Alternative Facts:
Knowledge Graphs in the Age of Large Language Models

Dr. Ora Lassila
Principal Technologist
Amazon Neptune
Who am I?

Principal Technologist in the Amazon Neptune graph database team

Co-author of
• the original RDF specification
• the seminal paper on the Semantic Web

Recipient of the 1st ISWC “10-year award”

Former W3C Fellow & elected member of the W3C Advisory Board

Author of the KR system that flew on NASA’s “Deep Space 1” probe in 1998

Grand Prize winner, 1989 USENIX Obfuscated C Code Contest
Game plan

1. General observations about AI and its history
2. My worries about the current state of AI
3. Knowledge graphs to the rescue?

NB: This is not a talk about Neptune, and I only mention the Semantic Web once (OK, twice)
I have been studying AI for a long time...

This is the first page of my first published conference paper:

- Finnish AI Symposium 1984
- (I was in kindergarten a college freshman…)

I will take a “long view” discussing AI in this talk
What is AI anyway?

Historically, AI has been about logic and the manipulation of symbols
- “symbolic AI”
- symbol grounding problem

More recently, this manipulation has been more statistical in nature
- “non-symbolic AI”
- miraculously successful, but unable to explain results (backlash looms)

The broad goal of AI has been (and remains) automated problem solving
- the dream of “artificial general intelligence” still eludes us…
What is AI anyway?

Many technologies may have started out in the field of AI, but are now “mainstream”

- object-oriented programming
- dynamic memory management
- rule systems
- ontologies and graphs
- etc.

Pictured: CPU board of Texas Instruments Explorer II, a 36-bit bespoke hardware architecture for running Lisp
What is AI anyway?

I entered the field during an “AI boom” (1980s)

Many technologies were quite promising, but expectations led to “over-promising”, and eventually the so-called ”AI winter” (1990s)

Later, the “miraculous success” of non-symbolic methods (2000s and onwards)

Note: Everyone now fashions themselves as an AI expert, including those former colleagues of mine who earlier were downright hostile in their opposition of anything that smelled like AI
What is AI anyway?

AI has suffered from scarcity of computational ability (algorithms) and capability (CPU, memory), driving innovation also outside the field of AI

- machine translation in the 1960s
- running Lisp programs
- ML, neural networks, etc., require lots of CPU and memory

Amara’s Law seems to apply to AI quite well:

“We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run.”

– Roy Amara (American futurologist, 1925-2007)
What is AI anyway?

AI has suffered from scarcity of computational ability (algorithms) and capability (CPU, memory), driving innovation also outside the field of AI

- machine translation in the 1960s
- running Lisp programs
- ML, neural networks, etc., require lots of CPU and memory

Amara’s Law seems to apply to AI quite well:

“We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run.”

– Roy Amara (American futurologist, 1925-2007)
Large Language Models

Essentially these are massive ML models which, given some text, are capable of predicting what should come next (your mileage may vary)

• “autocorrect on steroids”

Typical flow of operations:

Write a “prompt”  =>  LLM  =>  Generated text
Large Language Models

Essentially these are massive ML models which, given some text, are capable of predicting what should come next (your mileage may vary)

• “autocorrect on steroids”

Typical flow of operations:

Write a “prompt” → LLM → Generated text

Adjust the prompt

New discipline: “prompt engineering” (seriously)
Large Language Models need a “human in the loop”

When people show you results from (say) ChatGPT, they have typically gone through this loop many times.

What is happening here? Why did we get the answer we got? Is it correct?

Write a “prompt” → LLM → Generated text → Adjust the prompt
Large Language Models are now being productized

OpenAI: GPT, ChatGPT (available on Azure)

Google: Bard

Amazon: Bedrock, Titan

Custom (domain-constrained) LLMs (e.g., Bloomberg)

Many companies are now building UIs using LLMs
My worries

My colleague Charles Ivie was experimenting with ChatGPT and asked it to write some Python code against the RDFLib library.

