ailyas@mit.edu | (226) 606-1668
https://www.linkedin.com/in/andrewilyas
70 Pacific St, Cambridge, MA, 02139

Andrew Ilyas

http://andrewilyas.com
https://github.com/andrewilyas

Education

- **Massachusetts Institute of Technology (Ph.D)** *2018-Present*
  - Analog Devices (ADI) Graduate Fellow
  - *Relevant Coursework:* 6.854 (Advanced Algorithms)
- **MIT (B.S Math, B.S. CS, M.Eng. CS)** *2015-2018*
  - *Relevant Graduate-Level Coursework:* 6.867 (Machine Learning), 6.437 (Infererence), 6.860 (Statistical Learning Theory), 6.861 (Theory of Intelligence), 18.102 (Functional Analysis), 6.853 (Algorithmic Game Theory), 6.806 (Natural Language Processing)

Preprints

*** denotes equal contribution**

- **A Ilyas***, Logan Engstrom*, Aleksander Madry. "Prior Convictions: Black-box Adversarial attacks with Bandits and Priors." arXiv preprint (2018).
- **A Ilyas**, Ajil Jalal, Eirini Asteri, Constantinos Daskalakis, Alexandros G. Dimakis. "Robust Manifold Defense: Adversarial Training using Generative Models." arXiv preprint (2018).

Publications

*** denotes equal contribution**

- Shibani Santurkar*, Dimitris Tsipras*, **A Ilyas***, Aleksander Madry. "How does Batch Normalization help Optimization? (No, it is not about internal covariate shift)." To appear in *NIPS 2018*. Oral presentation (top 0.6% of submitted papers)
- **Andrew Ilyas***, Logan Engstrom*, Anish Athalye*, Jessy Lin.* "Black-box Adversarial Attacks with Limited Queries and Information." *ICML 2018*.
- Anish Athalye*, Logan Engstrom*, **A Ilyas***, Kevin Kwok. "Synthesizing Robust Adversarial Examples." Oral presentation/Spotlight Demo at Machine Learning and Computer Security Workshop (NIPS 2017). *ICML 2018*.
- Constantinos Daskalakis*, **A Ilyas***, Vasilis Syrgkanis*, Haoyang Zeng*. "Training GANs with Optimism." Deep Learning Theory and Practice Workshop at NIPS 2017. *ICLR 2018*.
- **A Ilyas**, Joana M.F. da Trindade, Raul C. Fernandez, Samuel Madden. "Extracting Syntactic Patterns From Databases." *ICDE 2018*.
- **A Ilyas**. "MicroFilters: Harnessing Twitter for Disaster Management." *IEEE Global Humanitarian Tech Conf* (2014). Chairman's Award for Excellence in Technical Presentation.

Invited Talks (not including conferences)

- **Training GANs with Optimism**: Spotlight Talk, NY Academy of Sciences ML Symposium
- **Synthesizing Robust Adversarial Examples**: O'Reilly AI Conference Speaker
- **3D Adversarial Examples**: Intel Labs Invited Talk
- **Adversarial Examples in the Real World**: Two Sigma Research Invited Talk

Professional/Research Experience

- **Research Intern** *at* Two Sigma Labs *Summer 2018*
  - Working at Two Sigma Labs, an academic research team within Two Sigma Investments, on the robustness of deep reinforcement learning
- **Founder/Member** *at* LabSix *Fall 17'—Present*
  - Founded LabSix (labsix.org), student-run machine learning research group with research featured in BBC, IEEE Spectrum, WIRED Magazine, etc.
- **Research Intern** *at* Two Sigma Labs *Summer 2017*

- Working at Two Sigma Labs, an academic research team within Two Sigma Investments, on theoretical ML and convex optimization

- **Undergraduate Researcher (UROP) Positions:**
  - Poggio AI lab, CBMM MIT: Invariances in deep neural networks *Spring-Fall '17*
  - Madden Database Lab, CSAIL MIT: structure extraction from DBs *Spring '16 — '17*
  - Torralba Vision Lab, CSAIL MIT: Predictive power of CNNs *Fall '15*

- **Machine Learning Intern** *at* Twine Health *Summer '16*
  Sole member of ML team, responsible for all Data Science and ML initiatives.

- **SigProc Intern, Lead WatchOS dev** *at* Cambridge Mobile Telematics *Summer '14, '15*
  Worked with Prof. Sam Madden on texting-while-driving detection with mobile sensors; built commercial WatchOS app from scratch

- **MicroFilters (independent published research)** *Fall '14*
  A **crisis-mapping** system, acquired by UN Office for Coordination of Humanitarian Affairs for disaster response after Typhoon Yolanda

Awards and Honors

- Best Student Poster Award *at* IBM AI Horizons Colloquium *2018*
- First Place, Battle of the Hacks v3, v4 *at* a16z (Venture Capital Firm) *2016, 2017*
- Loran Scholarship for top 30 leaders in Canada (Declined) *2015*
- Second Place, International Autonomous Robot Racing Competition *2015*
- Canadian Open Math Challenge top 50, qual. to Canadian Math Olympiad *2015*
- Chairman's Award *at* IEEE Global Humanitarian Technologies Conference *2014*
- Silver Medal *at* Canada-Wide Science Fair *2014*
- Gold Medal, Division Champion, Award of Merit, Best in Fair *at* Waterloo-Wellington Regional Science Fair *2014*
- National Robotics Olympiad Winner, Qatar (year abroad) — qualified to World Robotic Olympiad, Malaysia *2012*
- Bronze Medal *at* Canada-Wide Science Fair *2012*

Selected Press (by Project)

- **IEEE Spectrum:** Hacked Dog pics Can Play Tricks on Vision AI (**http://bit.ly/2kMtxhU**, 2017)
- **WIRED:** Researchers fooled A Google AI into thinking … (**http://bit.ly/2DF8qWF**, 2017)
- **Fast Co.Design:** How MIT Students Fooled A Google Algorithm (**http://bit.ly/2BIdNqI**, 2017)
- **Engadget:** MIT students trick an AI into classifying this turtle as a gun **(engt.co/2iXG5kO, 2017)**
- **The Guardian:** Shotgun shell: Google's AI thinks this turtle is a rifle **(bit.ly/2zGWlRC, 2017)**
- **Fortune:** Why Google's Artificial Intelligence Confused a Turtle for a Rifle **(for.tn/2zGT44N, 2017)**
- **CTV News:** Haiyan responders get boost from Waterloo teen's program **(bit.ly/1ktT9Yo, 2014)**

Implementation Projects

- **Cubic**: Winner, Battle of the Hacks v4 (2017)—Smart context generation for general browsing
- **Falcon**: Winner, *Battle of the Hacks v3 (2016)*— Cross-platform browser history
- **Snorkel**: Built at MHacks—a tool for beginners to learn about machine learning
- **Pompeii**: Top 15 project, *Hack the North 2014*—App to help students keep up with courses
- **Apps**: Two apps published, "Draft" (2015) and "Lightning Labyrinth" (2013)
- **HackMIT**: Member of the organizing committee of HackMIT since 2015

Personal Interests

- Table Tennis (competitive), Soccer, Piano, Violin, Languages (Egyptian Arabic, French)