and its inability to win against v_9 at 8192 visits, we cannot conclude that v_9 is invulnerable at high visits. Indeed, a_9 achieves a 42% win rate against v_9 at 65536 visits, showing that there is available attack surface at high visits. This is despite a_9 only training against v_9 up to 512 visits.

This brings up another question: how can we encourage adversary training to find strategies that are likely to generalize against high visits? `continuous-adversary`, `gift-adversary`, a_9, and `atari-adversary` only trained against their victims up to 512 visits. Yet `continuous-adversary` and a_9 generalize to high visits, whereas `gift-adversary` and `atari-adversary` do not. Likewise, Wang et al. (2023a) found one strategy that generalizes to high visits (`base-adversary`) and one that does not (their "pass-adversary").

One hypothesis is that `continuous-adversary` and a_9 simply used more training compute. Another is that training is highly path-dependent, so initialization, training curriculum, or randomness matter—`continuous-adversary` and a_9 were initialized from later adversary checkpoints and had a curriculum involving intermediate victim model checkpoints, whereas `gift-adversary` and `atari-adversary` were initialized from `base-adv-early` and had coarser curricula not involving intermediate victim models. `continuous-adversary` and a_9 were initialized from checkpoints `attack-may23` and `base-adversary` that already work against some strong high-visit victim, which may be important in biasing them away from discovering another vastly different fragile strategy that only works at low visits.

G. Vision transformers

In this appendix, after first summarizing our results, we provide an overview of our vision transformer (ViT) architecture and describe our ViT training procedure. For full architectural details, see our PyTorch implementation: `https://github.com/AlignmentResearch/KataGo-custom/blob/stable/python/model_pytorch.py`.

G.1. Results summary

Wang et al. (2023a)'s attack works not only against KataGo but also against a range of other superhuman Go AIs such as ELF OpenGo (Tian et al., 2019), Leela Zero (Pascutto, 2019b), Sai (Morandin et al., 2019), Golaxy (北京深客科技有限公司, 2018), and FineArt (Tencent, 2017). While it is possible that each of these systems is vulnerable to the cyclic attack for a different reason, it is more likely that shared properties such as their convolutional neural network (CNN) backbone cause their shared vulnerability.[††] Indeed, KataGo's developer proposed that vulnerability to cyclic attacks may be a result of the CNN backbone learning a local algorithm for classifying if a group is alive that fails to generalize to larger groups (polytope, 2023). However, we demonstrate that superhuman Go AIs with vision transformer (ViT) backbones are also susceptible to cyclic attacks. This suggests the shared weakness is either AlphaZero-style training—or deep learning more generally.

Since no prior work has trained strong Go AIs with a ViT architecture,[‡‡] we set out to train the first professional-level ViT-based Go AI. We follow a training recipe similar to the one used by KataGo (Wu, 2022c), except we replace the CNN backbone with a ViT (Appendix G). Our strongest ViT network, which we label `ViT-victim`, was trained for 537 V100 GPU-days. It is slower to train than a CNN agent and weaker at the same inference budget, but we estimate it still reaches near-superhuman levels when playing with 32768 visits. This estimate is derived from benchmarking against KataGo, pitting our agent against players on the KGS Go Server, and winning two out of three games against Go professionals (Appendix H).

Despite the new architecture, Figure 3.1 shows that our `ViT-victim` (at 65536 visits) remains vulnerable to the cyclic attack, losing 78% of games to a fine-tuned version of `base-adversary`, which we call `ViT-adversary` (Appendix G.6). `ViT-adversary`'s strategy resembles other cyclic attacks but is qualitatively distinct in its tendency to produce small groups inside the cyclic one, and dense board states with limited open space (Fig. E.1d). This attack can be replicated by a human expert (Appendix I).

Remarkably, `ViT-victim` (at 512 visits) also loses 2.5% of games to the original `base-adversary`—similar to the zero-shot transfer to CNN Go AIs such as ELF OpenGo reported by Wang et al. (2023a). This definitively shows that a CNN architecture is not the cause of the cyclic vulnerability. `base-adversary` certainly does not win through legitimate means: it is a very weak strategy that loses to amateur human players (Wang et al., 2023a).

G.2. ViT inputs

Our ViTs take in the same inputs as standard KataGo CNNs, namely two tensors of spatial and global features.

The spatial features are represented by a three-dimensional binary tensor $\mathbf{S}$ taking values in $\{0,1\}^{\texttt{height}\times\texttt{width}\times 22}$, where `height` and `width` are the maximum Go board dimensions the model supports (usually 19). In other words, each point of the Go board has 22 binary features associated with it. These features encode various properties such as whether a point is occupied, the color of a stone on a point, move history, and more complicated features like whether a point is involved in a potential ladder. For an exact specification of these features, see this source file: `KataGo/cpp/neuralnet/nninputs.cpp`.

The global features are represented by a real-valued vector $\mathbf{G}$ taking values in $\mathbb{R}^{19}$. These 19 features encode properties like which of the past 5 moves were passes, and the particular ruleset the current game is using.

[††]Golaxy and FineArt are closed-source but likely use the same design principles as other Go AIs.

[‡‡]Sagri et al. (2024) train ViT-based Go AIs but did not validate the strength of their systems or release weights. Moreover, they used supervised learning on KataGo self-play data generated by CNN agents, whereas we trained our ViT agents only on ViT-generated self-play data.

G.3. ViT architecture

Our ViT network replaces the KataGo CNN backbone with a transformer-based backbone, but reuses the same output layers as KataGo's networks (Figure G.1). Both our transformer backbone and the KataGo's CNN backbone output a real-valued tensor with dimensions `height` × `width` × c, where c is the embedding / residual-stream dimension of the network. This embedding tensor is processed by the standard KataGo output layers to produce the outputs KataGo expects networks to have: a scalar that estimates the value function, a vector that represents the next-move policy, etc. Our transformer backbone is built using a standard HuggingFace `transformers.ViTModel`.

Input preprocessing We zero-pad the spatial dimensions of **S** so that they are divisible by our ViT patch size (`patch_size=2`). We then expand **G** so it has shape `padded_width` × `padded_height` × 19 and concatenate it with **S** to form the actual input to our `ViTModel` of shape `padded_width` × `padded_height` × 41.

Unembedding The Huggingface `ViTModel` outputs a tensor of shape `n_patches` × c. We linearly project this tensor to one of size `height` × `width` × c in the canonical way that preserves spatial locality.

Architecture hyperparameters We tried a few different ViT architecture hyperparameters and measured how quickly they trained with supervised learning on training data from `katagotraining.org`. We found the following hyperparameters to work fairly well:

Patch size	# Attn. heads	Embedding dim.	MLP dim.
2	6	384	1536

We trained networks of varying depths, ranging from a 4-layer ViT to a 16-layer ViT. See Appendix section G.5 for more details.

Name	Model type	# Layers	Embedding dim.	# Parameters
`ViT-b4`	ViT	4	384	7,952,501
`ViT-b8`	ViT	8	384	15,050,357
`ViT-b16`	ViT	16	384	29,246,069
`b6c96`	CNN	6	96	1,001,613
`b10c128`	CNN	10	128	2,959,329
`b15c192`	CNN	15	192	9,875,893
`b20c256`	CNN	20	256	23,413,525
`b40c256`	CNN	40	256	46,632,501
`b18c384nbt`	CNN	18	384	26,389,941

Table G.1: Comparison of our ViT nets to KataGo CNNs in terms of depth, width, and parameter count.

G.4. ViT implementation

KataGo implements its architectures in Python for training and C++ for self-play. Because implementing models in C++ is fairly complex, we only implement the ViT in Python using PyTorch. To use ViTs during inference, we export the PyTorch model as a TorchScript model and modify KataGo's C++ code to be able to invoke TorchScript models. Since TorchScript models are made to be serialized and executed independently of Python, this removes the need to implement the ViT itself in C++.

However, this comes at the cost of slower inference. On our machines, running inference for a `b18c384nbt` or `b20c256` KataGo CNN model using TorchScript incurred a 43% and 28% slowdown, respectively, compared to running them with KataGo's C++ CUDA implementation.

G.5. Self-play training

In this section we describe our self-play training process for our ViT agent `ViT-victim`.

G.5.1. Network scaling

In our ViT training run, we start with a small 4-block ViT network that is quick to generate data. When the smaller model hits capacity, we switched to an 8-block network, and then finally switch to a 16-block network. We perform each switch by first pre-training the larger model on the smaller model's data, using the typical sliding training window method described in Appendix D.1 to sample training data, but using the smaller model's existing self-play games as data. We copy the smaller model's data into the pre-training dataset gradually in chronological order, copying roughly one epoch's worth of data after each pre-training epoch, so pre-training ends by training on the latest and presumably strongest data. We discard some of the smaller model's early data under the assumption that training on it would take extra time without much benefit due to the data being lower quality. We still increment N in Eq. (1) to keep the window size as large as it would have been had we not discarded the data.

G.5.2. Training configuration

Our configuration parameters matched those suggested by KataGo's example self-play configurations available in its codebase, except that we only used Tromp-Taylor rules instead of having rule variation, did not play any games on rectangular boards, and increased the percentage of 19x19 games to 53.6% to match the latest KataGo training runs. We trained exclusively on Tromp-Taylor rules because we always evaluate models under these rules, and our adversaries like `base-adversary` were all trained only under Tromp-Taylor rules.

KataGo also seeds 14% of its self-play games from custom positions that are rarely encountered in typical self-play (Wu, 2023d). This improves play on tricky positions like Mi Yuting's Flying Dagger joseki and improves analysis on human games (Wu, 2021a). Since we do not have access to this set of games, we do not include it in our ViT training run.

G.5.3. ViT training run

Figure G.2 shows the strength of our networks throughout self-play training. We successively trained three ViT networks (4-block, 8-block and 16-block) along with a control 10-block CNN. Larger ViT networks reached a higher Elo but quickly saturated. However, the ViT networks did not necessarily reach model capacity, as we were able to reach still higher Elo ratings by distilling KataGo CNN self-play training games into the ViT network.

We started with training a 4-block ViT with 600 visits using a configuration matching an example KataGo configuration, similar to the actual configuration used for training KataGo's 6-block and early 10-block networks.[§§] We trained for 64 GPU-days and 213 million steps.

We then switched to a 8-block ViT, pre-training it on the 4-block ViT's latest 24.9 million data rows (100 million training steps). After pre-training (2 V100 GPU-days, 92 million steps), the 8-block ViT was about 175 Elo stronger than the 4-block ViT at 256 visits. We then began self-play with the 8-block ViT. After 20 V100 GPU-days and 48 million steps of self-play, we increased the number of self-play visits to 1000 visits by swapping our configuration to make it similar to that used for training KataGo's 10-block and 15-block nets.[¶¶] At 461 million steps with self-play, we gained about 264 Elo at 256 visits. At this point we spent 301 V100 GPU-days on training the 8-block ViT. It was still making slow training progress, but we decided to switch to a larger architecture in hopes of achieving a faster increase in playing strength.

When we switched to a 16-block ViT, we pre-trained on the latest 24.9 million data rows generated by the 4-block ViT as well as all the data rows generated by the 8-block ViT, totaling 139 million data rows. For this pre-training, we used data-parallel training on 8 GPUs to decrease wall-clock training time. After training had reached 78% of the pre-training data, we noticed signs of overfitting: playing strength decreased, and the ViT's value loss (loss on the model's prediction of whether a position will lead to a win or a loss) was decreasing on training data yet increasing on validation data. We mitigated this by increasing the minimum window size m from 250000 to 10 million in Eq. (1), which roughly quadrupled the current window size. After training on 93%

[§§] KataGo example configuration: `https://github.com/lightvector/KataGo/blob/7488c47b6f6952f9703d9209f9afbd8d38a8afb5/cpp/configs/training/selfplay1.cfg`

[¶¶] KataGo example configuration: `https://github.com/lightvector/KataGo/blob/7488c47b6f6952f9703d9209f9afbd8d38a8afb5/cpp/configs/training/selfplay8b.cfg`

of the data, we reduced the learning rate by a factor of 2 since the loss plateaued.

After pre-training (22 V100 GPU-days, 532 million steps), the 16-block ViT was 286 Elo stronger than the 8-block ViT at 256 visits. We then started self-play. After 75 V100 GPU-days and 74 million steps of self-play, we increased the visits to 2000 and matched a configuration similar to that used for training KataGo's b18 models.*** At 126 V100 GPU-days and 104 million steps of self-play, we reduced the learning rate by another factor of 2. We stopped self-play at 118 million steps of self-play, at which point we had spent 172 V100 GPU-days on 16-block training and gained another 18 Elo at 256 visits. The resulting model is `ViT-victim`. We likely could have trained the ViT for longer—strength was still increasing, albeit slowly. Moreover, when we trained a separate 16-block ViT on training data from `katagotraining.org` generated by KataGo's stronger CNN networks, the resulting model was an estimated 277 Elo stronger than `ViT-victim` at 300 visits, suggesting there is still capacity in `ViT-victim`'s architecture.

G.5.4. Control CNN training run

As a control run, we train a model `control-victim` with a 10-block CNN architecture (`b10c128` in Table G.1). In total, we train it for 121 V100 GPU-days and 419 million steps. We started with the same 600-visit configuration used by the 4-block ViT, and at 29 V100 GPU-days (147 million steps), we switched to the 1000-visit configuration used by the 8-block ViT. At 35 GPU-days and 64 GPU-days (166 million and 251 million steps), we cut the learning rate in half, and at 110 GPU-days (396 million steps), we reduced the learning rate by 40%. By the end of the training run, the model was about as strong as the 8-block ViT.

In Fig. G.2, we see that `control-victim` learned quicker than the 4-block ViT and plateaued at about the same strength as the 8-block ViT, despite the 8-block ViT having five times as many parameters.

G.6. Training `ViT-adversary`

Figure G.3 shows the win rate of `ViT-adversary` against `ViT-victim` throughout `ViT-adversary`'s training. We trained the adversary for 409 V100 GPU-days and 328 million steps, stopping the run once we had high win rates against `ViT-victim` at 32768 visits, which we estimate to be just shy of superhuman (Appendix H). We fine-tuned `ViT-adversary` from `base-adversary` after observing that `base-adversary` is able to win against the final ViT at low victim visits. We used a curriculum of `ViT-victim` starting with 1 visit and doubling until 2048 visits. The curriculum win rate threshold was 75% until the curriculum reached 256 visits, after which the threshold was increased to 90%.

At 262 V100 GPU-days (206 million time steps) the curriculum reached 1024 victim visits. However, we noticed that the training win rate was higher than the evaluation win rate by about 14%, and also that the drop in win rate when the curriculum moved on to a higher visit victim was small. We considered it desirable to train for longer at lower victim visits since it would be cheaper to generate training data and high win rates at low visits were likely to translate to high win rates at high visits. We therefore changed the configuration parameters to bring the victim closer to evaluation settings as described in Appendix D.2. This reduced training win rate, so we rewound the curriculum from 1024 visits to 256 visits. With more training, the curriculum eventually reached 1024 visits again.

G.7. ViT vulnerability throughout training

Figures G.4 and G.5 show the vulnerability of `ViT-victim` to `base-adversary` and `ViT-adversary`. We observe that vulnerability to both adversaries develops early in training and shows no sign of decreasing. Figures G.6 and G.7 show the same results for the control CNN model `control-victim`.

Figure G.8 shows the win rate of `control-victim` against `ViT-adversary` and `base-adversary` at varying amounts of `control-victim` visits (the corresponding plot for `ViT-victim` is Fig. 3.1). We see that `control-victim` is also highly vulnerable to `ViT-adversary`, indicating that `ViT-adversary` is not conducting an architecture-specific attack.

***KataGo example configuration: `https://github.com/lightvector/KataGo/blob/7488c47b6f6952f9703d9209f9afbd8d38a8afb5/cpp/configs/training/selfplay8mainb18.cfg`

In Figs. G.9 and G.10, we plot how the playing strength of `ViT-victim` and `control-victim` throughout training compares to their vulnerability to `base-adversary`. More training yields greater strength but also increased vulnerability. `control-victim` develops vulnerability to `base-adversary` at a weaker strength than `ViT-victim`, suggesting that ViTs may be marginally more robust than CNNs against cyclic attacks at a given strength.

