Towards AI Ingredients

Cameron Hughes (Northeast Ohio ACM Chair; cameronhughes@acm.org)
Tracey Hughes (Northeast Ohio ACM Secretary; tracey.hughes@neoacmchapter.org)
DOI: 10.1145/3402562.3402567

We have AI in our cars, in our mobile phones, and AI in our video games. We have AI in medicine, AI in the military applications, and AI in government agencies. It's getting harder to find an aspect of our daily lives that doesn't purport to have some kind of interaction with AI. We are relinquishing more of the personal and professional decision-making process to vestiges of evolving notions of AI. Not only are we starting to defer to AI for the decision-making process, we are subtly transferring the ultimate responsibility for the decisions and the consequences of those decisions to the AI. The public's acceptance and reliance on various aspects of AI is becoming normalized. One major problem with this scenario is that we as a society are unclear about what constitutes AI. Our social position on AI is: we may not be able to concisely or correctly define it, but we all know it when we see it, right? Clearly the integral part that AI has in our society makes this position untenable and we can and should do better with our definition.

Even among AI researchers, educators, and practitioners, there is some consternation and disagreement about what constitutes AI and what doesn't, and the fact that we are currently in an AI hype cycle doesn't help matters. It's no wonder that in the general public the term "AI" is routinely misconstrued and misapplied. In the AI community, we have a responsibility to properly demarcate the tenets of Artificial Intelligence, its mathematics, science, and application. We need to define things clearly for the laymen and the public at large. But a clear, concise definition or presentation of AI for the laymen or the public at large is a tall order. AI research areas and techniques cover a wide range. Consequently, the commercial and government applications that deploy AI techniques from various research areas can have significant differences. Table 1 shows some of the research areas from the Bio-inspired [1] approach to AI and the symbolic approach to AI.

Table 1. Areas of Research from Bio-inspired and Symbolic approaches to Artificial Intelligence.

Some Areas in Bio-Inspired Artificial Intelligence Research

- Artificial Neural Networks,
- Cellular Automata,
- Bio-inspired, nature-inspired algorithms, search and machine learning algorithms,
- Deep Learning,
- Neural Networks,
- Behavior-based modeling,
- Swarm Intelligence,
- Evolutionary Computing,
- Nature-Inspired Metaheuristic Algorithms,

Some Areas in Symbolic Artificial Intelligence Research

- Knowledge Representation using frames, scripts, oav, conceptual graphs, modal logics,
- Expert Systems,
- Logic-based Machine Learning e.g. Inductive Logic,
- Programming and Relational Learning,
- Common Sense Reasoning,
- Situational Calculus, Event Calculus,
- Answer Set Programming,
- Symbolic and Mathematical Logic,
- Agent-Oriented Programming,
- Associative Memory Models

Bio-inspired approaches to AI have different assumptions, goals, vernacular, techniques and tools than what are typically found in symbolic approaches to AI. They both represent two very different schools of thought when it comes to the possibilities of replicating human intelligence and behavior by computer programs or in computer hardware. While there are hybrids of both approaches, most researchers tend to pick sides and consequently the boundaries and the fundamental definition of what constitutes AI can vary dramatically depending on which side has the podium. To make matters worse, vagueness and ambiguity are introduced once these differing techniques, tools, and vernacular are manifested in the form of commercial or government applications. Further, many of these applications carry serious social implications and can have major positive or negative impact on society. Table 2 shows some uses of AI-based systems that are used in the law enforcement, the military, and the legal system. The AI used in each of these areas can irrevocably change the trajectories of the human lives involved.

Table 2. Areas of Research from Bio-inspired and Symbolic approaches to Artificial Intelligence.

LAW ENFORCEMENT

- **Facial Recognition (FaceFirst, FACES, PoliceOne)**
  Identify criminals and missing persons in public spaces and video footage.
  - **Used by:**
  - Police Departments,
  - US Airports,
  - National Human Genome Research Institute,
  - FBI.
  - **Technology Used:**
  - Principal component analysis using eigenfaces,
  - Linear discriminant analysis,
  - Multilinear subspace learning.

- **Smarter Physical Robots (DroneDeploy in CA)**
  - Bomb detonation,
  - Crime surveillance,
  - Crime scene investigation,
  - Accident Scenes,
  - Search and Rescue,
  - Crowd monitoring.
  - **Used by:**
  - Police Departments,
  - ICE,
  - FBI,
  - Border Patrol.
  - **Technology Used:**
  - Unmanned and Remote controlled,
  - Autonomous,
  - Some equipped with Face Recognition and other technology.

