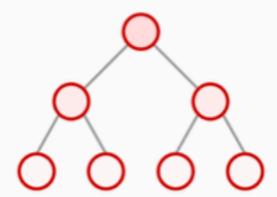
#### The Challenge of Compositionality for Al

June 29-30, 2022



A two-day online workshop on compositionality and artificial intelligence organized by Gary Marcus and Raphaël Millière.

#### What is compositionality?

A standard, theory-neutral way to state the principle of compositionality is as follows:

(C<sub>0</sub>) The meaning of a complex expression is a function of the meanings of its constituents and the way they are combined.

Zoltán Gendler Szabó/ The case for compositionality

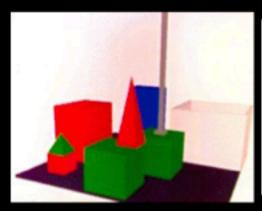
- The cat is on the mat specifies a meaning in terms of a relationship (ON) between some entities (THE CAT, THE MAT)
- the mat is on the cat specifies a different meaning; entities are same but relationship between entities is reversed
- Syntax guides the semantics
- Part of the goal of language comprehension is to recover those relationships
- Part of the goal of language production is to take an intent (specified in terms of relations between entities) in order to produce a structured string that represents the intent
- [also critical in vision, music, math, etc!]

# Is compositionality optional?

- Large Language Models don't directly implement compositionality at their peril
  - Whereas "semantic parsers" map sentences to meanings/intents, LLMs typically simply predict next words.
  - Those predictions are correlated with (traditional) meanings, but they aren't meanings.
    - there is no decomposition of a sentence into eg entities and relationships between those entities
    - and no accessible database that is (directly) updated
- This comes at a cost

## What's at stake (1): Dynamically-updated world models

 In a classical framework (eg SHRLDU), you can relate a compositionally-composed utterance to a dynamicallyupdated database



Person: DOES THE SHORTEST THING THE TALLEST PYRAMID'S SUPPORT SUPPORTS SUPPORT ANYTHING GREEN?

Computer: YES, THE GREEN PYRAMID.

Person: WHAT COLOR IS IT?

Computer: BY "IT", I ASSUME YOU MEAN THE SHORTEST THING THE TALLEST PYRAMID'S SUPPORT SUPPORTS.

Computer: RED

 Harder to do that (maybe impossible?) with unanalyzed points in vector space





# Blocks World would likely pose challenges for Gato

- GPT in general loses context over time
- Indirect tests\* indicate struggles with compositional interpretation
  - \*Prediction per se is not directly interpretable, so proxies for meaning can only be assessed indirectly eg via word problems



# What's at stake (2): Controllability

- pure prediction is hard to control; with holistic prediction, without interpretable meanings and database updates, you get terrific, broad linguistic coverage, BUT...
  - it's hard to ground LLMs ethically
    - tons of problems with bias and stereotyping, counseling harm etc
  - it's hard to ground them in terms of truth;
    - fabrication is frequent
  - it's hard to maintain coherence over the long term
- In systems like GPT-3, you can wind up a toxic spew of harmful advice and misinformation



#### Ethical and social risks of harm from Language Models

Lacer Weilinger<sup>2</sup>, John Weiler<sup>2</sup>, Marcheth Rath<sup>2</sup>, Cover Griffe<sup>2</sup>, Jonathus Tenain<sup>2</sup>, Po-Des Huang<sup>2</sup>, Myra Cheng<sup>2,2</sup>, Min Classe<sup>2</sup>, Sorje Rath<sup>2</sup>, Atomos Karistach<sup>2</sup>, <sup>2</sup>, Dat Rosme<sup>2</sup>, Anka Rosme<sup>2</sup>, Will Hawkins<sup>2</sup>, Ton Suphton<sup>2</sup>, Courtney Min<sup>2</sup>, Stokes Weiler<sup>2,2</sup>, Adda Stan<sup>2</sup>, Lacer Kinedi<sup>2</sup>, Lin Anne Hendricks<sup>2</sup>, William San<sup>2</sup>, Lone Legendri<sup>2</sup>, Coeffice Veiler<sup>2</sup>, and Sanon Colories<sup>2</sup>.

Sospilland, Validateia Institute al Technology, Valorenity al Tansans, Visionalty College Hobbs

#### Abstract

This paper aims to help ornerium the risk landwape associated with large scale Language Models (Libb). In order to finite advances in responsible interestion, as in depth understanding of the potential risks posed by those models is mented. A wide range of established and antisipated risks are analyzed in detail, drawing on multiblingibinary literature from computer science, languistics, and social sciences.

The paper confines do specific risk serse: I. Discrimination, Exclusion and Toxicity, E. Information Hazards, El. Manuformation Hazards, Nr. <u>Mathinso</u> Clees, V. Hazard-Computer Internation Factors, VI. Automation, Access, and Environmental Hazards.

