Science | DOI:10.1145/3323685

Gary Anthes

Lifelong Learning in Artificial Neural Networks

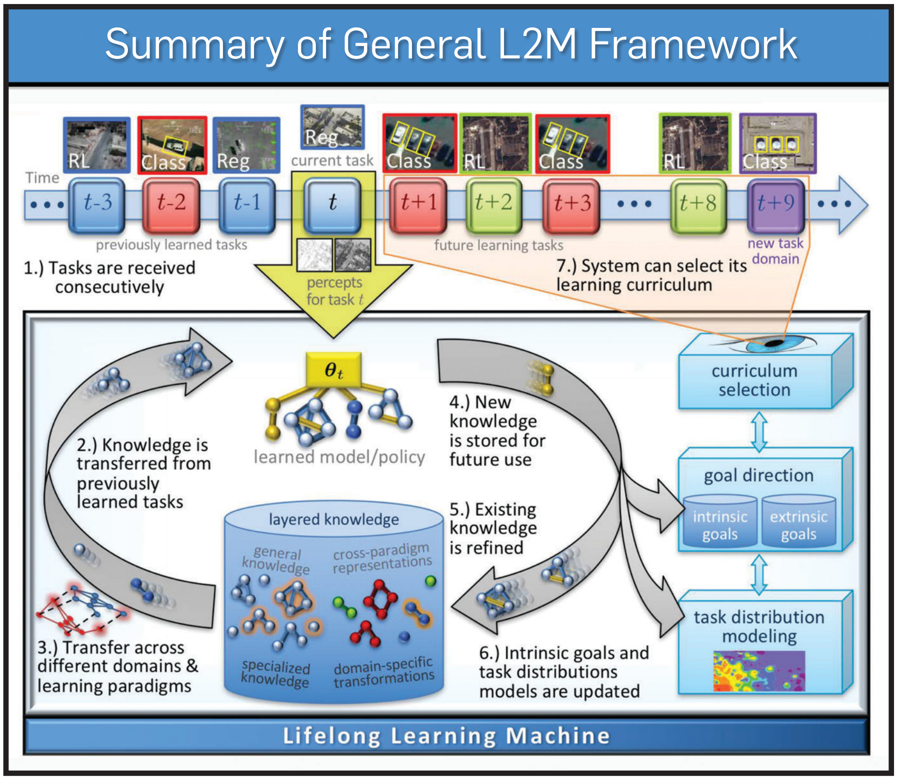
New methods enable systems to rapidly, continuously adapt.

Over the past decade, artificial intelligence (AI) based on machine learning has reached breakthrough levels of performance, often approaching and sometimes exceeding the abilities of human experts. Examples include image recognition, language translation, and performance in the game of Go.

These applications employ large artificial neural networks, in which nodes are linked by millions of weighted interconnections. They mimic the structure and workings of living brains, except in one key respect—they don't learn over time, as animals do. Once designed, programmed, and trained by developers, they do not adapt to new data or new tasks without being retrained, often a very time-consuming task.

Real-time adaptability by AI systems has become a hot topic in research. For example, computer scientists at Uber Technologies last year published a paper that describes a method for introducing "plasticity" in neural networks. In several test applications, including image recognition and maze exploration, the researchers showed that previously trained neural networks could adapt to new situations quickly and efficiently without undergoing additional training.

"The usual method with neural networks is to train them slowly, with many examples; in the millions or hundreds of millions," says Thomas Miconi, the lead author of the Uber paper and a computational neuroscientist at Uber. "But that's not the way we work. We learn fast, often from a single exposure, to a new situation or stimulus. With synaptic plasticity, the connections in our brains change automatically, allowing us to form memories very quickly."


Summary of General L2M Framework
Time
RL
Class
Reg
Reg
current task
Class
RL
Class
RL
Class
t-3
t-2
t-1
t
t+1
t+2
t+3
t+8
t+9
previously learned tasks
future learning tasks
new task domain
1.) Tasks are received consecutively
percepts for task t
7.) System can select its learning curriculum
θ_t
learned model/policy
2.) Knowledge is transferred from previously learned tasks
4.) New knowledge is stored for future use
curriculum selection
goal direction
intrinsic goals
extrinsic goals
layered knowledge
general knowledge
cross-paradigm representations
specialized knowledge
domain-specific transformations
5.) Existing knowledge is refined
3.) Transfer across different domains & learning paradigms
6.) Intrinsic goals and task distributions models are updated
task distribution modeling
Lifelong Learning Machine

The DARPA Lifelong Learning Machines (L2M) Program seeks to develop learning systems that continuously improve with additional experience, and rapidly adapt to new conditions and dynamic environments.

INFOGRAPHIC COURTESY OF DARPA'S ELECTRONICS RESURGENCE INITIATIVE

For more than 60 years, neural networks have been built from interconnected nodes whose pair-wise strength of connection is determined by weights, generally fixed by training with labeled examples. This training is most often done via a method called backpropagation, in which the system calculates an error at the synaptic output and distributes it backward throughout the networks layers. Most deep learning systems today, including Miconi's test systems, use backpropagation via gradient descent, an optimization technique.