Resulting code was decent Python, but ChatGPT invented completely new API calls (that do not exist in the library, and never have).

This is still easy to detect, though.
My worries

A more chilling example:

• fake scenario (a school class trip that never actually took place)
• fake WP article cited as “evidence”
• but… a real person was named
My worries

We might be entering a true gilded age of “fake news”…

This example: AI-generated video used as a political attack ad, deliberately created to have nothing to do with actual facts
My worries

Many AI researchers and practitioners have called for LLM development to be paused or slowed down

• an open letter from the Future of Life Institute has approx. 30k signatures

They have the right set of worries…

• they call for AI to be “accurate, safe, interpretable, transparent, robust, aligned, trustworthy, loyal”

I think trying to limit innovation is a bad idea, however

• (and the proverbial cat is already out of the bag anyway…)

Instead, we need to develop technological safeguards and guardrails

• many such tools already in development (e.g., NVIDIA NeMo)
My worries, specifics

Symbol grounding, truth, world models

“Hallucinations”

Complexity of these systems is beyond what we can understand
  • hence the trial-and-error of “prompt engineering”

Cost? (= carbon footprint)

Non-symbolic AI in general tends to be “opaque”
  • more calls for “responsible AI” or “accountable AI” (this is hard, though)
  • backlash possible
Knowledge graphs?

The Semantic Web (as the foundation for practical KR and modern knowledge graphs) is much what we wanted from AI before the “AI winter”

Properly constructed knowledge graphs
  • employ well thought-out models/ontologies
  • represent curated knowledge (verifiable facts)

Graph databases (as means of storing KGs) have become commonplace, and graph technologies are now “mainstream”

What we need now is to understand how generative AI (and non-symbolic methods in general) can work with knowledge graphs
Knowledge graphs?

There are already promising results in letting LLMs write graph queries. KGs could provide the “grounding” and world models for LLMs.
Knowledge graphs?

There are already promising results in letting LLMs write graph queries. KGs could provide the “grounding” and world models for LLMs. Not just queries, but also (arbitrarily complex) ontological reasoning.

Ask a question → LLM → Generated query → Answers

© 2023, Amazon Web Services, Inc. or its Affiliates.
Knowledge graphs?

“System 1” and “System 2” [Stanovich & West, Kahneman]…?

Also, “architecture” of intelligence and consciousness [Sloman, Dennett, …]
What “scarcities” do we now experience with ML & LLMs?

At least these:
• correct, truthful results
• accountability
• explainability

In the past, unaddressed scarcity resulted in unkept promises and backlashes against the whole AI industry
## Knowledge graphs & LLMs

<table>
<thead>
<tr>
<th></th>
<th>LLMs (&amp; ML in general)</th>
<th>LLMs + KGs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Truth, world models</td>
<td>Nope</td>
<td>Yes</td>
</tr>
<tr>
<td>Hallucinations</td>
<td>Yes</td>
<td>I hope not…</td>
</tr>
<tr>
<td>Curated knowledge</td>
<td>Maybe</td>
<td>Yes</td>
</tr>
<tr>
<td>Timely results</td>
<td>Some day</td>
<td>Yes</td>
</tr>
<tr>
<td>Explainable results</td>
<td>Nope</td>
<td>Yes</td>
</tr>
<tr>
<td>“Accountability”</td>
<td>Nope</td>
<td>Yes</td>
</tr>
</tbody>
</table>
My “big” observation

AI systems are getting more sophisticated and more capable, and are more and more functioning autonomously

What we really need is a better understanding of how to operate such autonomous systems, how to limit their behavior appropriately, how to make them safe, etc.

Can we learn from human behavior?
• in human-to-human interaction, we tend to build a track record, and we build trust gradually
Summary

AI has a history of “bloated expectations”

LLMs: amazing results, but caution is called for

Knowledge graphs could provide the necessary grounding for LLMs

We have much to learn about how to operate autonomous systems
Thank you!

Contact:
- ora@amazon.com
- Twitter: @oralassila