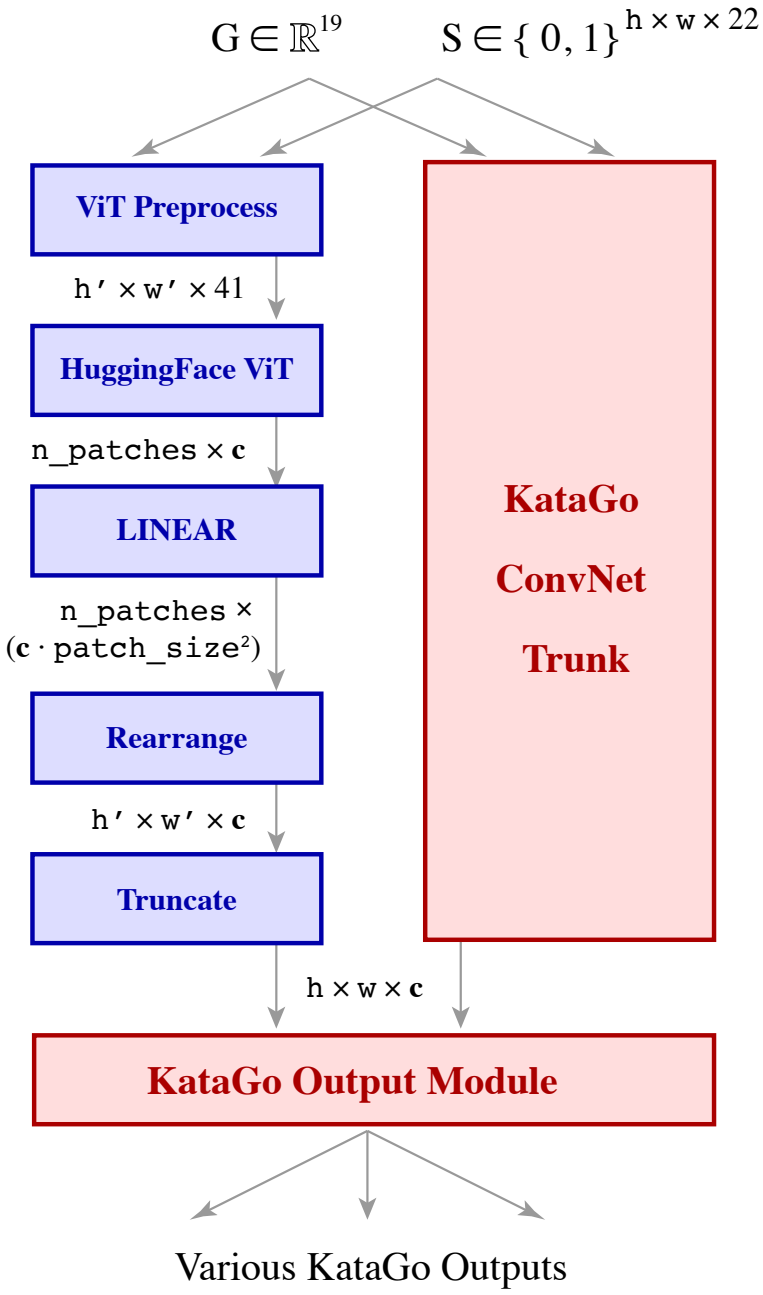


Figure G.1: A diagram comparing our ViT architecture to the standard KataGo CNN architecture. Our ViT architecture replaces the KataGo **CNN backbone** with a **transformer backbone**, and reuses the KataGo CNN output layers. Boxes denote neural network components and unboxed quantities denote tensor shapes.

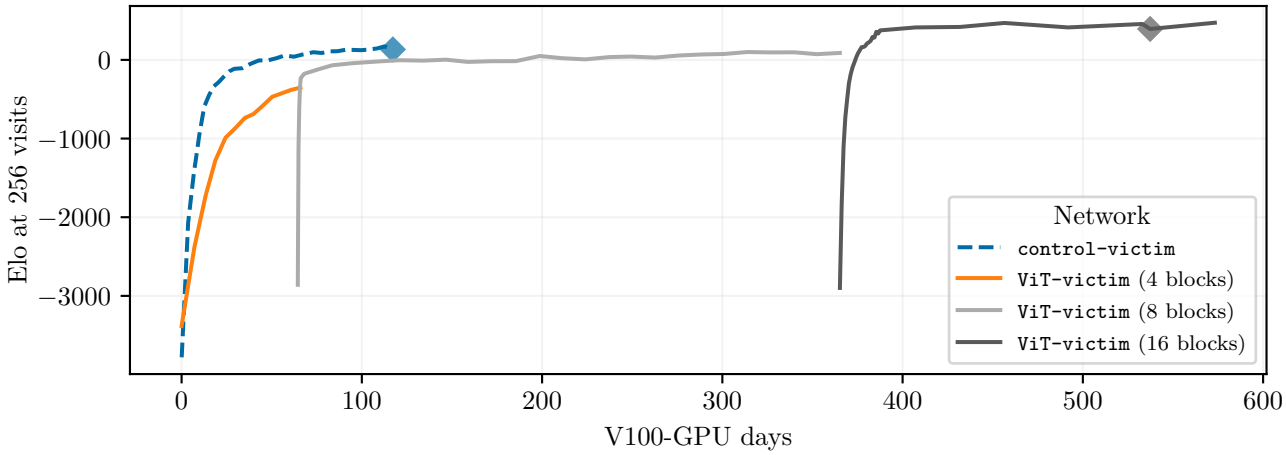


Figure G.2: The strength of our ViTs (`ViT-victim` = black ⧫) throughout their training as well as a control 10-block CNN `control-victim` (blue ⧫) trained with the same settings. Playing strength was estimated by playing the models against each other as well as against a few KataGo networks.

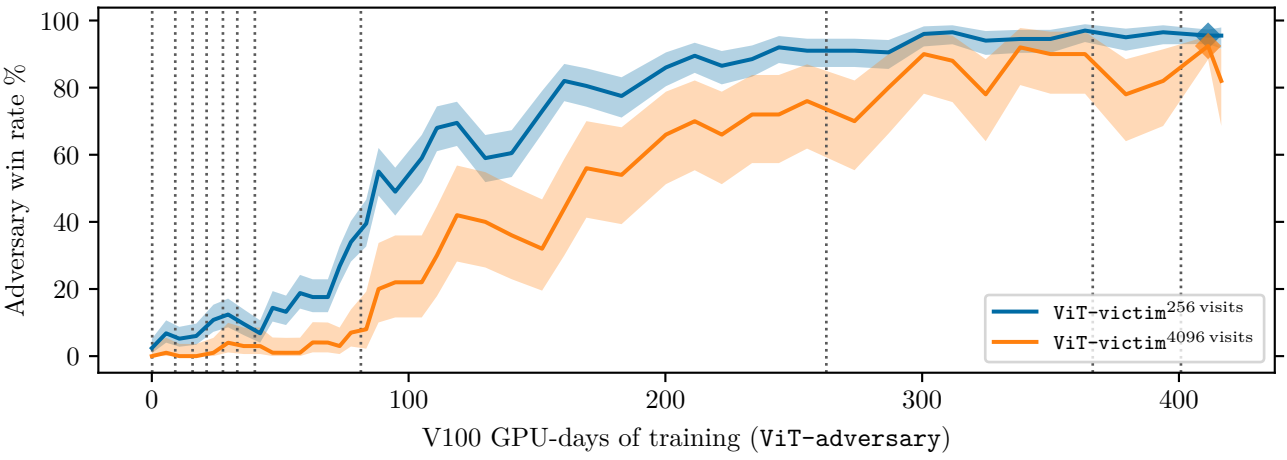


Figure G.3: Win rate (%) of `ViT-adversary` (⧫) against our superhuman ViT agent `ViT-victim` throughout `ViT-adversary` training. The zero of the x-axis represents the win rate of the warm-start `base-adversary` against `ViT-victim` before the fine-tuning against `ViT-victim` began. Dotted lines represent victim visit increases.

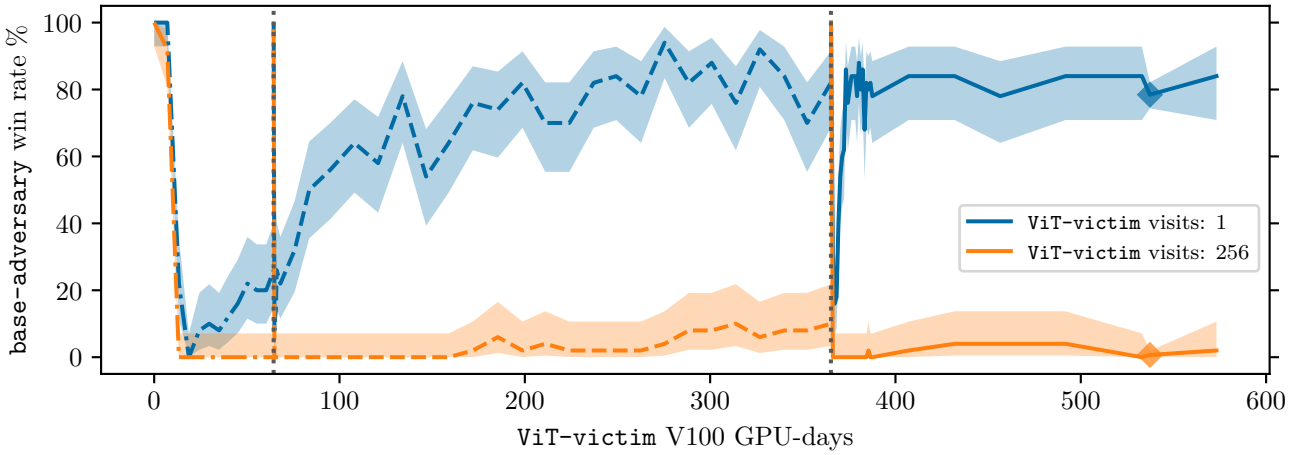


Figure G.4: Vulnerability of `ViT-victim` to `base-adversary` throughout `ViT-victim` training. A dotted gray line represents switching to a larger ViT architecture, at which point the vulnerability drops as the larger architecture is initialized randomly but then quickly rises during pre-training.

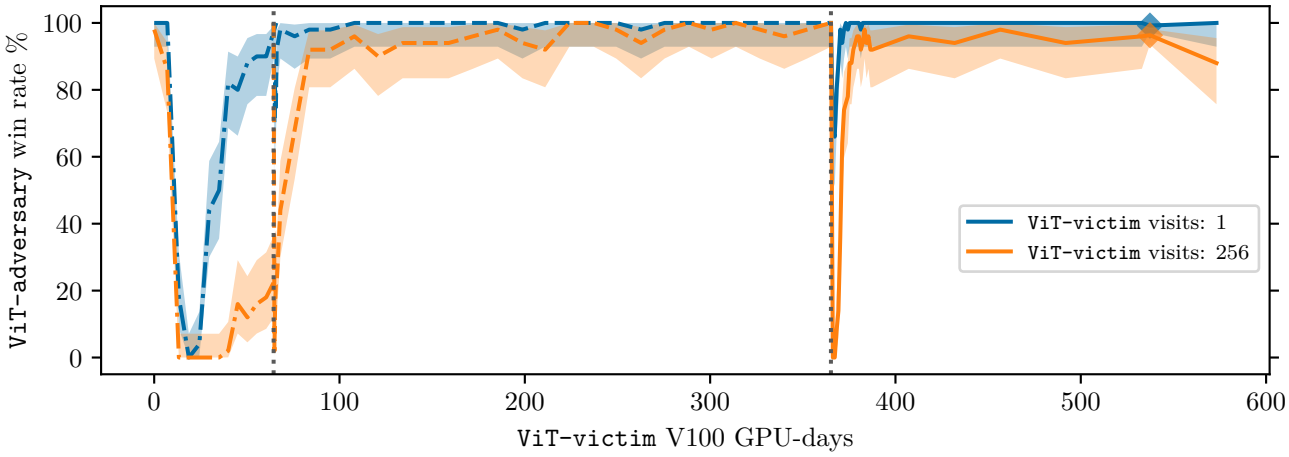


Figure G.5: Vulnerability of `ViT-victim` to `ViT-adversary` throughout `ViT-victim` training. A dotted gray line represents switching to a larger ViT architecture, at which point the vulnerability drops as the larger architecture is initialized randomly but then quickly rises during pre-training.

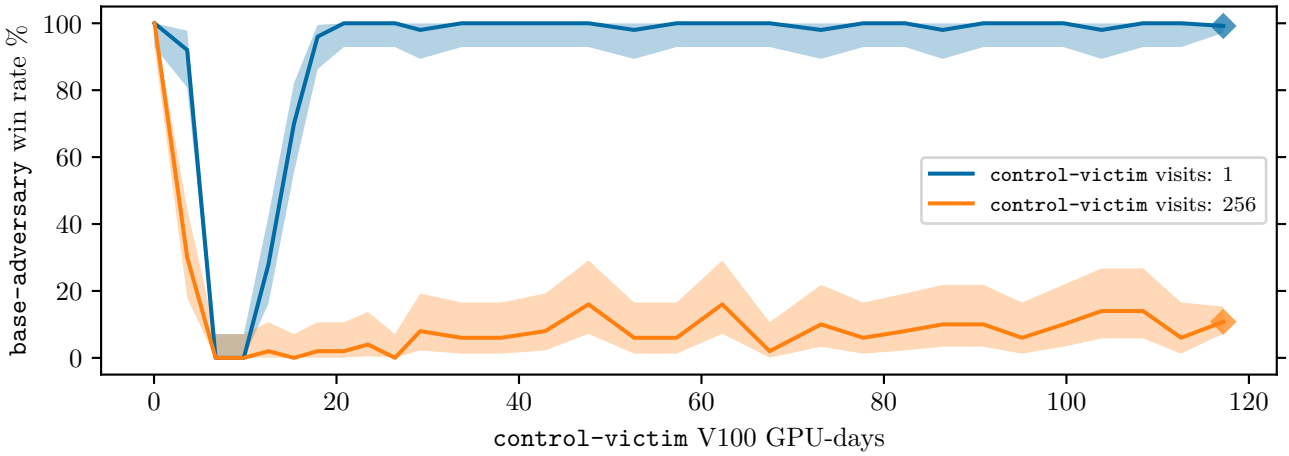


Figure G.6: Vulnerability of `control-victim` to `base-adversary` throughout `control-victim` training.

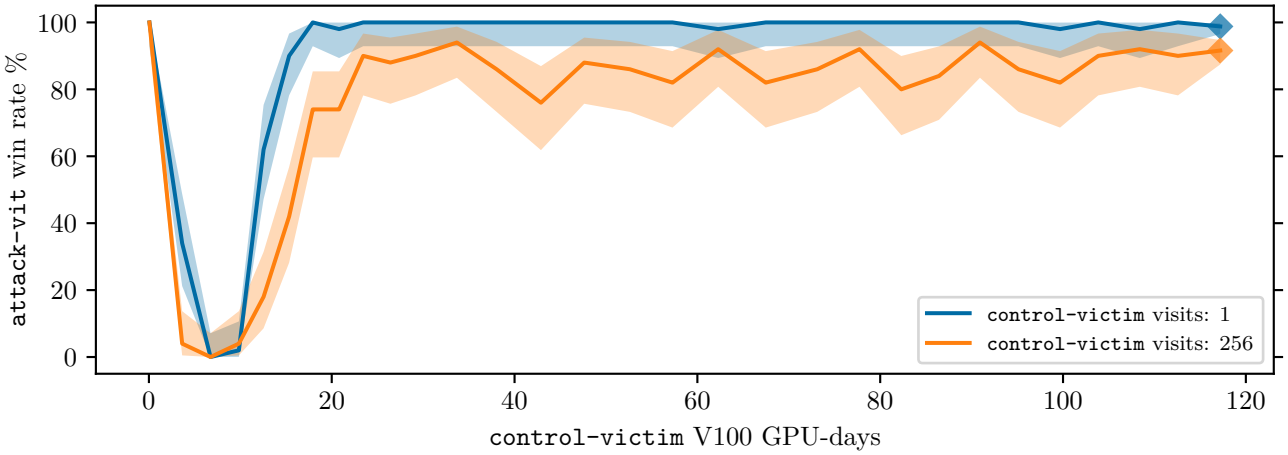


Figure G.7: Vulnerability of `control-victim` to `ViT-adversary` throughout `control-victim` training.

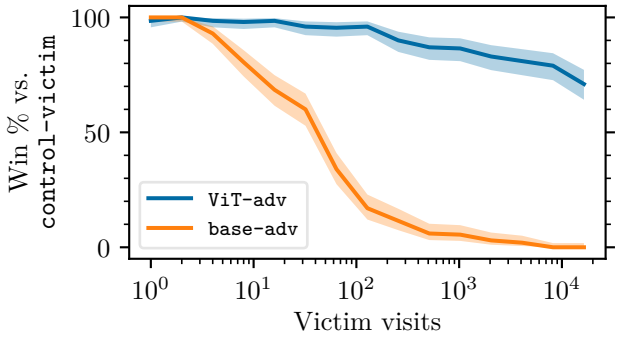


Figure G.8: Win rate (%) for `control-victim` against `ViT-adversary` and `base-adversary`, with varying victim visits.

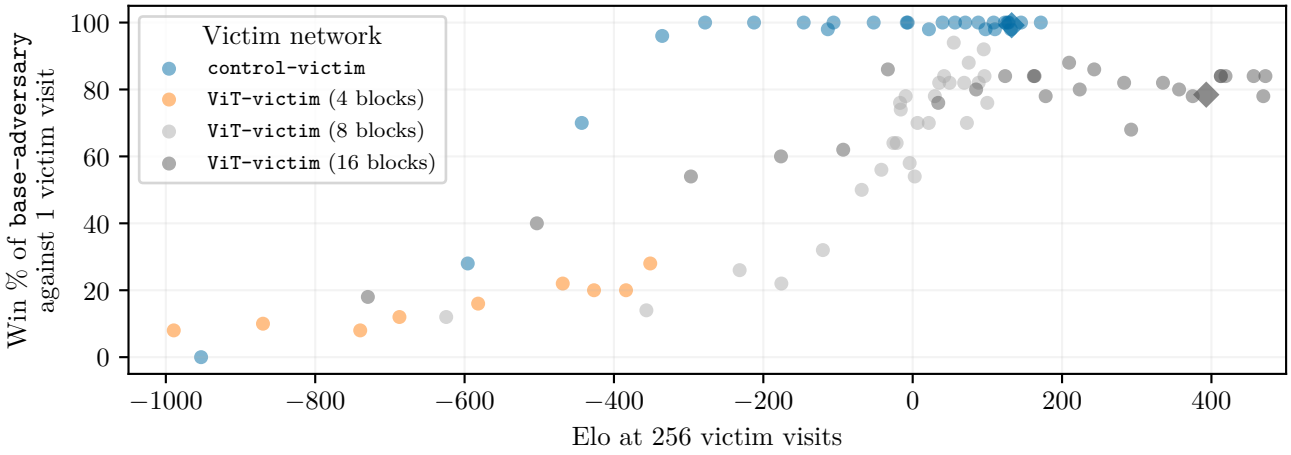


Figure G.9: Plot of several `ViT-victim` (black ♦) and `control-victim` (blue ♦) training checkpoints with their playing strength on the x-axis and their vulnerability to `base-adversary` at 1 victim visit on the y-axis.