> **"In a few years, much of what we consider AI today won't be considered AI without lifelong learning."**

Using that as a starting point, Miconi employs an idea called Hebbian learning, introduced in 1949 by neuro-psychologist Donald Hebb, who observed that two neurons that fire repeatedly across a synapse strengthen their connection over time. It is often summarized as, "Neurons that fire together, wire together."

With this "Hebbian plasticity,"

networks employ a kind of "metalearning"—in essence, they learn how to learn—based on three conceptually simple parameters. Pairs of neurons have the traditional fixed weights established during the training of the system. They also have a plastic weight called a Hebbian trace, which varies during a lifetime according to the actual data it encounters. These Hebbian traces can be computed in different ways, but in a simple example it is the running average of the product of pre- and post-synaptic activity.

The Hebbian traces are themselves weighted by a third fixed parameter, called the plasticity coefficient. Thus, at any moment, the total effective weight of the connection between two neurons is the sum of the fixed weight plus the Hebbian trace multiplied by the plasticity coefficient. Depending on the values of these three parameters, the strength of each connection can be completely fixed, completely variable, or anything in between.

"This is important work," says Ziv Bar-Joseph, a computational biologist at Carnegie Mellon University who was not involved in the work at Uber. "They have taken a principle from biology that was well known and shown it can have a positive impact on an artificial neural network." However, it is too early to say whether the method will represent an important advancement in large, mainstream applications of AI, he says.

With most large AI systems today, Bar-Joseph says, "You optimize, and optimize, and optimize, and that's it. If you get new data, you can retrain it, but you are not trying to adapt to new things." For example, he says, a neural net might have been trained to give

DARPA Projects in Lifelong Learning Machines

Columbia University is learning how to build and train self-aware neural networks, systems that can adapt and improve by using internal simulations and knowledge of their own structures.

The University of California, Irvine, is studying the dual memory architecture of the hippocampus and cortex to replay relevant memories in the background, allowing the systems to become more adaptable and predictive while retaining previous learning.

Tufts University is examining an intercellular regeneration mechanism observed in lower animals such as salamanders to create flexible robots capable of adapting to changes in their environment by altering their structures and functions on the fly.

SRI International is developing methods to use environmental signals and their relevant context to represent goals in a fluid way rather than as discrete tasks, enabling AI agents to adapt their behavior on the go.

—Gary Anthes

ACM News

The Trouble with SMS Two-Factor Authentication

Many use SMS two-factor authentication (2FA) on their smartphones to secure their online accounts, but not everyone understands its potential vulnerabilities.

You've probably seen SMS 2FA in action. An online account, upon login, prompts you to receive a second code on your phone via text message. You receive the second code, then enter it to confirm that you are the legitimate user of the account, and not a hacker.

Yet SMS 2FA can be hacked, too.

In late 2018, Amnesty International reported hackers had hijacked 2FA codes and compromised online accounts; malicious actors had recreated the websites of legitimate services to convince users to reveal their 2FA authentication codes.

SIM swapping is used by hackers to gain access to sensitive accounts "protected" by SMS 2FA, which has resulted in hundreds of millions of dollars in cryptocurrency theft. SIM swapping is when a hacker goes into a phone store pretending to be you, and convinces a staff member to port your SIM card information to a phone they own. The hackers then either convince the original owner to fork over login details, using the swapped SIM to intercept the SMS 2FA code sent after logging in, or they attempt to reset account passwords, using the swapped SIM to intercept the code sent to confirm they are the legitimate account owners.

In July 2018, a suspect was arrested for SIM swapping for the first time, according to crypto/blockchain media outlet CoinTelegraph. The perpetrator allegedly stole $5 million in cryptocurrency using the technique.

SMS 2FA has vulnerabilities, but these are not necessarily flaws in how it is designed, says Kaspersky Lab security researcher Vladimir Dashchenko. "In general, 2FA itself is a secure concept. Yet, the ways it is implemented may differ and could have vulnerabilities," he says.

"Codes sent over the Internet almost always have at least some risk of being stolen," says Mark Risher, Google director of product management for counter-abuse and identity services. "Any form of 2FA improves user security over a password alone; however, not all 2FA provides equal protection. Sophisticated attacks can work around some methods of 2FA."

Risher cites SMS-based phishing attacks as one such method. "Despite this, adding a phone number for two-step verification is still recommended if you can't use any other options," he notes.

The good news is there are other options.

One is Google's own Titan Security Key, a physical key developed using the open source security standard FIDO. When you log into Google services, the SMS 2FA code is sent to the security key instead of your phone; the physical security key then is inserted into your phone to complete the verification process. Risher says the firmware in the security keys has been "sealed permanently into a secure element hardware chip at production time and is designed to resist physical attacks aimed at extracting firmware and secret key material."

Another potential solution is Kaspersky's fraud prevention platform, which leverages machine learning and "continuous analysis of hundreds of parameters in real time" to assess if a user is legitimate. Says Daschenko, "During the whole session, [the system] is analyzing the behavioral and biometric data, device reputation, and other nonpersonalized information to detect any signs of abnormal or suspicious behavior."