- **Pattern Identification and Predictive Policing**
  - Identification of counterfeit goods,
  - Crime detection/prediction,
  - Forensic analysis,
  - Identification of potential perpetrators, victims and locations at increased risk of crime.
  - **Used by:**
  - Police Departments (California, Washington, South Carolina, Alabama, Arizona, Tennessee, New York and Illinois).
  - **Technology Used:**
  - Big Data Algorithms/ML behavior scripts,
  - Neural networks,
  - Databases,
  - Predictive Analytics.

- **Bias Mitigation Tools**
  - Removes racial biasness from police reports that identifies a suspects race.
  - **Used by:**
  - Police Departments.
  - **Technology Used:**
  - Automatic Translation Information,
  - Identification, retrieval and information extraction.

- **Speech Recognition Interface (Nexgen, Dragon Law Enforcement for CAD/RMS Systems)**
  - Police reports, incident reports and search.
  - **Used by:**
  - Police Departments.
  - **Technology Used:**
  - Customized-Language/Statistical modeling.

- **AFI System Data Collection and Mining(Project Maven/Algorithmic Warfare Cross-Function Team)**

- Used to identify individuals, associations, or relationships that pose a potential law enforcement or security risk.
- **Used by:**
- Homeland Security,
- DoD.
- **Technology Used:**
- Computer vision algorithms,
- TensorFlow APIs assist in object-recognition on unclassified data.

- **COPLINK:**
  Develop information and knowledge management systems technologies from heterogeneous data sources.
  - Captures, accesses, analyze, visualize, and share law enforcement-related information in order to solve cases and develop police reports.
  - **Used by:**
  - Police Departments,
  - ICE.
  - **Technology Used:**
  - Database assessment/integration.

MILITARY

- **Lethal Autonomous Weapon Systems**
  Can independently search for and engage targets based on programmed constraints and descriptions. Current systems (as of 2018) are restricted to a human giving final command to attack.
  - **Offensive (Drones, Unmanned Vehicles):** Autonomously search, identify, and locate enemies but can only engage with a target when authorized by mission command.
  - **Defensive:** Autonomously identify and attack oncoming weapon systems.
  - **Used by:**
  - Military.
  - **Technology Used:**
  - Facial recognition,
  - Decision-making algorithms.

LEGAL SYSTEM

- **Prison Sentencing Recommendations (Compas-Correctional Offender Management Profiling for Alternative Sanctions)**
- **Predicting outcomes of future trials**
  - Combat biasness and provide consistency,
  - Used to assist in the sentencing of defendants by human judges,
  - Weighing contradicting legal evidence, rule on cases in order to help humans make better legal decisions.
  - **Used by:**
  - Court systems (New York, Wisconsin, California, Florida, and other jurisdictions).
  - **Technology Used:**
  - Machine Learning.

The applications and the domain areas shown in Table 2, express the seriousness and growing deference to AI in many aspects of society. We in the AI community have a solemn obligation to define what we mean by Artificial Intelligence, its limits, its applicable scope, failure rates, risks, potential benefits and costs. We have to find a way to clearly and effectively educate and inform the public about this technology. How else does the domain expert, community advocate as well as the laymen or public at large navigate the potential morass of notions that can be attributed to AI?

Considering the severity of the consequences of using AI in these applications and domains, what precautions and communications have been employed regarding the fallibility of AI? Humans are fallible. Our technology is fallible. Data models can be incorrect and incomplete. They can be correct and complete but transient in nature because of structure, geographical or culture changes in the underlying sample sets. Rules learned by machine learning can expire as a result of dramatic changes in the environment from which the data culled. Valid decisions made, or conclusions drawn by the AI today, might be invalid 10 years from now when made in the same environment but different circumstances. We have to effectively communicate the risks involved. But where to start? We've yet to produce a clear concise, correct definition of AI suitable. How do we communicate limits, risks, safety issues?