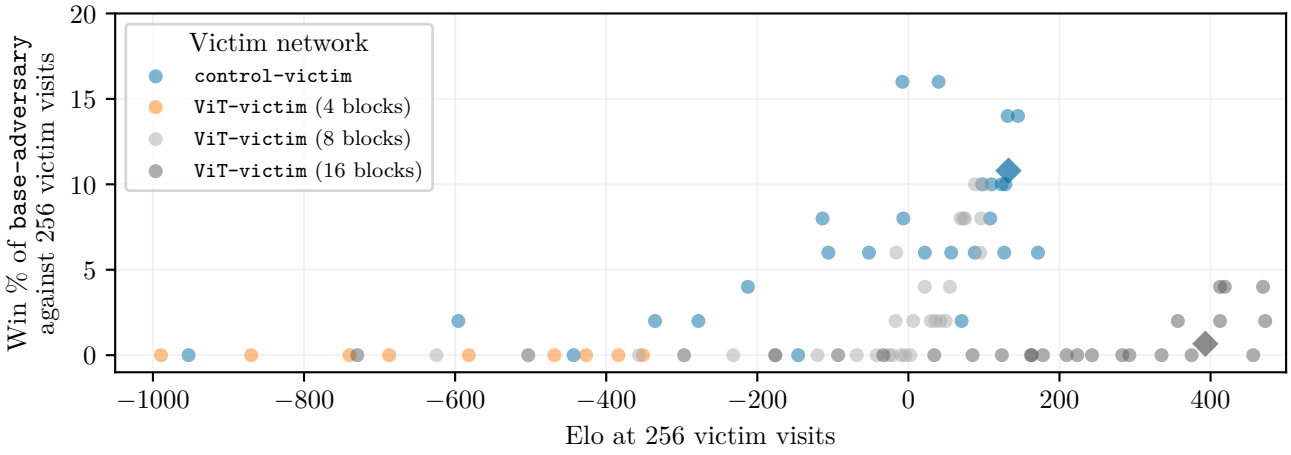


Figure G.10: Same as Fig. G.9 but with vulnerability at 256 victim visits on the y-axis.

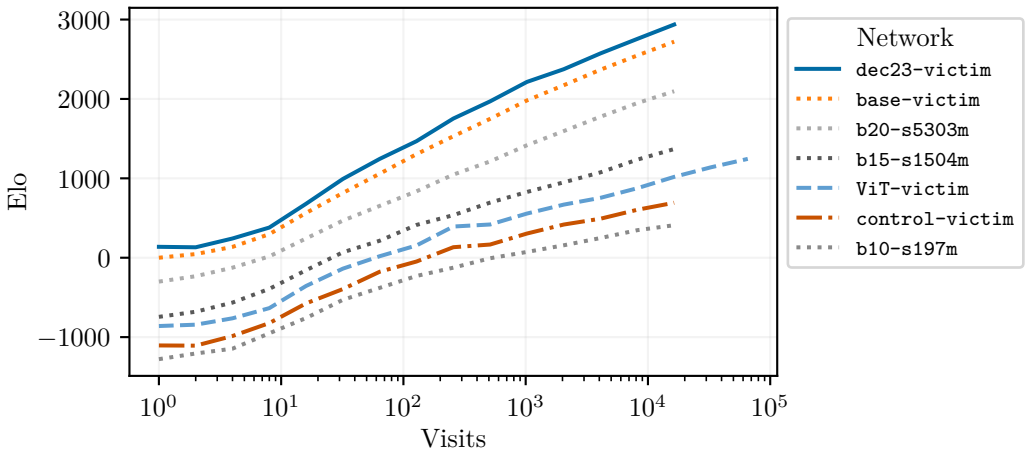


Figure H.1: Elo strength of networks (different colored lines) by visit count (x-axis). The four dotted lines are KataGo networks.

H. Network strength

H.1. Performance of defenses vs base KataGo networks

We estimate the strength of the defended victims at playing regular Go games by pitting them against regular KataGo networks. We find that the defended victims `ViT-victim`, `dec23-victim` and `v9` all possess superhuman Go capabilities.

We evaluate `dec23-victim` (positional adversarial training; Appendix E) and `ViT-victim` (vision transformer; Appendix G.1) by playing games against several KataGo networks at varying visit counts and then running a Bayesian Elo estimation algorithm. We plot the results in Fig. H.1. The KataGo networks we use are `b10-s197m`, `b15-s1504m`, `b20-s5303m`, and `base-victim`, which Wang et al. (2023a) refer to `cp79`, `Original`, `cp127`, and `Latest` respectively.

We estimate that `ViT-victim` at 32768 visits is 1139 Elo stronger than `base-victim` at 1 visit. Using Wang et al. (2023a)'s estimate that `base-victim` at 1 visit would have an Elo of 2738 on `goratings.org`, `ViT-victim` at 32768 visits has an estimated Elo of 3877. This is just shy of superhuman, as the strongest historical Elo rating on `goratings.org` is 3877 at the time of writing (as of 2024-05-02). At 65536 visits, `ViT-victim` has an estimated Elo of 3983, which is superhuman.

Likewise, `dec23-victim` at 64 visits is 1245 Elo stronger than `base-victim` at 1 visit, giving it a superhuman estimated Elo of 3983.

We estimate the strength of `v9` by playing against `base-victim` at varying visit counts. We plot the results in Fig. H.2. We estimate that `v9` has an Elo of 4997 at 4096 visits, which is 110 points weaker than `base-victim` but still clearly superhuman.

H.2. Performance of `ViT-victim` against human players

We also deployed a 64-thread, 65536 visit / move version of `ViT-victim` on the KGS Online Go server (KGS, 2022). From the previous section, we estimate this bot has a `goratings.org` Elo of 3855, around the level of a top human professional.[†††] Our results support this: our `ViT-victim` bot achieved a peak ranking of 9th

[†††]In the previous section we estimated a `goratings.org` Elo of 3983 for `ViT-victim` at 65536 visits. However, KataGo's internal benchmarks suggest that above 5000 visits, each search thread decreases performance by around 2 Elo (see `https://github.com/lightvector/KataGo/blob/v1.13.0/cpp/program/playutils.cpp#L868`). Adjusting for this gives a Elo of $3983 - 2 * 64 = 3855$. Using multiple search threads parallelizes inference, decreasing inference latency at the cost of overall strength. That is to say, for a fixed number of visits, using fewer threads generally leads to a stronger agent. All of our training and evaluation runs in the paper are done with a single search thread unless noted otherwise.

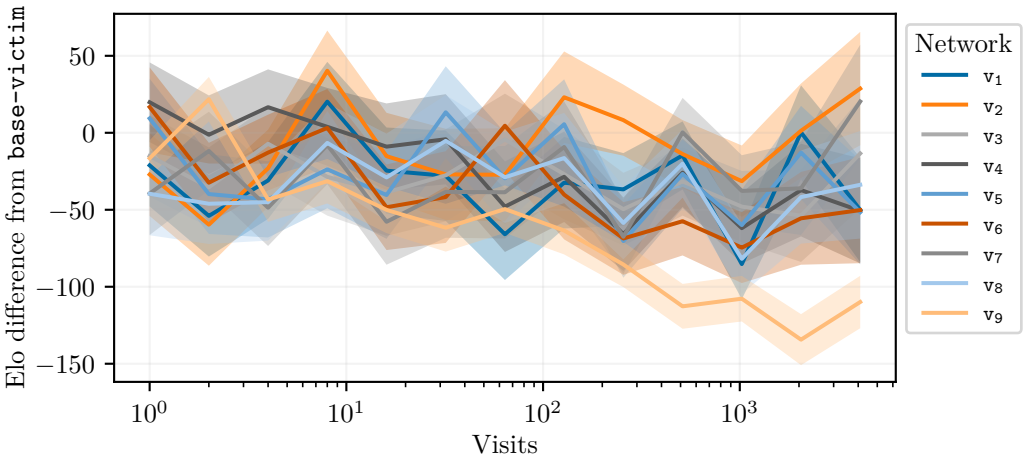


Figure H.2: Elo difference between each $\mathtt{v}_n$ to `base-victim` at visit counts up to 4096. Shaded regions are the standard deviation of the Elo estimate. Each $\mathtt{v}_n$ is slightly weaker than `base-victim`.

on KGS (KGS, 2022), ahead of many KataGo bots but behind others playing with stronger settings. Since professional players rarely play on KGS, we also commissioned three games against strong professionals: our bot won two out of three, losing one largely due to a weakness that also affected early versions of KataGo (see discussion below).

H.2.1. Public KGS games

Our bot played 1000 ranked games on the KGS website with members of the public, achieving a peak rating of 10.87 dan on the KGS website (KGS, 2022).[‡‡‡] We note that bots are common on the server; we follow the standard best practice of notifying players that they are playing a bot, and our bot was approved for ranked games by the KGS administrators. Indeed, the top ranked players on KGS are dominated by bots: our ranking of 9th puts us ahead of several KataGo bots and behind several others, though the exact configuration settings of these bots are unknown. However, the majority of ranked games played by our `ViT-victim` bot were against human players, usually with our bot giving 1 to 6 stones of handicap to the human player.

Despite our `ViT-victim` bot having a strong showing on the KGS Online Go server, it is understood within the Go community that strong professional players rarely play on KGS. Thus our results on KGS only show that a 64-thread, 65536 visit / move version of `ViT-victim` is much stronger than many strong amateur Go players.

H.2.2. Games against professional Go players

We therefore also commissioned a game against the 7 dan professional Yilun Yang and two games against the 4 dan professional Ryan Li. The players were informed that they were playing a bot and agreed to acknowledgement in the paper. They were also compensated at a rate greater than 4x the minimum wage in the relevant jurisdiction.

Yilun Yang played with 90 minutes base time for each player, and 5 periods of 30 seconds byo-yomi overtime. `ViT-victim` won, with Yang feeling he may have gotten behind early and missed some better ways to play in the middle game.

Ryan Li played with 5 minutes base time per player, and the same 5x30 byo-yomi overtime. `ViT-victim` lost the first game and won the second. In the first game, Li played the "Flying Dagger" joseki, a notoriously difficult opening corner sequence, and obtained a substantial early advantage after `ViT-victim` misplayed. Li played accurately for the rest of the game and `ViT-victim` never caught up. This joseki was a known weakness in early versions of KataGo as well; it was eventually corrected through manually adding positions from the sequence to

[‡‡‡]The KGS website has a special rating system (`www.gokgs.com/help/rmath.html`). Official ranks are discrete and only go up to 9 dan, but KGS computes an internal Elo for all players with a minimum number of ranked games. These internal Elos can go past 9 dan. See the top rated accounts at `www.gokgs.com/top100.jsp` to see some examples of this.

the training run. In our training, we did not include those positions (Appendix G.5.2), and it seems `ViT-victim` developed a similar weakness.

In the second game Li played, we requested and Li agreed to avoid that joseki, and with that constraint `ViT-victim` won.

Overall, these results indicate `ViT-victim` has some weaknesses that might lead to a lower Elo. But in general it plays at a strong professional level, in line with our original estimate. Explore the games on the accompanying project website.

I. Human replication of attacks

A Go expert author (Kellin Pelrine) was also able to replicate several of our attacks after studying the game records but without AI assistance at attack time. Full game records, along with additional commentary on the play, are available on our website and linked in the following sections.

I.1. Human replication of the continuous adversary

This attack was the most challenging to replicate, requiring multiple components chained together. In addition to carefully engineering the shapes of the attack, a key discovery was that the final step approaching the capture seems to require obfuscation. That is, the attack failed many times after seemingly achieving the salient features of the cyclic group like the distinctive double cut formation highlighted in Fig. E.1a. To succeed, it appears that the final threat against the cyclic group needs to be a natural move for a purpose other than attacking the cyclic group. This, we hypothesize, leads `dec23-victim` to be less likely to search follow-up sequences attacking its cyclic group, and consequently miss the danger that it is in.

The successful attack was performed against `dec23-victim` playing with 512 visits. Although the final obfuscation is likely to become more challenging against higher visits, we believe it should still be possible for humans to achieve, as it is possible to engineer situations where the final threat has a very large threat against something besides the cyclic group and appears very natural. For example, the critical move in the successful game is also (mis-)played by KataGo with 4096 visits. Meanwhile, the other components of the attack do not seem related to search depth and should not be harder to achieve. We plan to test human attacks against higher visits in future work.

I.2. Human replication of the gift adversary

Unlike the preceding attack, setting up the apparent shapes for this attack is relatively straightforward. It was not too challenging to produce a successful attack against 1 visit. In particular, it was quite simple to induce `dec23-victim` to make errors—the challenge was ensuring `dec23-victim`'s lead was sufficiently narrow for the errors to change the game outcome.

Scaling to higher visits, however, proved difficult. Multiple attempts at 256 and 512 visits failed. We hypothesize that this is because the victim must assign enough value to the sending-two "gift" move to play it, but at the same time not keep searching locally and see disaster coming after the adversary's next move. These requirements are conflicting: if there are valuable areas to play elsewhere then the victim is likely to play those instead of sending-two, but if there are none, then there are none for the adversary either, so the victim is more likely to expect the adversary to continue locally and accept the gift – and then to see the danger.

This need for some but not too much local search so that the victim plays the local "gift" move is in stark contrast with all versions of the cyclic attack, where the attack is more likely to succeed the less search is allocated by the victim to the locality of the vulnerability. Furthermore, at least in the versions of the attack observed so far, the number of moves that the victim needs to look ahead locally, between its deciding move and realized loss (adversary group living), is fixed and small. This again contrasts with the cyclic attack, where the deciding move can take place a virtually arbitrary amount of moves ahead of realized loss (cyclic group captured or something else lost while saving the cyclic group).

This requirement means the attack needs to balance search probabilities over the entire board to a greater and greater degree at higher visits. By contrast, in the cyclic attack it suffices to control the local situation to make the attack more hidden, requiring a greater victim search depth needed to notice the attack. This also fits with our empirical observations: humans can perform the attack at one visit but seemingly not at 256+, while `gift-adversary` can reach 512 visits and somewhat beyond but falls off vary sharply after 1024 visits (Fig. 3.1). `gift-adversary` is likely able to balance search probabilities of the victim with much higher precision than humans can, but it becomes prohibitively difficult at high enough visits.

I.3. Human cyclic attack on `ViT-victim`

Pelrine was also able to use a cyclic attack to beat `ViT-victim`. This attack was the easiest to execute of those discussed in this section. It was performed against a 64-thread, 65536 visit / move version of `ViT-victim`, the same used in the strength evaluation in Appendix H.2. The shape used for the inside group paralleled some of the wins by `base-adversary` against this victim. The attack emphasized ensuring lots of liberties for the groups surrounding the cyclic one so that `ViT-victim` would have to see the danger early to have a way out.

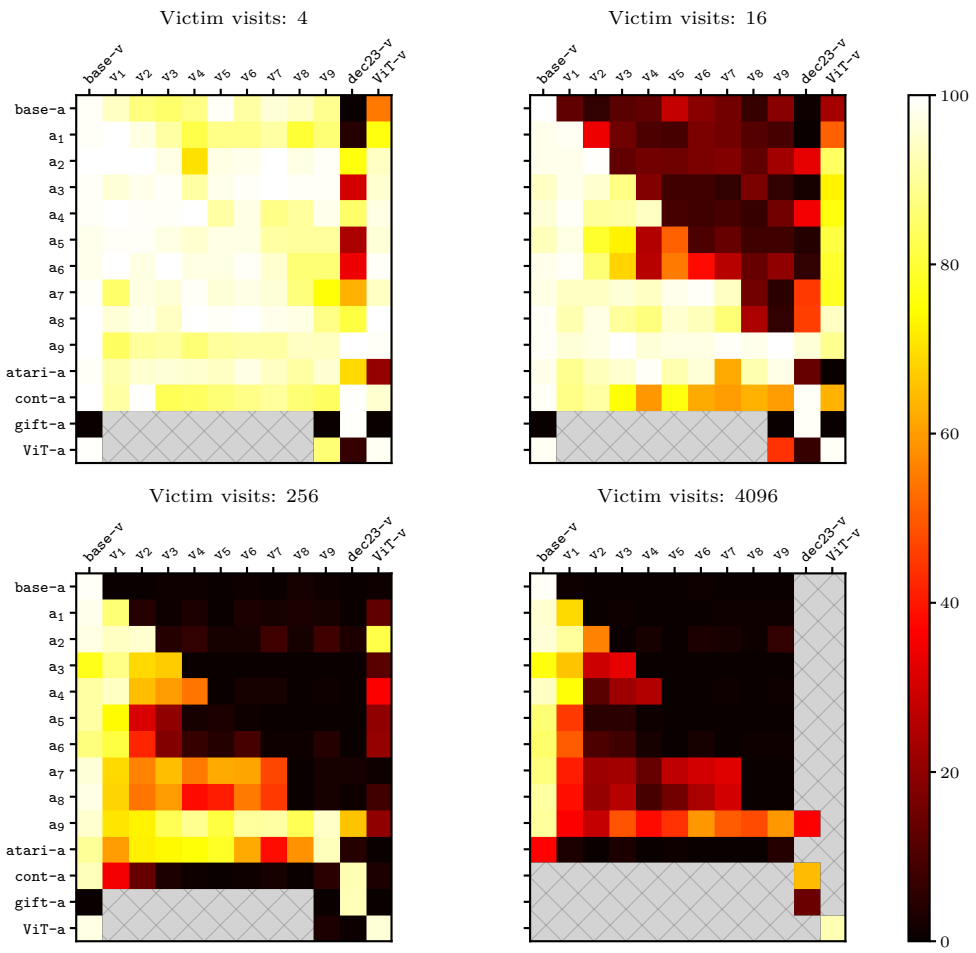


Figure J.1: We extend Fig. 3.2's plot of adversaries' win rates against various victims to include more adversaries on the y-axis and more victims on the x-axis.