The first risk error discourse fairness and matrixy risks in large scale larguage models. This includes four distinct risks: Lisk case oreast units illustrationates and expresserational and material laren by perpetuating attentions and social values, i.e. haveful associations of specific value with social obstation. Social socies and conqueries can exclude or manifolds who who exist nations them. Where a LM perpetuates such access quite the people coulder flow or "lastific" or flow "landing" obsept counts of a follow, mother and dulls" such a second entire, flowing a Life than professor many landing for some excluding people than others can create have the distribution of the contract of the c

The second risk area includes risks from priorse data leaks or from LMs correctly infecting private or order assailine information. These risks seem from private data that is present in the training corpus and from advanced informer capabilities of Life.

The third titl area comprises risks associated with 18th providing blue or midrading information. This includes the risk of creating less well informed soons and of seconding year in absent information. Mininformation can once beam in a seasitive domains, such as had bigal or models abstrat. Plear or this information may also had outen to profit on the information may also had outen to profit on the information may also had outen to profit out the profit of the information risks some in part from the processor by which Life boom to experience language; the underlying statistical methods are not well quotationed to distinguish formers information to increase information.

The fronth-risk area space risks of soons or product directiopers who any to use LMs to opean horn. This includes using LMs to increase the officery of distributions comparigns, to create personalized scene or frond at scale, or to directly-comparing could be of stream or weapon systems.

The Bifs this area forces on risks from the question or one of a "conversational agent" shot directly interests with huston some; This includes risks from presenting the quients as "bustons like", possibly leading users to occur one occurs to consider and one it is considerable risk to the consequences with each agents stay occur one occurs to study-late or exitant priors information from some. Life based conversational agents any pose title for our disability beams from consequences and an properturing atmosphes to self-presenting e.g. or "female unitsets". These risks seem to part from Life training objectives underlying each conversational agents and from product designs decisions.

The sinth risk area includes risks that apply to LHs and Artificial intelligence (NL) systems more broadly. Training and operating LHs can incur high environmental custs. LH based applications may benefit some groups more

# Compositionality is not mysterious

- Programming languages assume it, for example. So does math.
  - The semantics of (eg) a Python program are determined by the parts and the ways in which those parts are put together
  - Programs are represented by syntactic trees that have semantics that can directly be inferred from those trees.
- What is mysterious:
  - The precise nature of compositionality in human language
  - The proper role and implementation of compositionality in Al

# Three options going forward

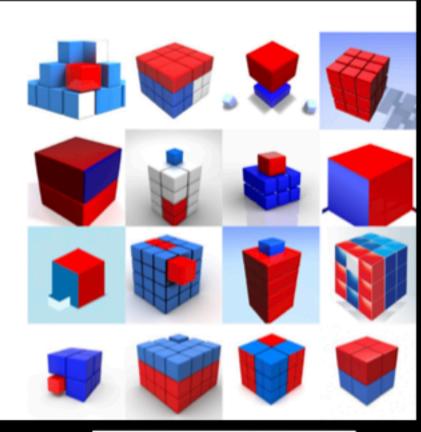
- We could build all of our AI on a symbol-manipulation framework, in which compositionality is explicit, and well-understood.
  - Lots of potential virtues in terms of verifiability and intepretability
  - Symbol systems are typically largely hand-wired, often brittle, not entirely satisfactory
- We could ignore the issue of compositionality, and hope that with enough data, things will sort themselves out.
  - LLM's produce strings that reflect the grammar of human language
  - But lack stability and grounding and do not produce interpretable meanings of input language
- We could try to find ways of incorporating compositionality into neural networks
  - Smolensky (1988, 2022); Marcus (2001)

# Banking on scaling alone might not be the best strategy

A look at compositionality in DALL-E

with examples of what you might hope for, and how it fails

### Dall-E 2 has lots of data, and lots of problems w compositionality



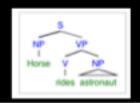
"a red cube on top of a blue cube".



Marcus, Davis, Aaronson (2022, arxiv)

# **Horse Rides Astronaut**

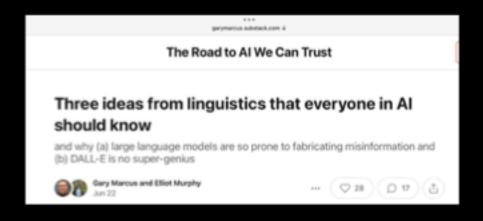








# comparatives



and see forthcoming manuscript, with Evelina Leivada

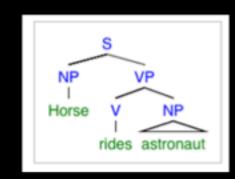


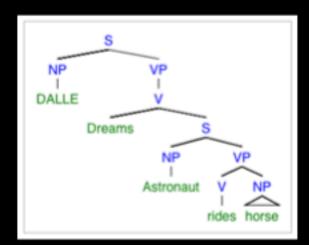
#### Does this mean neural networks are incompatible with compositionality?