Could labels on the proverbial container help? That is, should we have labeling in AI suitable for public consumption? In the same way that we are now starting to demand labels for fruits and vegetables that have been genetically modified, or meats that are synthetic. Should we develop labels that describe the ingredients of the AI in these applications or services? Should we apply the notion of expiration dates and safe use to our AI applications and services in the same way that we place expiration dates and directions for safe use on foods and other consumables? Data models that are used as the basis of decision-support systems for Prison Sentencing Recommendation systems or criminal profiling can quickly become outdated as the result of population, cultural, social, or geographic change. So that a model that may be appropriate now, may not be applicable at some future date. Those data models are historic and may not take into account the biasness that exist in the data collection. The cost and effort required to produce data models, or rule-based systems that support the AI might introduce reluctance to routinely update those models or rules. Once these systems are put in place, there will be inertia to prevent change.

What Are the AI Ingredients?

Therefore, should we label the AI application, data model, or rule set with an expiration date or other temporal restrictions? Being able to describe AI ingredients such as:

- **Epistemic metrics,**
- **Reliability indices,**
- **Expiration dates, and other temporal restrictions,**
- **Applicability scope,**
- **Failure rates,**
- **Safety considerations,**
- **Federal Regulations/Law Alignment,**

require that we have shared concise and correct definitions for the various AI technologies for which these ”ingredients” will define and affect. Perhaps the simplest path to educating the public is to provide labels that contain the AI ingredients of an application, device or service. Using labels would allow the public to know what AI is being purported, under which situations it can be reliably and safely used, and when it expires. Table 2 shows some of the domain areas where AI-based systems are in use that have serious consequences for the public. If we had labels that detailed the AI ingredients of these applications then the public would be in a better position to ascertain the value and legitimate uses of such applications.

In AI Matters, Volume 5 Issue 2 entitled: What Metrics Should We Use To Measure Commercial AI?, we discussed the need to not only define AI, but to also be able to measure the AI that is in any given application, device, or service. Clearly and concisely definable AI, measurable AI, and labels that contain AI ingredients are steps in the right direction of educating and informing the public with respect to the proper viability, applicability, and utility of applications, devices, or services that claim the use of AI. The notion of AI ingredients is related to transparent AI and explainable AI. In the next issue of AI Matters, we want to take a closer look at the notions of labeling AI, measuring AI, and transparent AI.

References

[1] Floreano, Dario and Mattiussi, Claudio (2008). *Bio-Inspired Artificial Intelligence. Theories, Methods, and Technologies*. Cambridge, The MIT Press.

Related Articles

- Greengard, Samuel. *Policing the Future.* Communications of the ACM. VOL. 55 No. 3. March 2012. pages 19-21.
- Kugler, Logan. *AI Judges and Juries: Artificial intelligence is changing the legal industry*. Communications of the ACM. VOL. 61 No. 12. December 2018. pages 19-21.
- Goose, Stephen., Arkin, Ronald. *The Case for Banning Killer Robots*. Communications of the ACM. VOL. 58 No. 12. December 2015. pages 43-45.
- Pasquale, Frank. *Law and Technology: When Machine Learning Is Facially Invalid*. Communications of the ACM. VOL. 61 No. 9. September 2018. pages 25-27.

- Chen, Hsinchun., Zeng, Daniel., et. al. *COPLINK: Managing Law Enforcement Data and Knowledge*. Communications of the ACM. VOL. 46 No. 1. 2003. pages 28-34.

Cameron Hughes is a computer and robot programmer. He is a Software Epistemologist at Ctest Laboratories where he is currently working on A.I.M. (Alternative Intelligence for Machines) and A.I.R (Alternative Intelligence for Robots) technologies. Cameron is the lead AI Engineer for the Knowledge Group at Advanced Software Construction Inc. He is a member of the advisory board for the NREF (National Robotics Education Foundation) and the Oak Hill Robotics Makerspace. He is the project leader of the technical team for the NEOACM CSI/CLUE Robotics Challenge and regularly organizes and directs robot programming workshops for varying robot platforms. Cameron Hughes is the co-author of many books and blogs on software development and Artificial Intelligence.

Tracey Hughes is a software and epistemic visualization engineer at Ctest Laboratories. She is the lead designer for the MIND, TAMI, and NOFAQS projects that utilize epistemic visualization. Tracey is also a member of the advisory board for the NREF (National Robotics Education Foundation) and the Oak Hill Robotics Makerspace. She is the lead researcher of the technical team for the NEOACM CSI/CLUE Robotics Challenge. Tracey Hughes is the co-author with Cameron Hughes of many books on software development and Artificial Intelligence.