J. Transfer

Figure J.1 shows the result of playing adversaries against a variety of victims. The ability of victims to defeat adversaries they were not trained against provides evidence of their robustness.

Victims: We find all victims remain vulnerable at extremely low amounts of search (4 victim visits), although `dec23-victim` does better than others. `base-victim` through $\texttt{v}_4$ progressively improve at defending against `continuous-adversary`, after which their performance plateaus.

Adversaries: $\texttt{a}_9$, trained against $\texttt{v}_9$, transfers surprisingly well to defeat `dec23-victim`, winning 66% of games at 256 visits and 36% at 4096 visits (Fig. J.2). `atari-adversary`, trained against $\texttt{v}_9$, wins 4% of games against `dec23-victim` at 256 victim visits. By contrast, `continuous-adversary`, trained against `dec23-victim`, wins 5% of games against $\texttt{v}_9$. `gift-adversary` does not transfer at all to other victims, achieving no wins even at 4 visits against `base-victim` and `ViT-victim`.

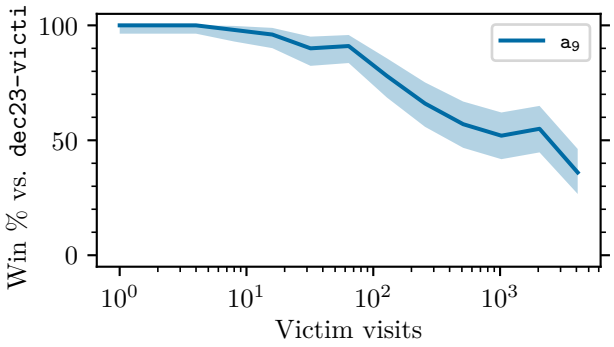


Figure J.2: Win rate (y-axis) of `a9` versus `dec23-victim` at varying victim visits (x-axis), demonstrating considerable transfer performance.

K. Compute resources

K.1. Compute infrastructure

We ran experiments using cloud computing infrastructure orchestrated with Kubernetes configured with the Kueue batch scheduler. We used A6000 GPUs for nearly all our training runs. The main exception is that $\texttt{v}_1$, $\texttt{v}_2$, $\texttt{v}_3$, and $\texttt{v}_4$ used A100 80GB GPUs as we were trying a different compute platform. We also used some H100 GPUs during the `gift-adversary` and $\texttt{a}_9$ runs, but they were mainly run on A6000 GPUs.

K.2. Compute for our training runs

We convert our compute numbers to V100 GPU-days so that our numbers can be straightforwardly compared to the V100-based compute estimates of Wang et al. (2023a). According to Wang et al.'s conversion estimates, one A100 80GB GPU-day is 1.873 A6000 GPU-days and one A6000 GPU-day is 1.704 V100 GPU-days. We estimate that one H100 GPU-day generated as much training data as 0.369 A6000 GPU-days. Note we did not tune our H100 setup as we made minimal use of these GPUs.

Most of our compute estimates are measured by parsing our training logs. However, when training $\texttt{a}_1$, ViT, and `ViT-adversary`, we made sub-optimal configuration choices that slowed down our training runs. For these runs, we provide idealized compute estimates by benchmarking the slow-down caused by the poor configuration and scaling our compute estimates downwards accordingly.

Our error in $\texttt{a}_1$ training was using too few game threads, a parameter controlling how many victim-play games are played at once. We were using 16–32 game threads rather than the 128–256 game threads that we used in later training runs, which gave higher training throughput. $\texttt{a}_1$ used 703 V100 GPU-days, and we estimate that with higher game threads it would have cost 238 V100 GPU-days instead.

Our error in training our ViT networks and `ViT-adversary` was using single-precision floating point rather than half-precision floating point for ViT inference. Inference with half-precision floating point is significantly faster. Our actual compute cost for training ViT with single-precision floating point was 128 V100 GPU-days for the 4-block ViT, 661 V100 GPU-days for the 8-block ViT, and 457 V100 GPU-days for the 16-block ViT, totalling 1247 V100 GPU-days. We estimate that with half-precision floating point, the cost would have been 537 V100 GPU-days instead. For `ViT-adversary`, we switched to half-precision floating point near the end of the run and spent 711.0 V100 GPU-days. We estimate that had we used half-precision floating point for the entire training run, it would have been 409 V100 GPU-days instead.

K.3. Compute for KataGo models

`base-victim`, `may23-victim`, and `dec23-victim` all come from KataGo's ongoing distributed training run, which was initialized from KataGo's "third major run." Wu (2021b) reports training compute estimates for the third major run, from which we can extrapolate the training cost of models from the distributed training run. (Our compute estimate calculations are similar to those of Wang et al. (2023a), except in our estimates we do not anchor on the initial 38.5 days of the third major run that generated data with smaller models, and we account for the greater search used in the distributed training run.)

In the last 118.5 out of 157 days in the third major run, the run switched from using `b20c256` nets to using `b40c256` and `b30c320` nets for self-play data generation. The final `b20c256` net used for self-play was trained on 468,617,949 data rows whereas the third major run generated 1,229,425,124 rows in total, so over the course of those 118.5 days, the run generated $1{,}229{,}425{,}124 - 468{,}617{,}949 = 760{,}807{,}175$ rows. This segment of the run used 46 V100 GPUs, costing $118.5 \times 46 = 5451$ V100 GPU-days. The total cost of the the third run across all 157 days is 6,730 V100 GPU-days (Wang et al., 2023a).

The distributed run generates data with `b40c256`, `b60c320`, and `b18c384nbt` nets, all of which have similar or higher inference cost to the `b40c256` and `b30c320` used in the third major run.[§§§] Therefore, we estimate the average inference from the distributed run is at least as expensive as the average inference from the last 118.5

[§§§] `b60c320` is a strictly larger in width and depth than `b40c256` and therefore has a higher inference cost. `https://github.com/lightvector/KataGo/blob/v1.14.1/python/modelconfigs.py#L1384` states that `b40c256`, `b30c320`, and `b18c384nbt` have similar inference costs.

days of the third major run.

Moreover, the distributed training run uses more inferences to generate each data row. The third major run used 1000 full-search visits or 200 cheap-search visits per move, where full searches are used to generate high-quality policy data and cheap searches are used to play games quickly (Wu, 2020b). The distributed training run started with 1500 full-search visits and 250 cheap-search visits (Wu, 2020a). Assuming inference count scales proportionally with search and that data row compute cost scales proportionally with inference count, we crudely estimate each training row generated with these search parameters costs 1.25× as much as each training row from the third major run. The distributed run switched to 2000 full-search visits and 350 cheap-search visits in March 2023 (Wu, 2023c), after about 3.211 billion data rows (including the 1.2 billion from the third major run) were generated. We estimate each row generated with these parameters costs 1.75× as much as each third-major-run row.

Putting this all together, our training compute estimate in V100 GPU-days for a model from KataGo's distributed training run that has trained on $D \geq 1{,}229{,}425{,}124$ rows is

$$6730 + \frac{(\min\{D, 3211000000\} - 1229425124) \cdot 1.25 + \max\{D - 3211000000, 0\} \cdot 1.75}{760807175} \cdot 5451.$$

Since `base-victim` trained on 2,898,845,681 data rows, its estimated cost is 21681 V100 GPU-days. `may23-victim` trained on 3,323,518,127 rows, giving a cost of 25888 V100 GPU-days, and `dec23-victim` trained on 3,929,217,702 rows, giving a cost of 33482 V100 GPU-days.

For adversarial training, the last KataGo network before adversarial training began was trained with 3,057,177,418 data rows (Wu, 2022b). Based solely on the number of data rows, `dec23-victim` has had $(3929217702 - 3057177418)/(3323518127 - 3057177418) = 3.3$ times as much adversarial training as `may23-victim`.

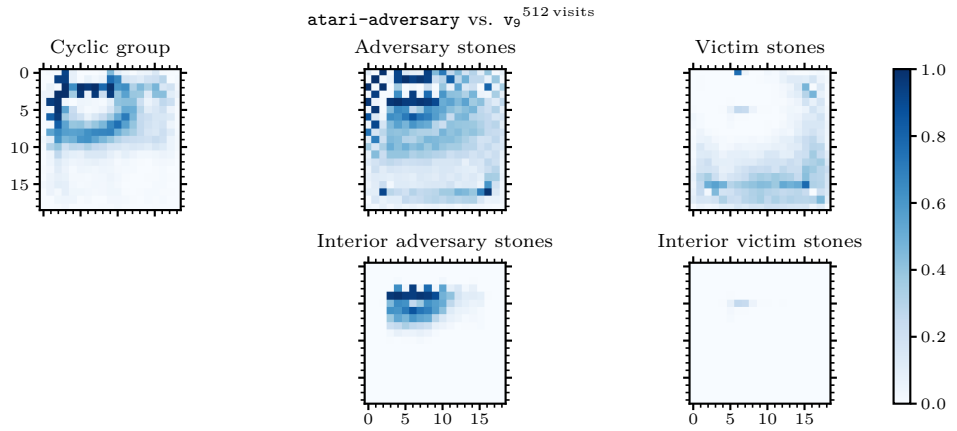


Figure L.1: Heat map showing the cyclic attack made by `atari-adversary` against v_9.

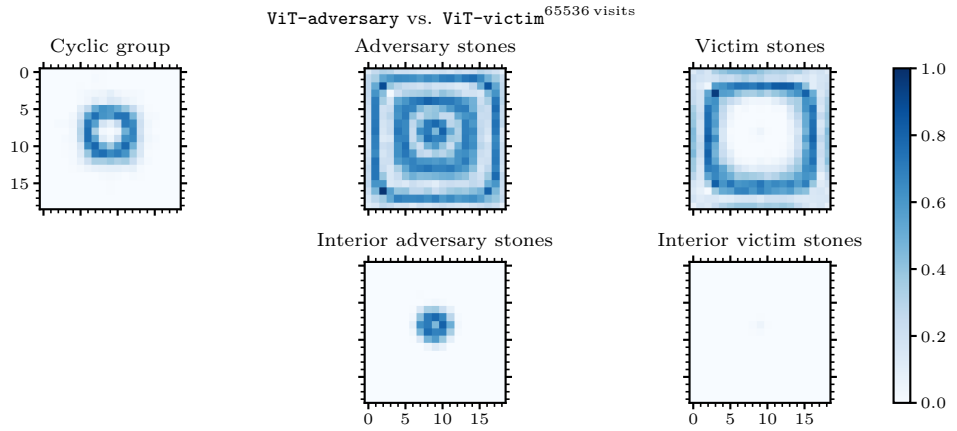


Figure L.2: Heat map showing the cyclic attack made by `ViT-adversary` against `ViT-victim`.

L. Heat maps of cyclic attacks

In this section, we present heat maps illustrating the cyclic shapes constructed by each of our cyclic adversaries. We also plot differences between heat maps to show changes in the cyclic group constructed by different adversaries.

To construct the heat maps for an adversary, we took games where the adversary beats the victim it was trained against. We then inspect the board state during the move at which a large cyclic group of victim stones is captured. To remove board symmetries, we rotate the game board so that the center of the cyclic group is in the top-left quadrant of the board, and flip across the major diagonal of the board to keep the center of the group above the major diagonal. We then plot the frequency of each board square being in the captured cyclic group. We also plot the adversary's stones, the victim's other stones, and the adversary and victims' stones falling in the interior of the cyclic group at the time of capture.

Figure L.1 shows heat maps for `atari-adversary` against v_9, with the dark squares in the cyclic group being the bamboo joints discussed in Section 3.2.2. We also see a checkerboard pattern of adversary stones near the cyclic group. These are likely isolated pieces, mentioned in the same discussion, that could be captured if the victim saw the danger its cyclic group was in.

Figure L.2 shows heat maps for `ViT-adversary` against `ViT-victim`, which moves the cycle into the center and forms another boundary of stones around it.

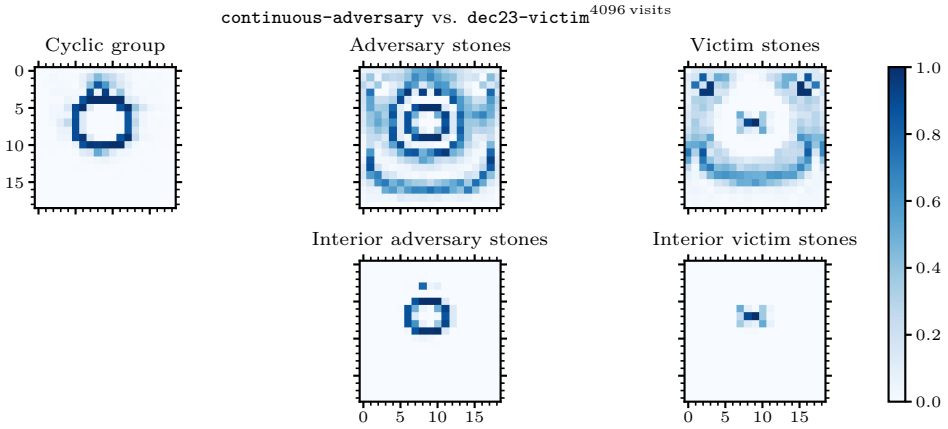


Figure L.3: Heat map showing the cyclic attack made by `continuous-adversary` against `dec23-victim` with 4096 victim visits of search.

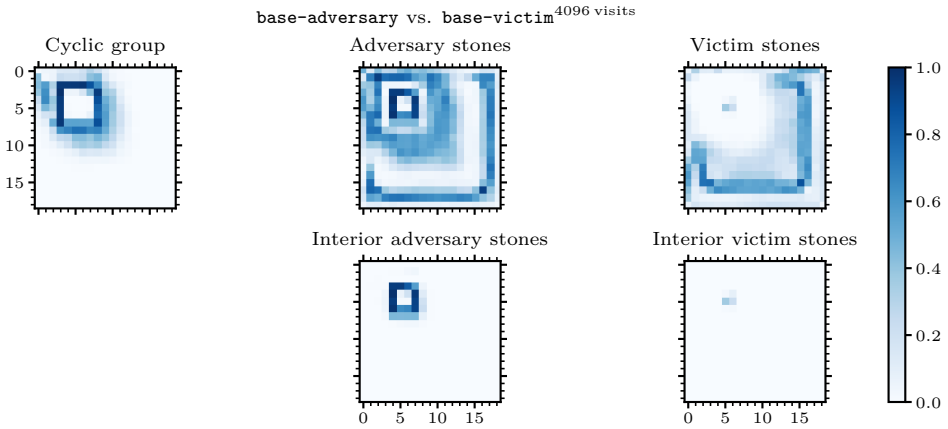


Figure L.4: Heat map showing the cyclic attack made by `base-adversary` against `base-victim` with 4096 victim visits of search.

`continuous-adversary`'s attack against `dec23-victim` (Fig. L.3) shows less variation in the cyclic group than the attack made by `base-adversary` (Fig. L.4): the cyclic stone heat map (Fig. L.3) is deeply colored throughout with few lightly colored squares. We also see a larger and consistent shape of interior adversary stones for `continuous-adversary`, along with a pattern in interior victim stones that isn't present for the `base-adversary`.

For `base-adversary`, using more victim visits does not substantially affect the shape of the cyclic attack. Fig. L.5 plots the difference between the heat map for 4096 (Fig. L.4) and 16 (Fig. L.6) victim visits, finding minimal differences.

Figures L.8 to L.24 show heat maps for each adversary $\texttt{a}_1$ through $\texttt{a}_9$ trained in iterated adversarial training against their corresponding victims at 16 victim visits:

- $\texttt{a}_1$ (Figs. L.7 and L.8) has a less consistent structure to the stones outside the cyclic group than `base-adversary`, which tends to form a boundary of stones near the edge of the board outside the cycle.
- $\texttt{a}_2$ (Figs. L.9 and L.10) forms a larger cycle than $\texttt{a}_1$.
- $\texttt{a}_3$ (Figs. L.11 and L.12) moves the cycle towards the center on one axis, and the cycle shrinks again but with less consistent shapes.