- No!
- It means that some neural networks (e.g. DALL-E 2) are incompatible.
- Any symbol-manipulating system can be implemented (realized) in many different ways, including in a neural network (McCulloch & Pitts; Siegalmann & Sontag).
- The real question is, if we are to build AI out of neural networks, must we build a
  neural network that implements compositionality, in a way that maps 1:1 onto a
  classic symbolic system, or might a successful neural network offer some kind of
  alternative? (What kind of alternative?)
- Subquestion: might compositionality be something that is learned, rather than being something inherent (a la in the design of LISP)?

# Minimal Requirements for Compositionality as developed e.g. in Marcus (2001)

- Stable encodings of individual elements
- An operation that concatenates pieces of trees together
  - or disassembles wholes into parts
- Iterative processes for (de)constructing larger structures
- Representational formats for trees (or something very similar)
- Plus: Linking mechanisms that derive semantics relative to syntactic representation (eg Pinker 1984, 1989)





# the thing that Hinton is trying to do is very relevant

 GLOM is really an effort at building stable encodings that could be used in representations of complex wholes, very much like slide 1 on previous slide



Search...

Help | Adva

Computer Science > Computer Vision and Pattern Recognition

[Submitted on 25 Feb 2021]

#### How to represent part-whole hierarchies in a neural network

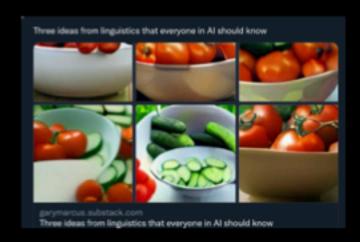
#### Geoffrey Hinton

This paper does not describe a working system. Instead, it presents a single idea about representation which allows advances made by several different groups to be combined into an imaginary system called GLOM. The advances include transformers, neural fields, contrastive representation learning, distillation and capsules. GLOM answers the question: How can a neural network with a fixed architecture parse an image into a part-whole hierarchy which has a different structure for each image? The idea is simply to use islands of identical vectors to represent the nodes in the parse tree. If GLOM can be made to work, it should significantly improve the interpretability of the representations produced by transformer-like systems when applied to vision or language

Comments: 43 pages, 5 figures

### Compositionality is not sufficient; it is a part of a framework

- Syntax -> Semantics -> cognitive models [best guess at external world, fictional worlds]
- we use language to accumulate knowledge ("is junk food more or less expensive than regular food?", "do people make junk food? do they grow it?")
- The real challenge is to build language understanding systems that can update their understanding of the world by decomposing meanings in terms of their parts, taken in context of speaker intent.





## A few words about humans

- Humans are interesting; we clearly understand wholes in terms of their parts, but there are also some deviations from ideal.
  - Machines allow arbitrary embedding; humans have trouble with center embedding (A man that a woman that a child that a bird that I heard saw knows loves)
    - My view: variable binding is expensive in humans, and we use a cuedependent substitute that is vulnerable to inference (Marcus, 2008).
  - Humans allow an immense number of "frozen forms" and idioms that are not internally compositional (kick the bucket, dead end, etc).

# Idioms are part of what makes NLU hard

- You don't understand kick the bucket by forming a representation of someone sending a
  projective force towards a pail.
- A good NLU system must blend (at least) two pathways:
  - pure semantics from syntax (which works for tipped over the pail)
  - with idiomatic retrieval (kick the bucket = died)
- A single sentence can combine both:
  - The person who tipped over the pail on Tuesday suddenly and unexpectedly kicked the bucket on Wednesday)
  - Getting all this right cries out for ML and classical NLU to work together

## **Conclusions**

- Compositionality in language is about systematically inferring (or generating) a meaning from parts, in a structure-dependent way
  - Flows naturally in symbolic paradigms (e.g. Python has a clear, structure-dependent semantics)
  - It doesn't automatically emerge from very large data (DALL-E)
  - You need some kind of innate architectural underpinning.
- · No fully adequate solution exists
  - Hand-writing all rules of a language is difficult
  - There is a large idiomatic periphery that ML ought to be able to help with
  - Current ML approaches tend to focus on feature-wise correlations; we need robust ML that works at scale over higher level abstractions
  - Hence lots of reasons for a r'approchment between symbolic and statistical approaches
- Compositionality ultimately is in service of something larger: dynamically updated cognitive models of the world. Capturing that workflow is vital if we are to build systems we can trust.