That is certainly an improvement over relying on SMS 2FA alone.

—Logan Kugler is a freelance technology writer based in Tampa, FL, USA. He has written for over 60 major publications.

highly accurate results when classifying different kinds of automobiles, but when a new kind of car (a Tesla, say) is seen, the system stumbles. "You want it to recognize this new car very quickly, without retraining, which can take days or weeks. Also, how do you know that something new has happened?"

Artificial intelligence systems that learn on the fly are not new. In "neuroevolution," networks update themselves by algorithms that employ a trial-and-error method to achieve a precisely defined objective, such as winning a game of chess. They require no labeled training examples, only definitions of success. "They go only by trial and error," says Uber's Miconi. "It's a powerful, but a very slow, essentially random, process. It would be much better if, when you see a new thing, you get an error signal that tells you in which direction to alter your weights. That's what backpropagation gets you."

Military Apps

Miconi's ideas represent just one of a number of new approaches to self-learning in AI. The U.S. Department of Defense is pursuing the idea of synaptic plasticity as part of a broad family of experimental approaches aimed at making defense systems more accurate, responsive, and safe. The U.S. Defense Advanced Research Projects Agency (DARPA) has established a Lifelong Learning Machines (L2M) program with two major thrusts, one focused on the development of complete systems and their components, and the second on exploring learning mechanisms in biological organisms and translating them into computational processes. The goals are to enable AI systems to "learn and improve during tasks, apply previous skills and knowledge to new situations, incorporate innate system limits, and enhance safety in automated assignments," DARPA says at its website. "We are not looking for incremental improvements, but rather paradigm-changing approaches to machine learning."

Uber's work with Hebbian plasticity is a promising step toward lifelong learning in neural networks, says Hava Siegelmann, founder and manager of DARPA's L2M program and a computer science professor at the University of Massachusetts, Amherst. "We will never be safe in a self-driving car without it," she says. But it is just one of many necessary steps toward that goal. "It's definitely not the end of the story," she says.

There are five "pillars" of lifelong learning as DARPA broadly defines it, and synaptic plasticity falls into the first of these. The pillars are: continuous updating of memory, without catastrophic forgetting; recombinant memory, rearranging and recombining previously learned information toward future behavior; context awareness and context based modulation of system behavior; adoption of new behaviors through internal play, self-awareness, and self-simulations; and safety and security, recognizing whether something is dangerous and changing behavior accordingly, and ensuring security through a combination of strong constraints.

Siegelmann cites smart prostheses as an example of an application of these techniques. She says the control software in an artificial leg could be trained via conventional backpropagation by its maker, then trained to the unique habits and characteristics of its user, and finally enabled to very quickly adapt to a situation it has not seen before, such as an icy sidewalk.

A computational neuroscientist, Siegelmann says lifelong learning has been a goal of AI researchers for many years, but major advancements have only recently become feasible, enabled by advancements in computer power, new theoretical foundations and algorithms, and a better understanding of biology. "In a few years, much of what we call AI today won't be considered AI without lifelong learning," she predicts.

DARPA's Lifelong Learning Machines program does not seek incremental improvements, "but rather paradigm-changing approaches to machine learning."

Miconi's team is now working on making learning more dynamic and sophisticated than it is in his test systems so far. One way to do that is to make the plasticity coefficients, now fixed as a design choice, themselves variable over the life of a system. "The plasticity of each connection can be determined at every point by the network itself," he says. Such "neuromodulation" likely occurs in animal brains, he says, and that may be a key step toward the most flexible decision-making by AI systems.

Further Reading

Chang, O. and Lipson, H.
Neural Network Quine,
Data Science Institute, Columbia University, New York, NY 10027, May 2018
https://arxiv.org/abs/1803.05859v3

Chen, Z. and Liu, B.
Lifelong Machine Learning, Second Edition, ***Synthesis Lectures on Artificial Intelligence and Machine Learning*****, August 2018**
https://www.morganclaypool.com/doi/10.2200/S00832ED1V01Y201802AIM037

Hebb, D.
The Organization of Behavior: A Neuropsychological Theory, New York: Wiley & Sons, 1949
http://s-f-walker.org.uk/pubsebooks/pdfs/The_Organization_of_Behavior-Donald_O._Hebb.pdf

Miconi, T., Clune, J., and Stanley, K.
Differentiable Plasticity: Training Plastic Neural Networks with Backpropagation, ***Proceedings of the 35th International Conference on Machine Learning*** **(ICML 2018), Stockholm, Sweden, PMLR 80, 2018**
https://arxiv.org/abs/1804.02464

Miconi, T.
Backpropagation of Hebbian Plasticity for Continual Learning, ***NIPS Workshop on Continual Learning*****, 2016**
https://github.com/ThomasMiconi/LearningToLearnBOHP/blob/master/paper/abstract.pdf

Gary Anthes is a technology writer and editor based in Arlington, VA, USA