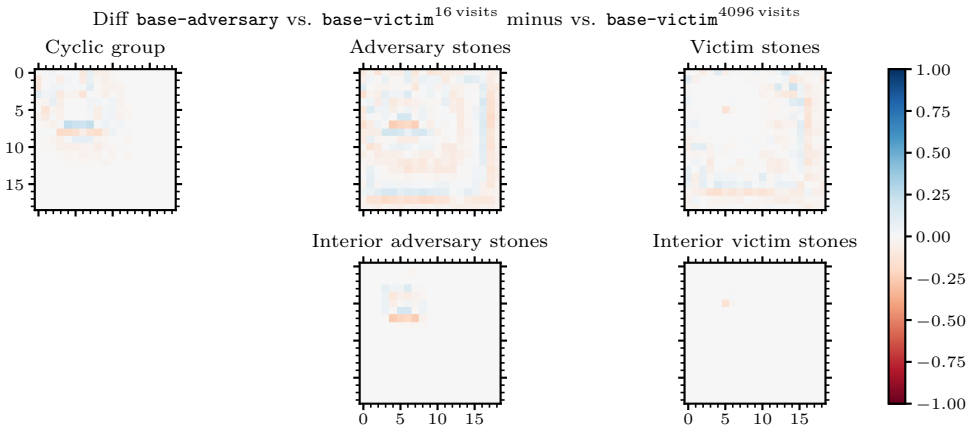


Figure L.5: Difference between the heat maps of `base-adversary` against `base-victim` with 16 (Fig. L.6) and 4096 (Fig. L.4) victim visits of search. `base-adversary`'s attack does not change much when victim visits are increased.

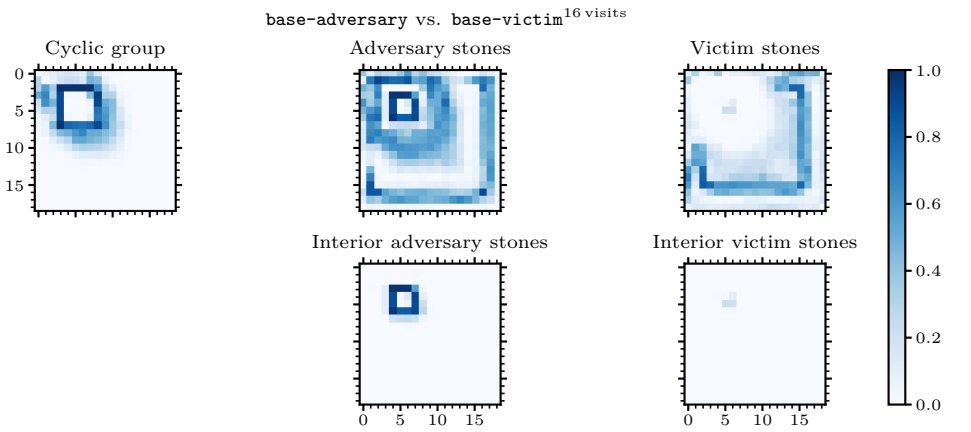


Figure L.6: Heat map showing the cyclic attack made by `base-adversary` against `base-victim` with 16 victim visits of search.

- $\mathtt{a}_4$ (Figs. L.13 and L.14) moves the cycle towards the center along the other axis.
- $\mathtt{a}_5$ (Figs. L.15 and L.16) makes the cycle larger.
- $\mathtt{a}_6$ (Figs. L.17 and L.18) does not show much qualitative difference in the heat maps.
- $\mathtt{a}_7$ (Figs. L.19 and L.20) tends to place stones on board locations of a particular parity near the boundaries of the board, leading to a checkerboard pattern in the heat map.
- $\mathtt{a}_8$ (Figs. L.21 and L.22) does not show much change.
- $\mathtt{a}_9$ (Figs. L.23 and L.24) shrinks the cycle slightly.

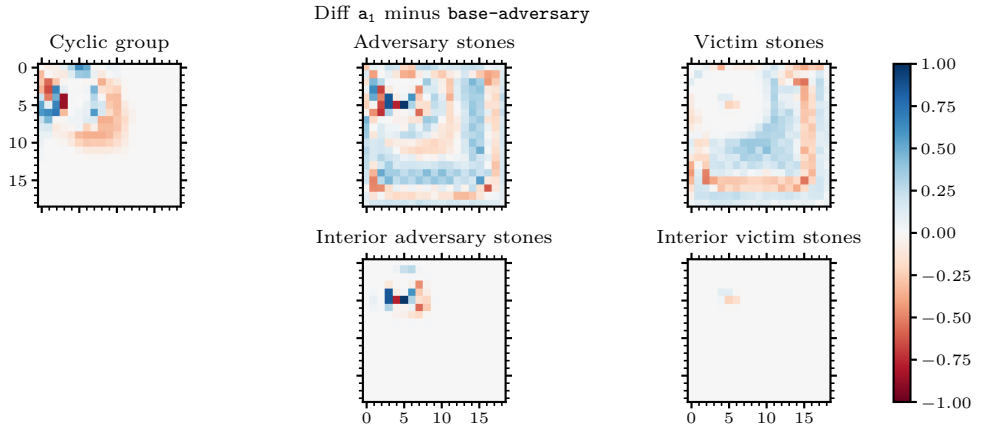


Figure L.7: Difference between the heat maps of $\mathtt{a}_1$ (Fig. L.8) and `base-adversary` (Fig. L.6).

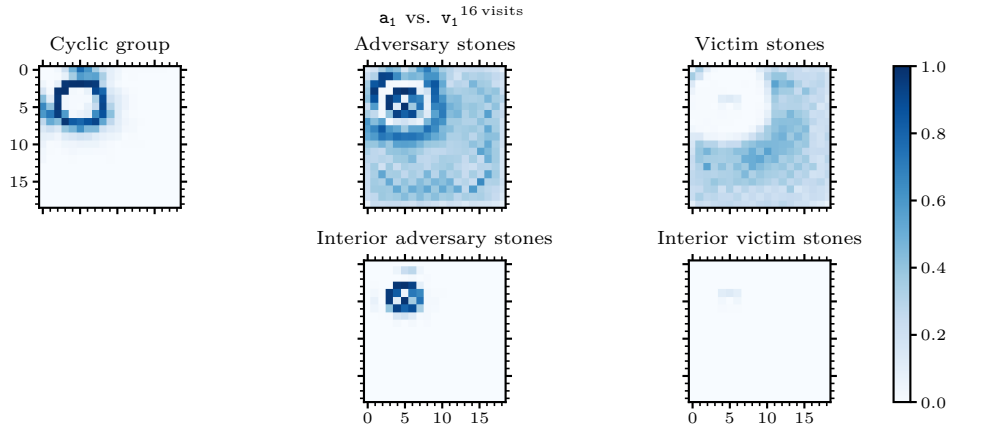


Figure L.8: Heat map showing the cyclic attack made by $\mathtt{a}_1$ against $\mathtt{v}_1$.

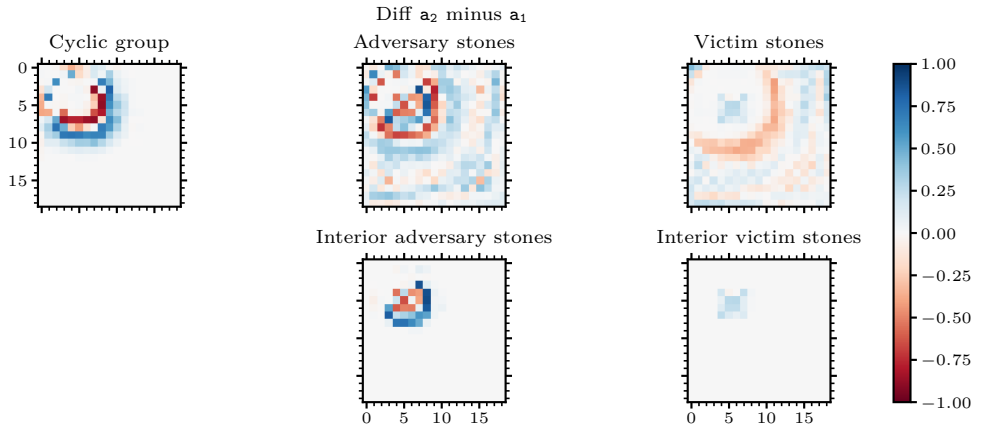


Figure L.9: Difference between the heat maps of $\mathtt{a}_2$ (Fig. L.10) and $\mathtt{a}_1$ (Fig. L.8).

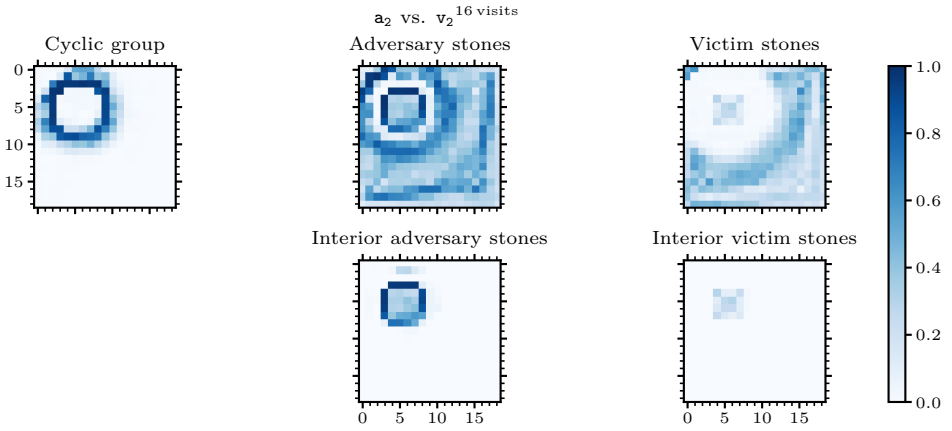


Figure L.10: Heat map showing the cyclic attack made by $\mathtt{a}_2$ against $\mathtt{v}_2$.

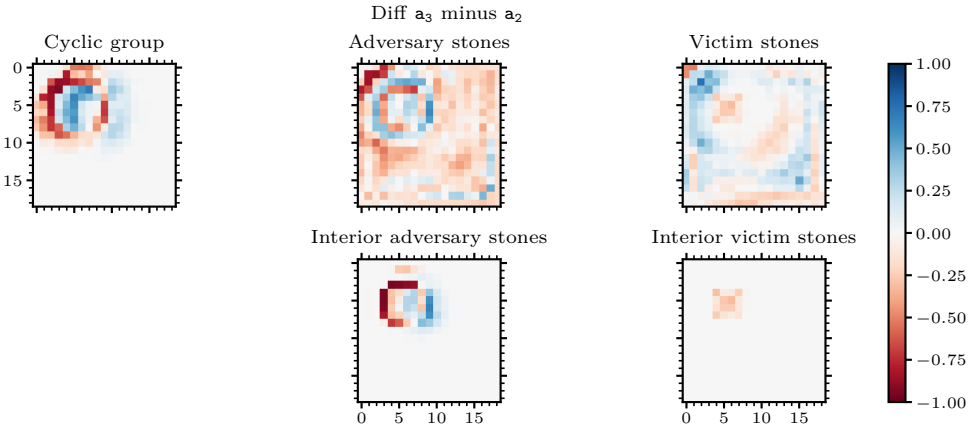


Figure L.11: Difference between the heat maps of $\mathtt{a}_3$ (Fig. L.12) and $\mathtt{a}_2$ (Fig. L.10).

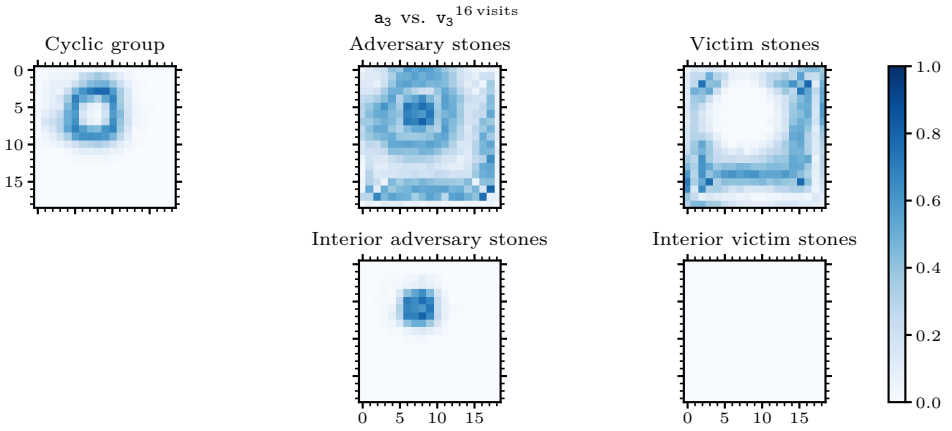


Figure L.12: Heat map showing the cyclic attack made by $\mathtt{a}_3$ against $\mathtt{v}_3$.

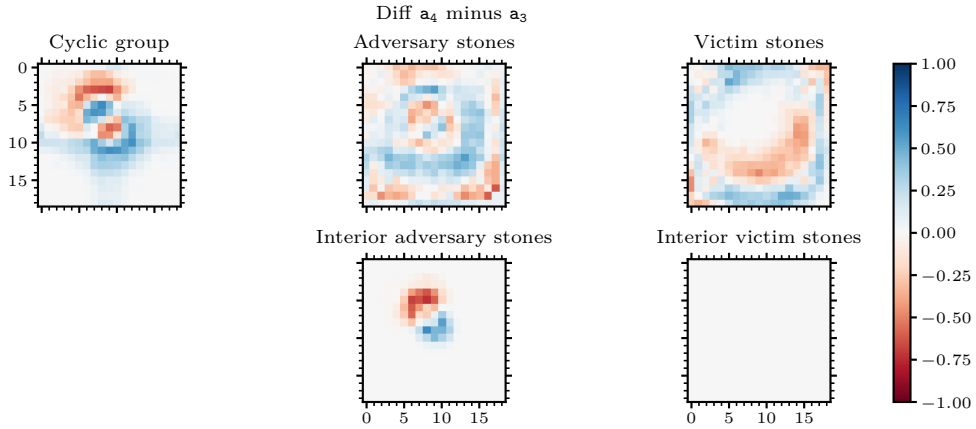


Figure L.13: Difference between the heat maps of $\mathtt{a}_4$ (Fig. L.14) and $\mathtt{a}_3$ (Fig. L.12).

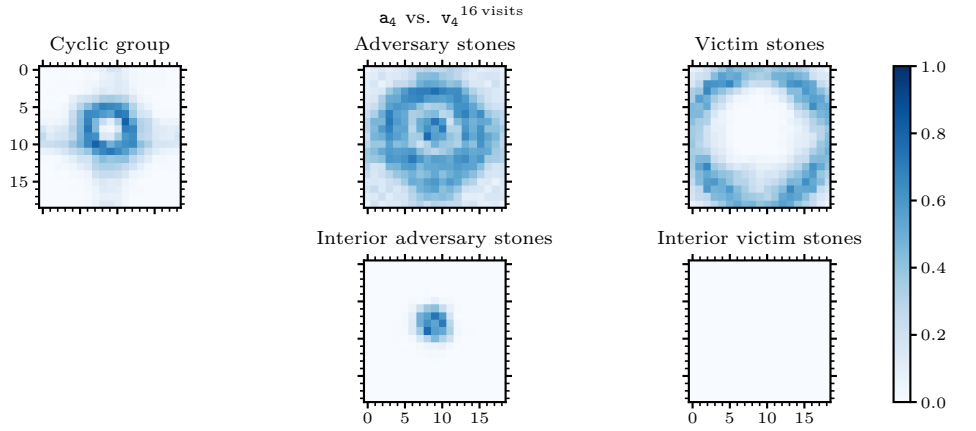


Figure L.14: Heat map showing the cyclic attack made by $\mathtt{a}_4$ against $\mathtt{v}_4$.

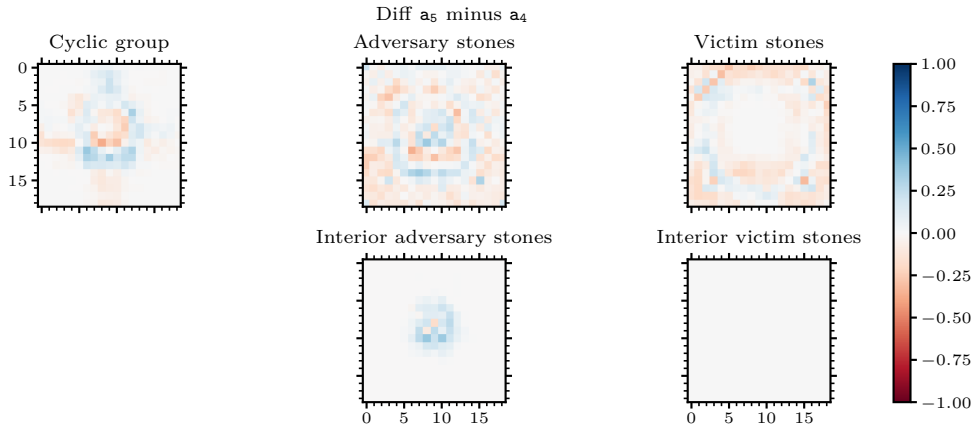


Figure L.15: Difference between the heat maps of $\mathtt{a}_5$ (Fig. L.16) and $\mathtt{a}_4$ (Fig. L.14).

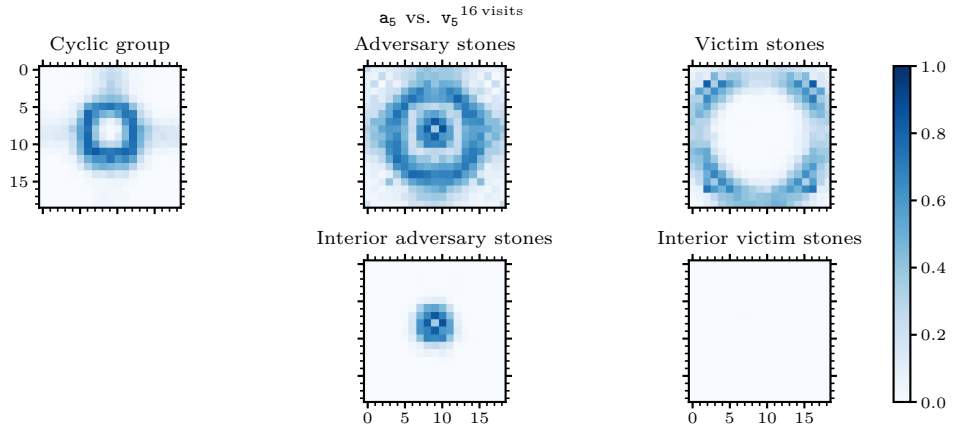


Figure L.16: Heat map showing the cyclic attack made by $\mathtt{a}_5$ against $\mathtt{v}_5$.

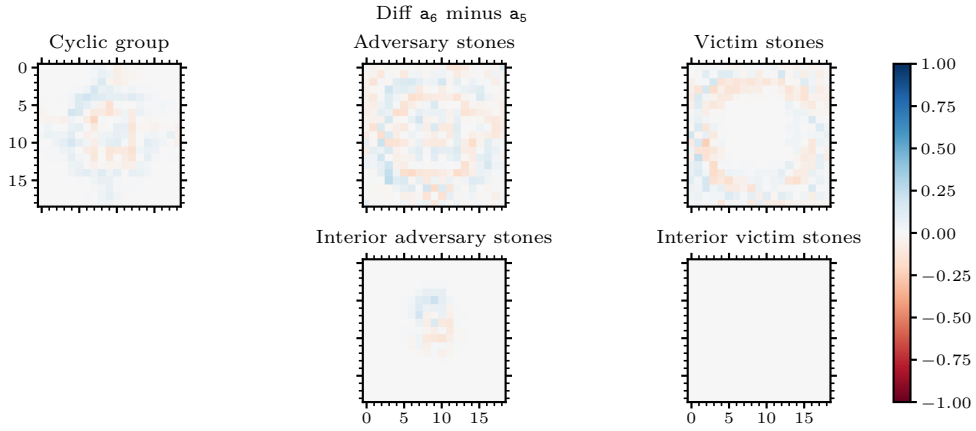


Figure L.17: Difference between the heat maps of $\mathtt{a}_6$ (Fig. L.18) and $\mathtt{a}_5$ (Fig. L.16).

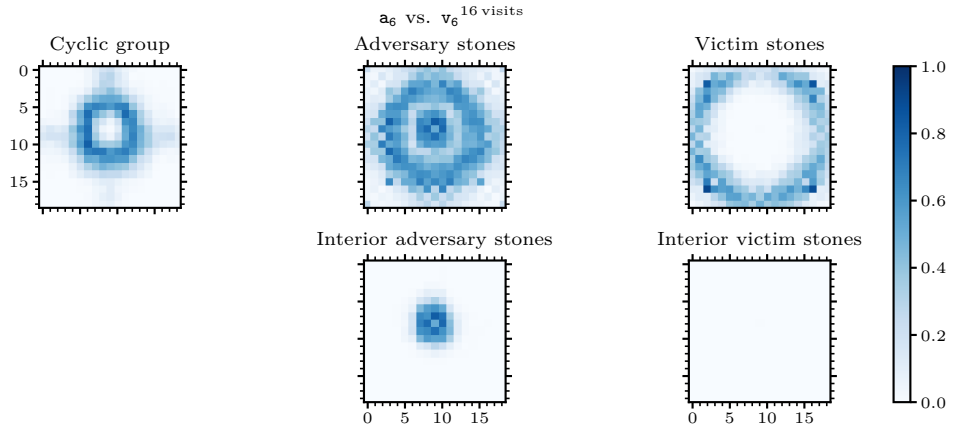


Figure L.18: Heat map showing the cyclic attack made by $\mathtt{a}_6$ against $\mathtt{v}_6$.

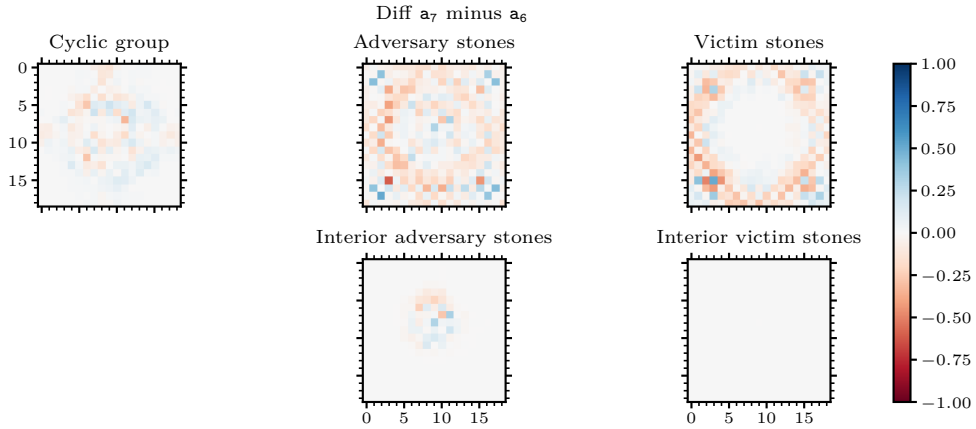


Figure L.19: Difference between the heat maps of $\mathtt{a}_7$ (Fig. L.20) and $\mathtt{a}_6$ (Fig. L.18).

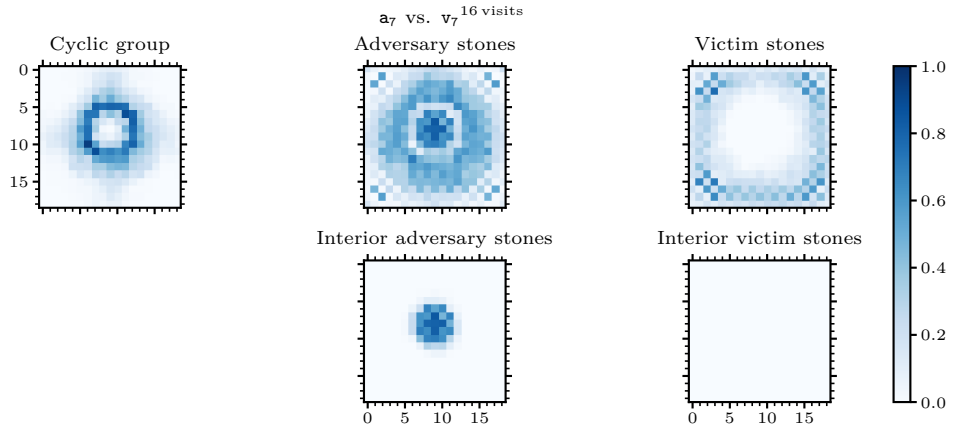


Figure L.20: Heat map showing the cyclic attack made by $\mathtt{a}_7$ against $\mathtt{v}_7$.

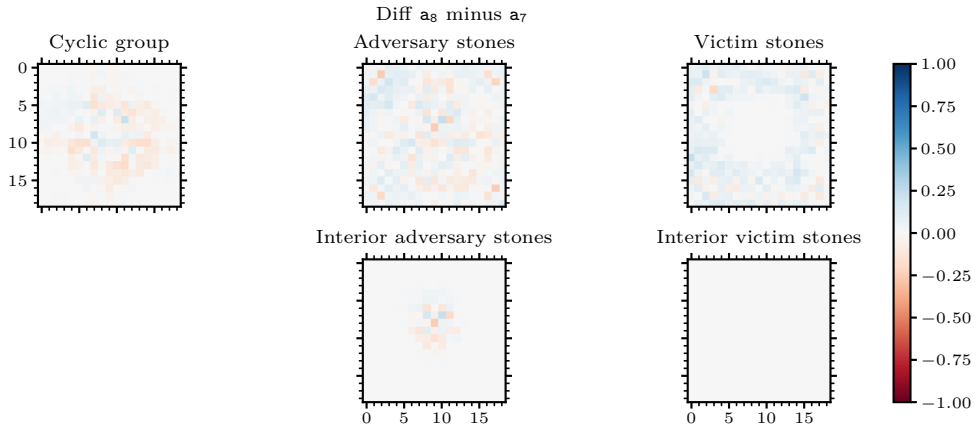


Figure L.21: Difference between the heat maps of $\mathtt{a}_8$ (Fig. L.22) and $\mathtt{a}_7$ (Fig. L.20).

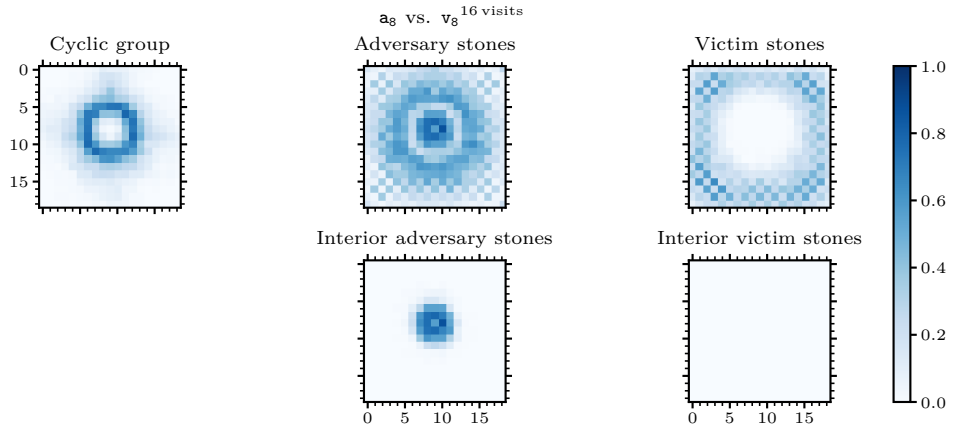


Figure L.22: Heat map showing the cyclic attack made by $\mathtt{a}_8$ against $\mathtt{v}_8$.

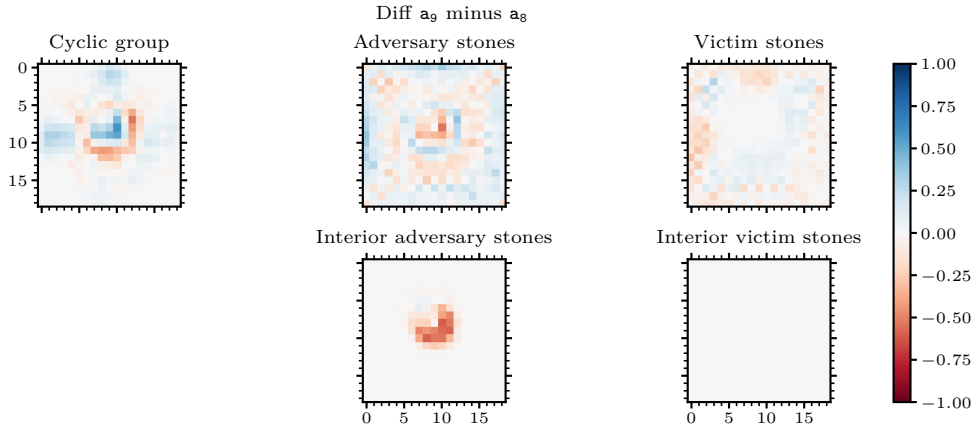


Figure L.23: Difference between the heat maps of $\mathtt{a}_9$ (Fig. L.24) and $\mathtt{a}_8$ (Fig. L.22).

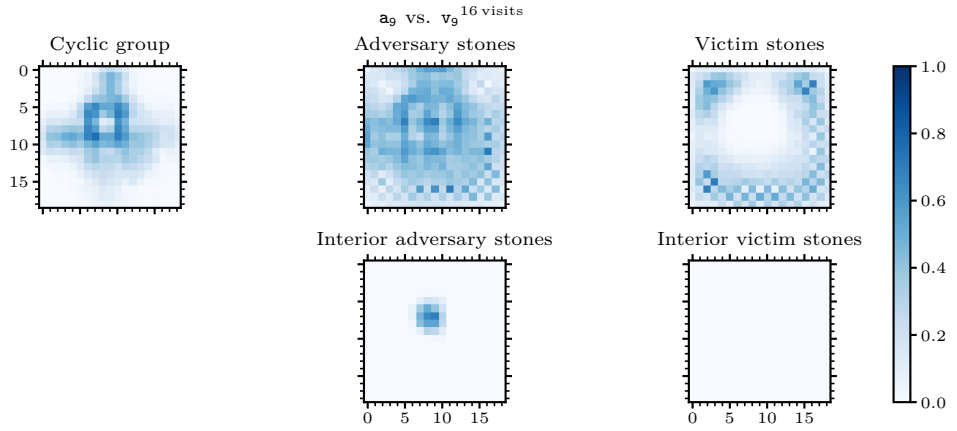


Figure L.24: Heat map showing the cyclic attack made by $\mathtt{a}_9$ against $\mathtt{v}_9$.

M. Extra experimental plots

This section collects additional, visually large plots referenced in previous sections.

M.1. Individual iterated adversarial training plots

Whereas Figs. F.1 and F.2 concatenate all defense iterations into one plot and all attack iterations into another plot, Figs. M.1 and M.2 give training progress plots for each iteration separately.

M.2. Training steps plots

In Figs. M.3 to M.15 we display versions of previous plots but use victim-play or self-play training steps on the x-axis to measure training time instead of GPU-days. We tended to use GPU-days throughout this paper since it is a unit that is more understandable for readers, but as GPU-days are machine-dependent, training steps may be more useful for other researchers who want to compare our runs to other KataGo-like training runs.

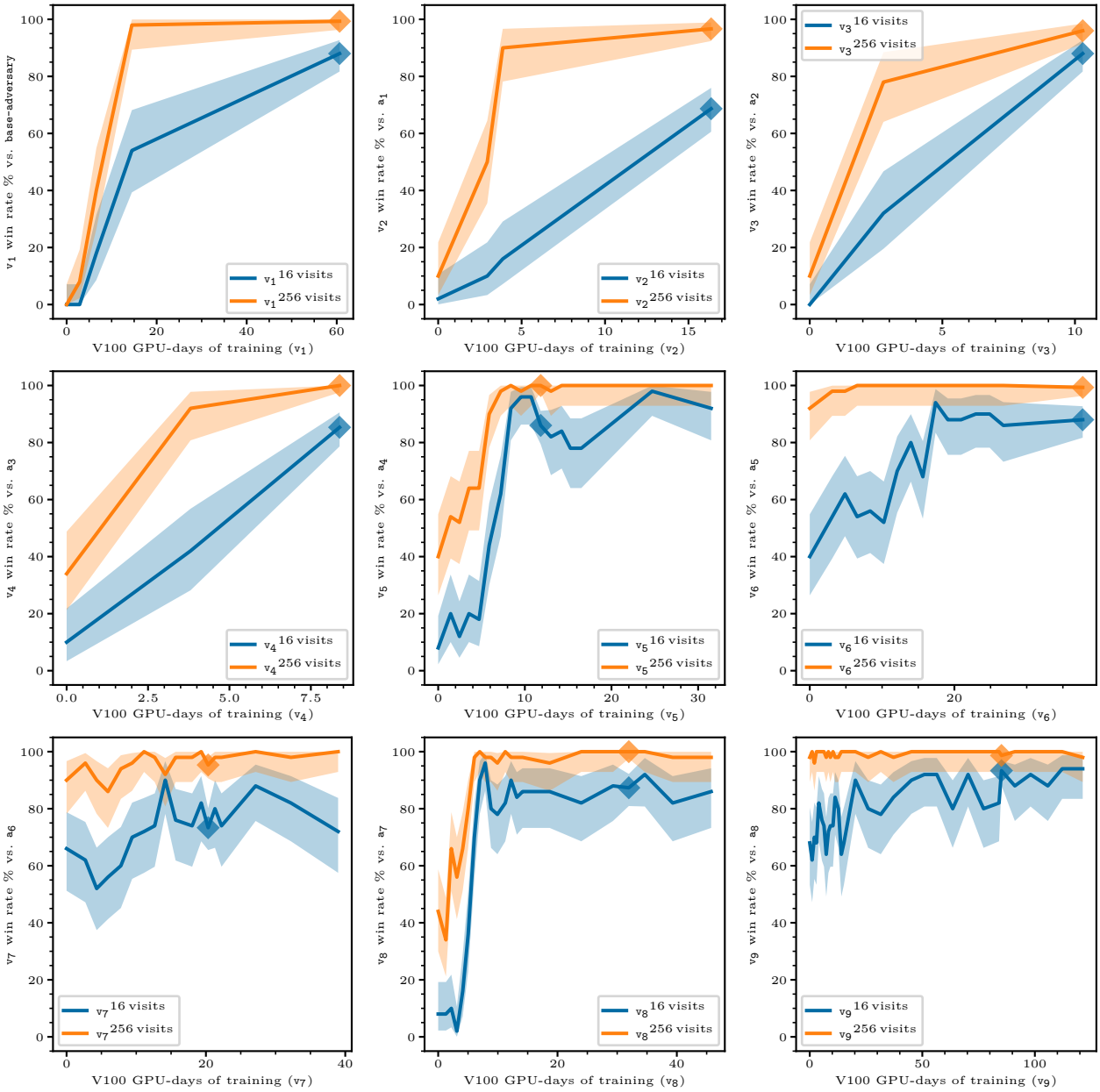


Figure M.1: Win rate (y-axis) of each $\texttt{v}_N$ (♦) against $\texttt{a}_{N-1}$ throughout $\texttt{v}_N$'s training (x-axis). The curves for $\texttt{v}_1$ to $\texttt{v}_4$ only have a few data points along the x-axis as intermediate checkpoints were lost.

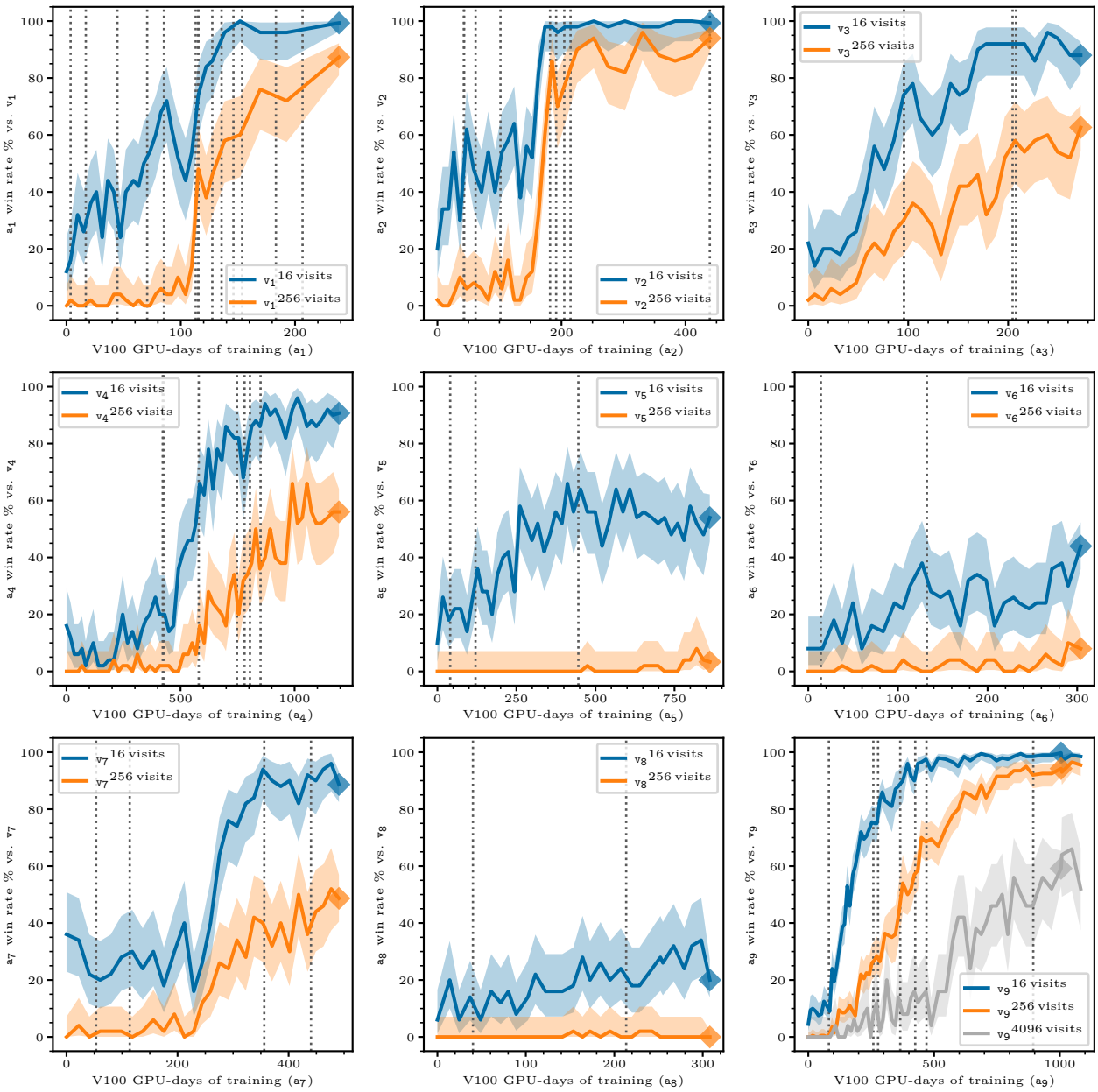


Figure M.2: Win rate (y-axis) of each $\mathtt{a}_N$ against $\mathtt{v}_N$ throughout $\mathtt{a}_N$'s training (x-axis). Dotted lines represent advancing to the next victim in the curriculum.

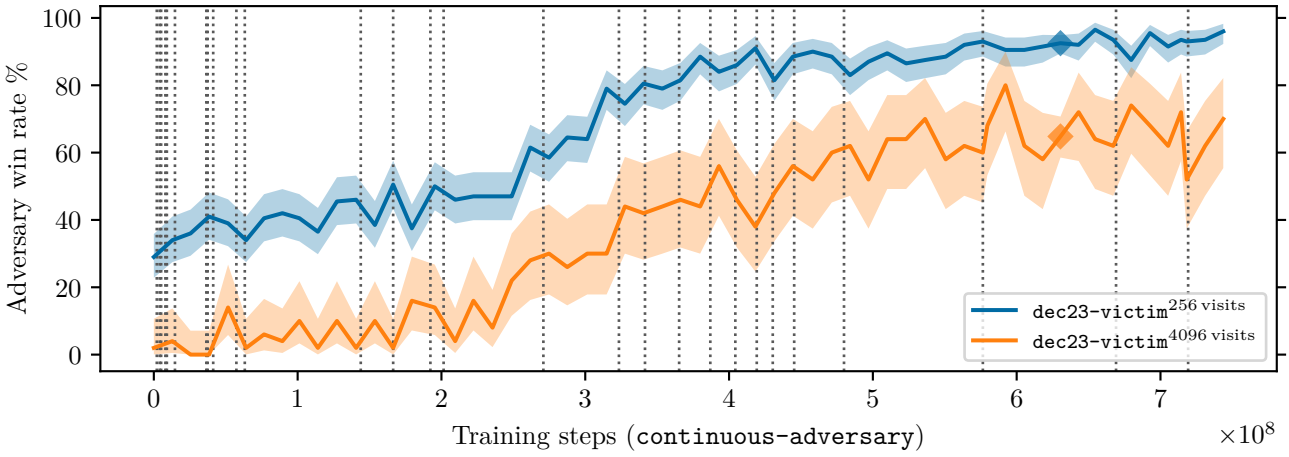


Figure M.3: This plot is the same as Fig. E.2 but with training steps on the x-axis instead of GPU-days.

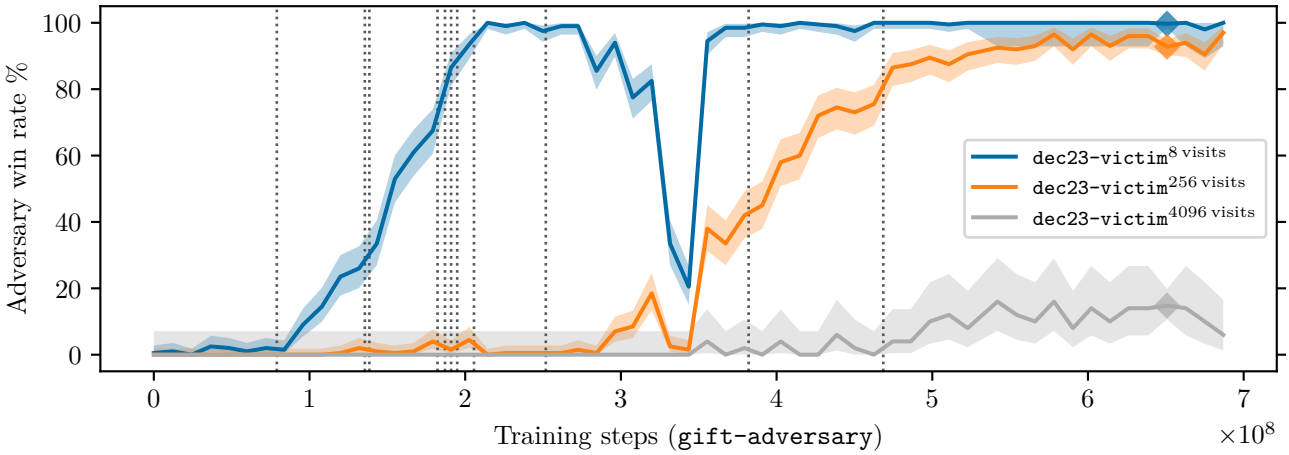


Figure M.4: This plot is the same as Fig. E.4 but with training steps on the x-axis instead of GPU-days.

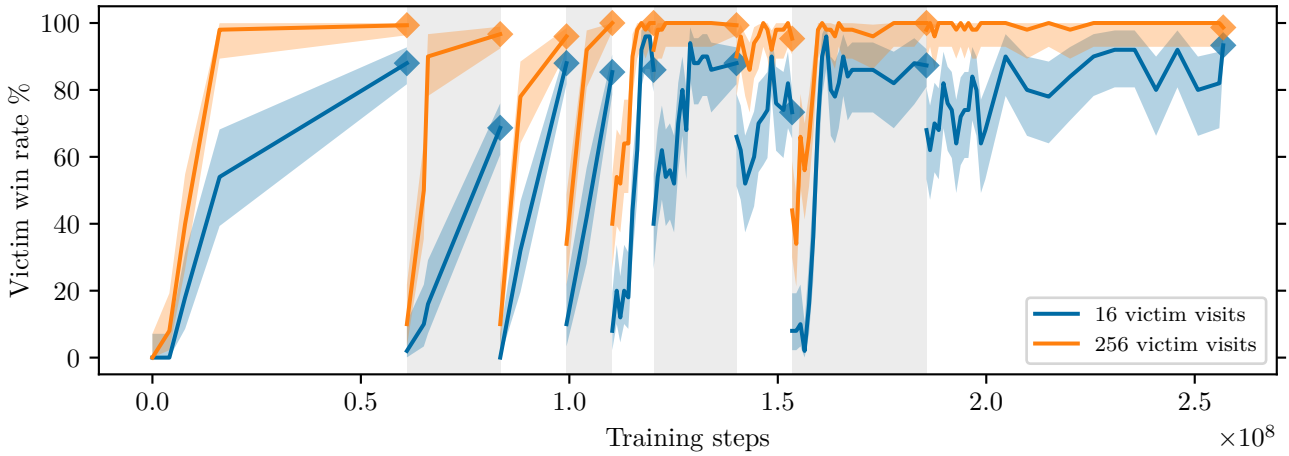


Figure M.5: This plot is the same as Fig. F.1 but with training steps on the x-axis instead of GPU-days.

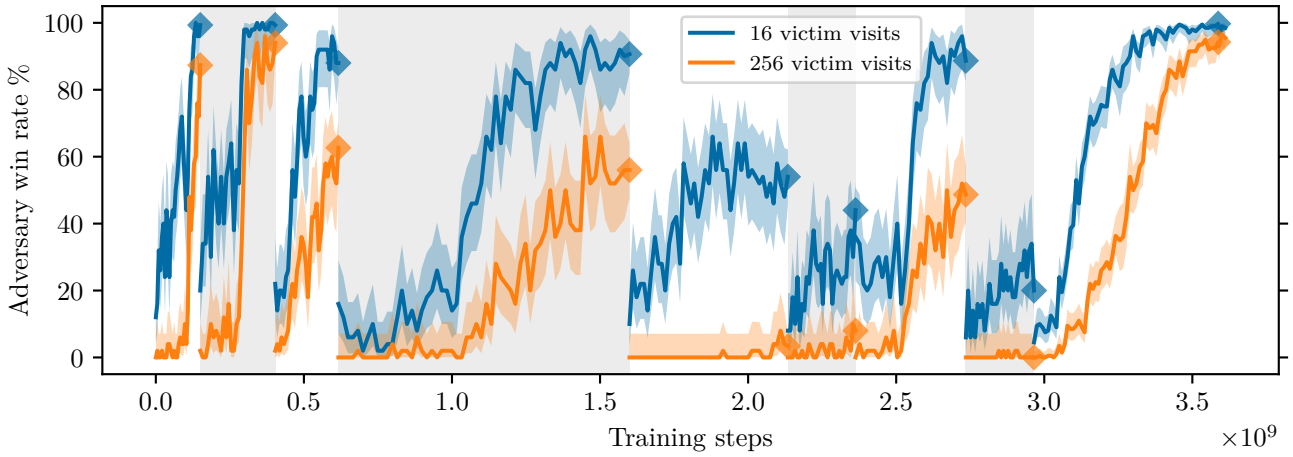


Figure M.6: This plot is the same as Fig. F.2 but with training steps on the x-axis instead of GPU-days.

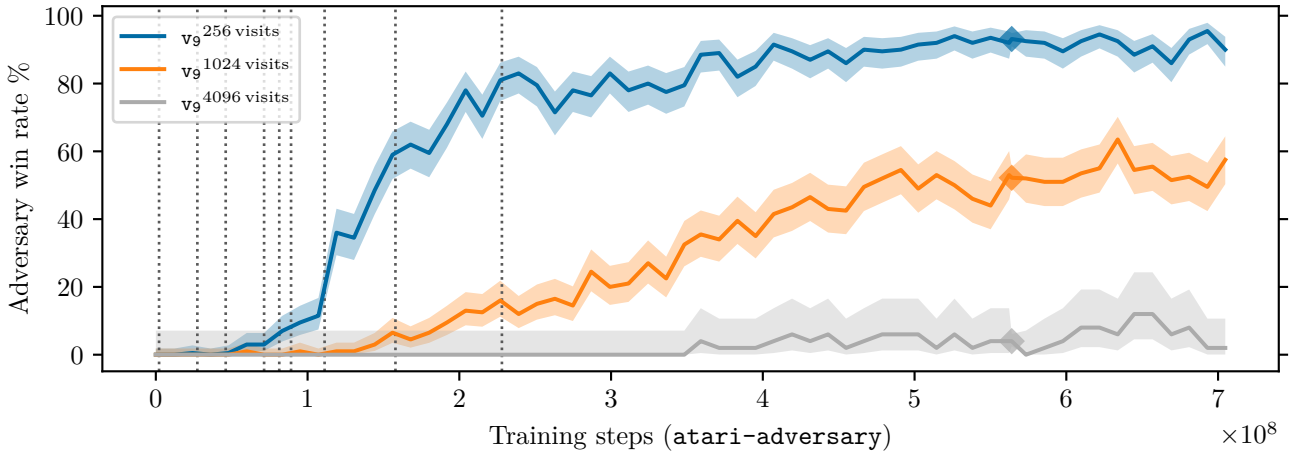


Figure M.7: This plot is the same as Fig. F.4 but with training steps on the x-axis instead of GPU-days.

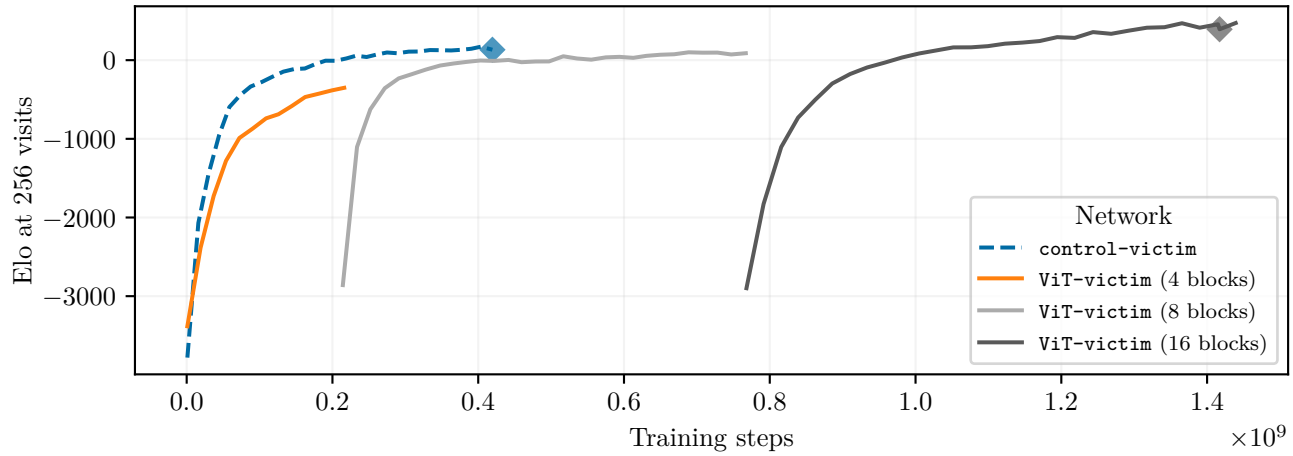


Figure M.8: This plot is the same as Fig. G.2 but with training steps on the x-axis instead of GPU-days.

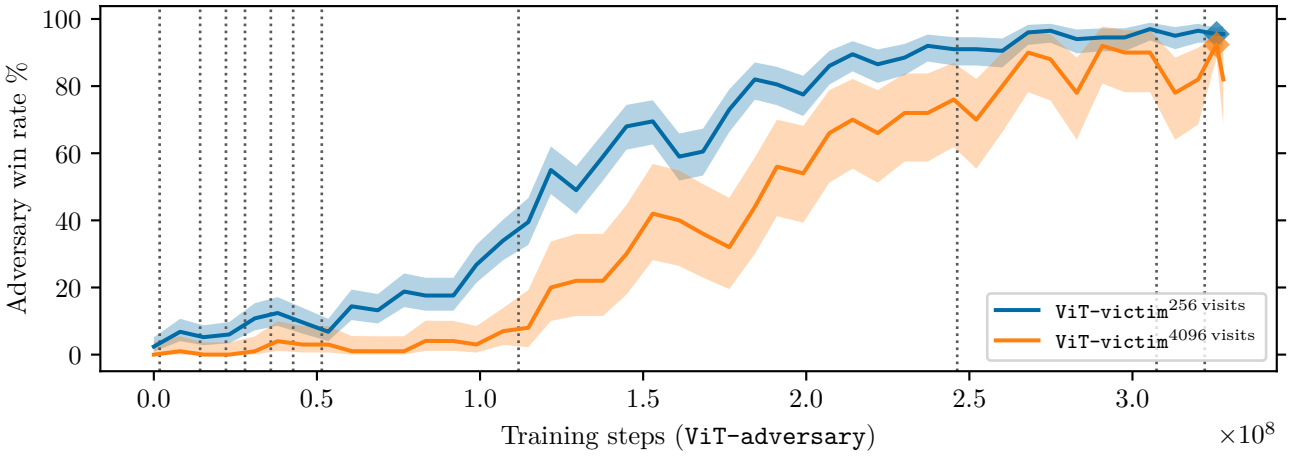


Figure M.9: This plot is the same as Fig. G.3 but with training steps on the x-axis instead of GPU-days.

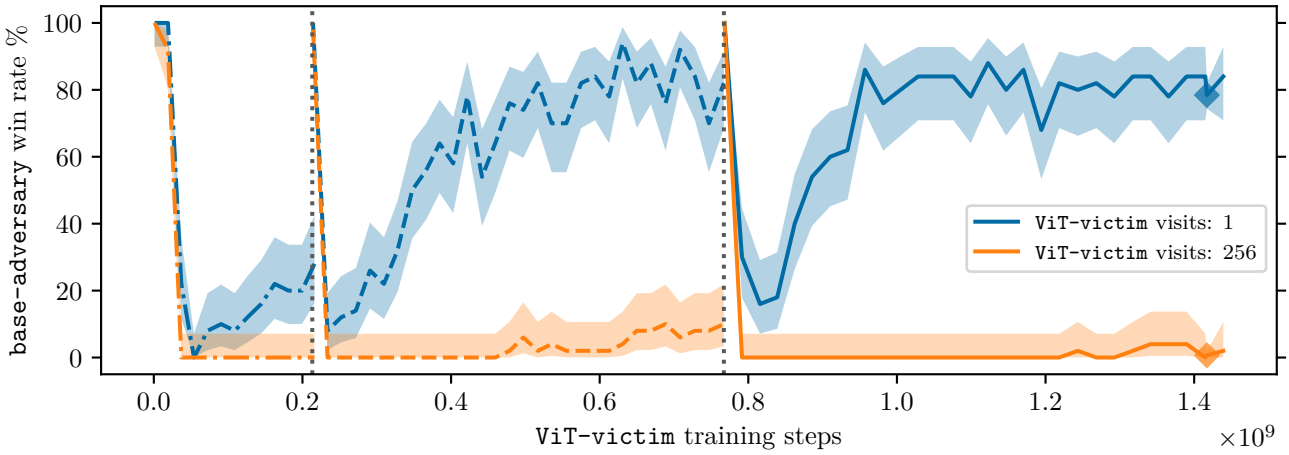


Figure M.10: This plot is the same as Fig. G.4 but with training steps on the x-axis instead of GPU-days.

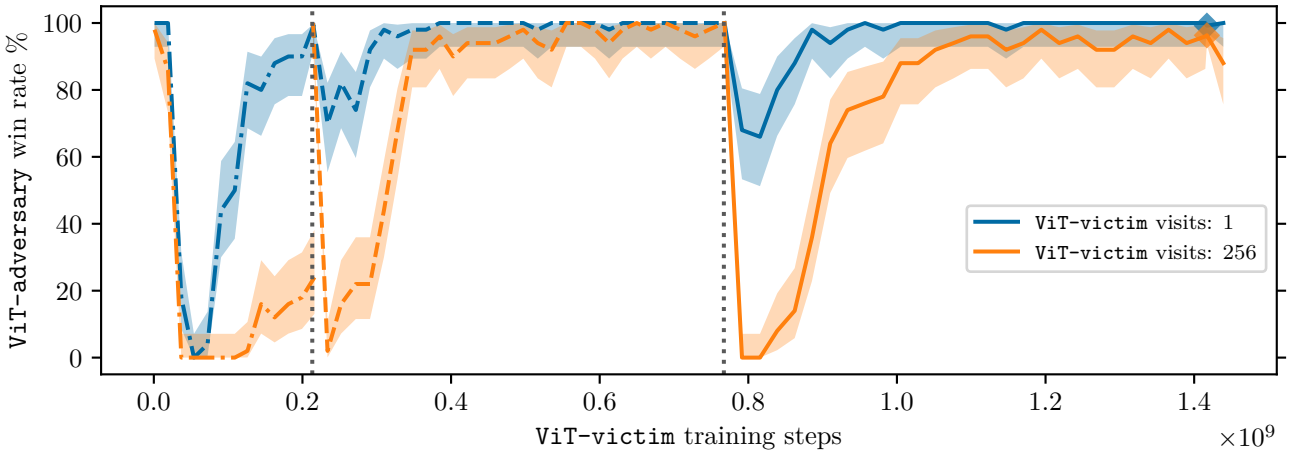


Figure M.11: This plot is the same as Fig. G.5 but with training steps on the x-axis instead of GPU-days.

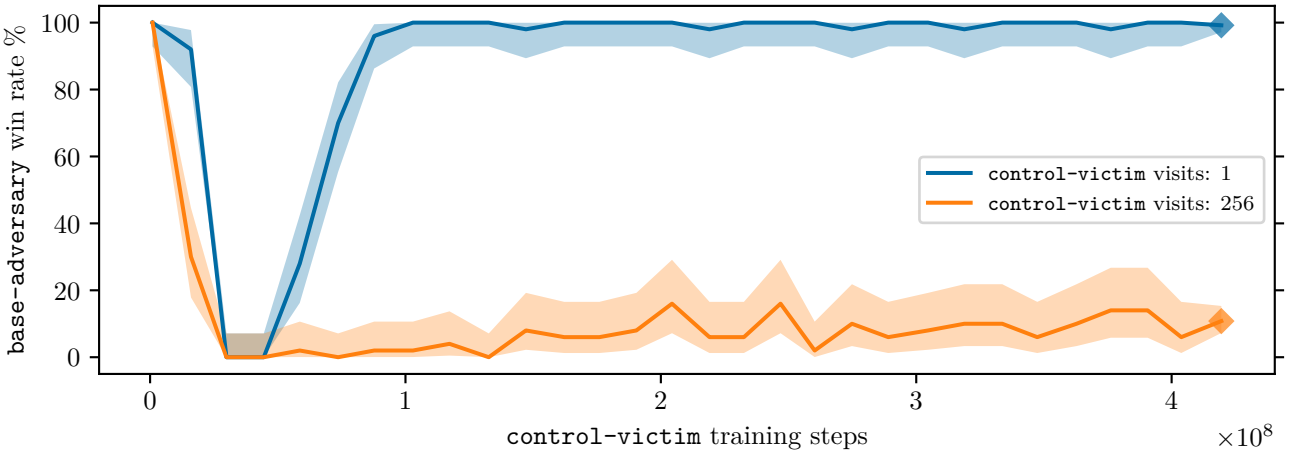


Figure M.12: This plot is the same as Fig. G.6 but with training steps on the x-axis instead of GPU-days.

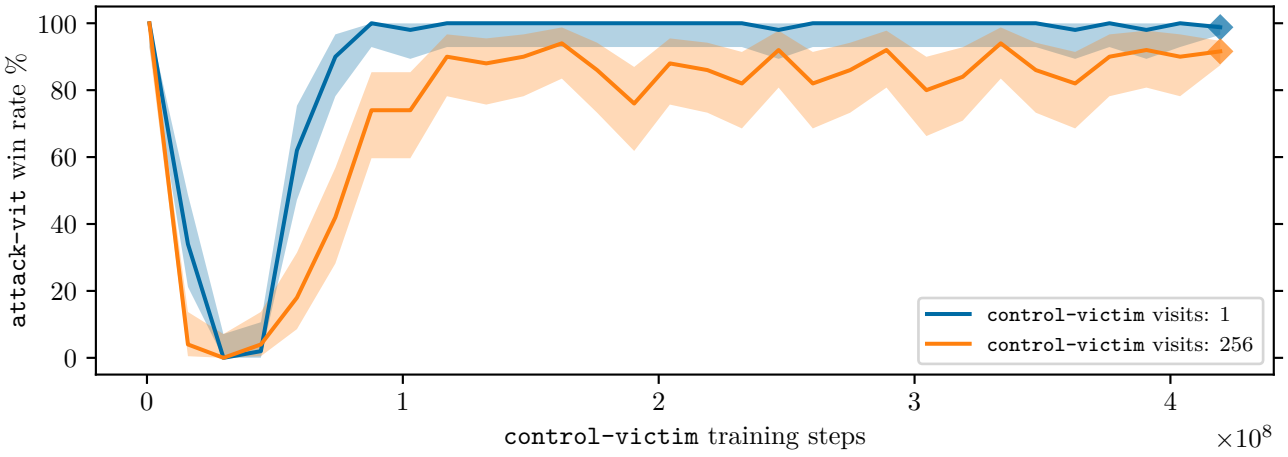


Figure M.13: This plot is the same as Fig. G.7 but with training steps on the x-axis instead of GPU-days.

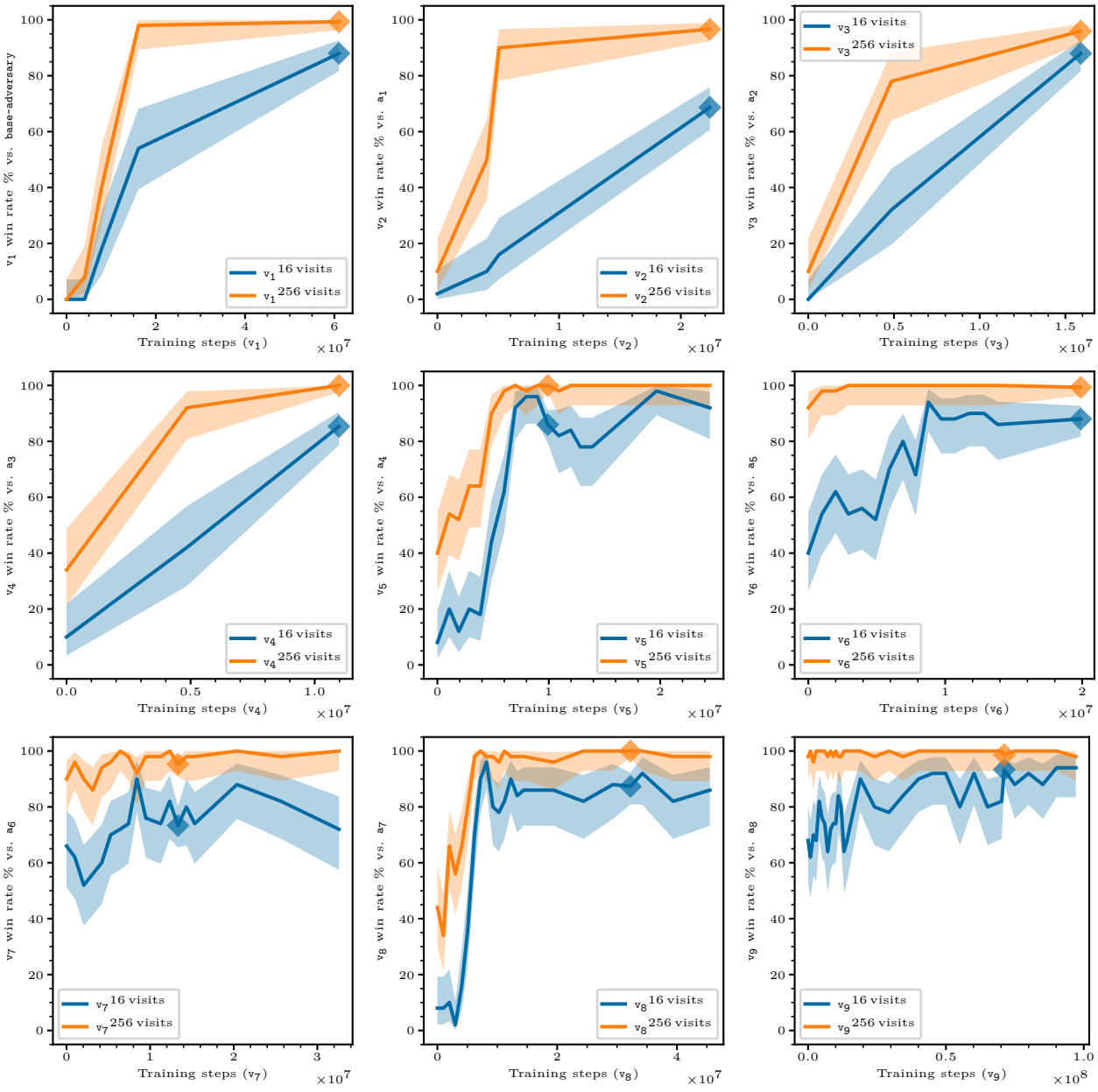


Figure M.14: This plot is the same as Fig. M.1 but with training steps on the x-axis instead of GPU-days.

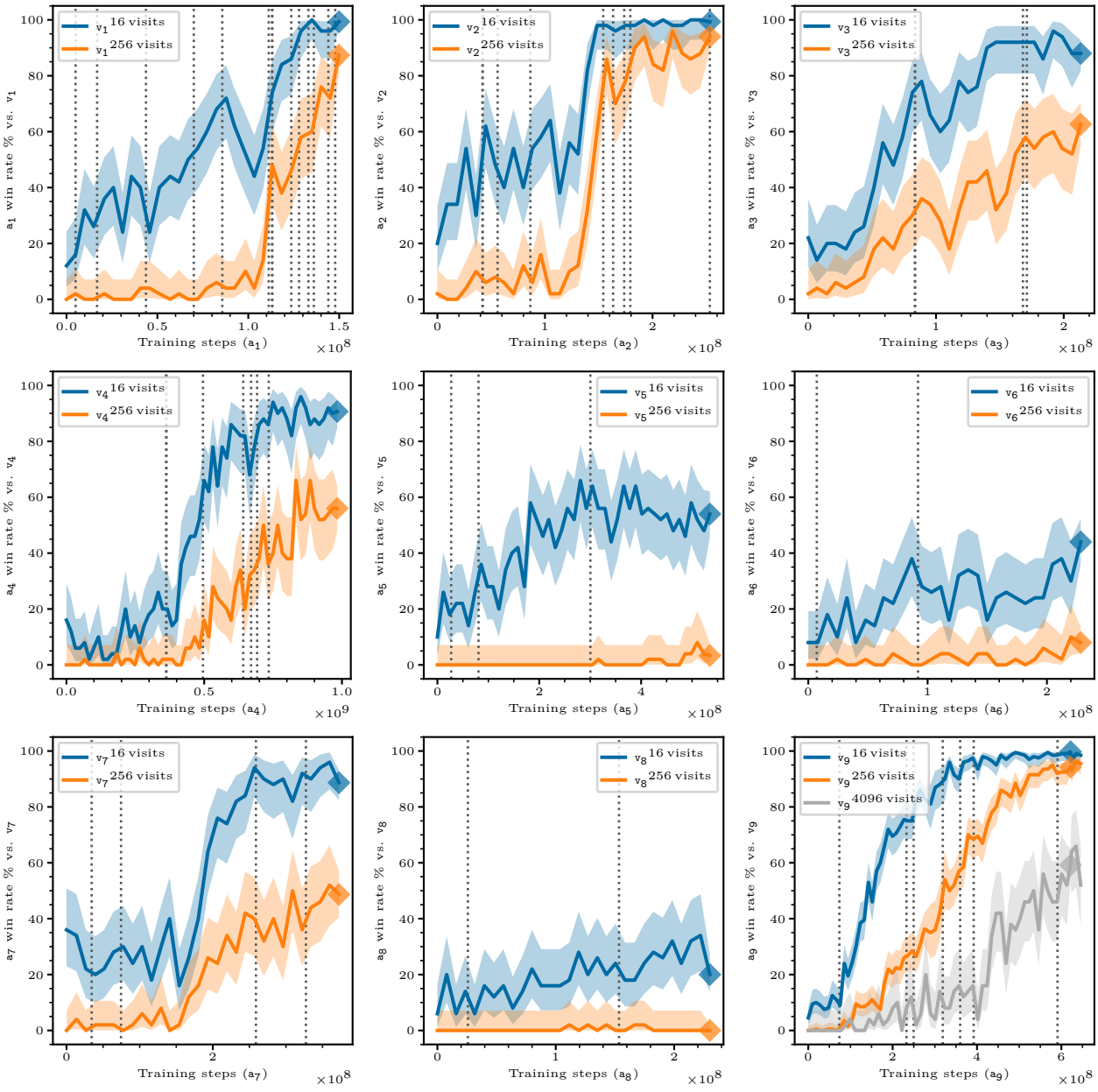


Figure M.15: This plot is the same as Fig. M.2 but with training steps on the x-axis instead of GPU-days.