AI INSTITUTE #AIISC
UNIVERSITY OF SOUTH CAROLINA

UNIVERSITY OF SOUTH CAROLINA

CSCE 771: Computer Processing of Natural Language
Lecture 24: Conversation Agents

PROF. BIPLAV SRIVASTAVA, AI INSTITUTE

14TH NOVEMBER, 2024

Carolinian Creed: "I will practice personal and academic integrity."

Organization of Lecture 24

- Opening Segment
  - Recap of Lecture 23
- Main Lecture
- Concluding Segment
  - About Next Lecture – Lecture 25

Main Section
- Conversation Agents
  - Rule based methods
  - (Deep) learning based methods
- Applications
- Ethical Issues

Recap of Lecture 23

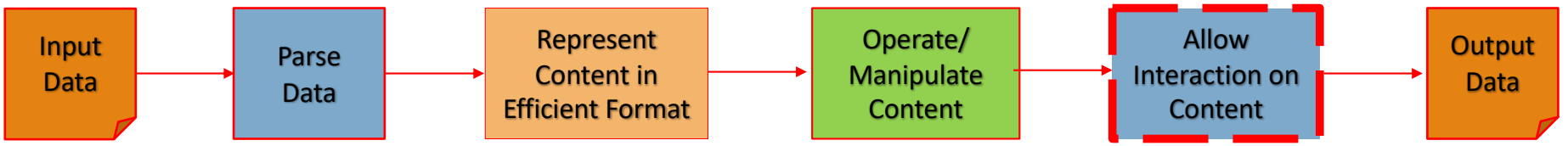
- Summary generation
- Methods
  - Extractive - traceable to original content
  - Abstractive – non traceable to original content
  - Compressive – remove content but not information
- Applications

Main Lecture

NLP Task – Stateful Interaction

The system itself can do any task:

- Question / answering
- Information retrieval
- Chitchat
- …



Chatbots - Background

- Conversation agents and interfaces (chatbots) are getting easy to build and deploy
  - Can be text-based or speech-based
  - Usually multi-modal (i.e, involving text, speech, vision, document, maps)
- Current chatbots typically interact with a single user at a time and conduct
  - Informal conversation, or
  - Task-oriented activities like answer a user's questions or provide recommendations

Demonstrations

- *Eliza*, http://www.manifestation.com/neurotoys/eliza.php3
- *Mitsuku*, https://www.pandorabots.com/mitsuku/

Current State

- Handle uncertainties related to
  - Natural language
  - Human behavior
- Dialog Management
  - Reasoning on data's abstract representations (Inouye 2004)
  - Learning policies over predictable nature of data (Young et al. 2013)
  - Statistical machine learning for dialog management: its history (Crook 2018)
- Hype around potential
- User feedback is mixed
  - Novelty value for chit-chat but concerns about usability (e.g., Tay)
  - Deployed for customer support commonly but usage is often low (compared to other channels), capability is limited (usually single turn), and not considered the preferred channel of choice for most users

References:

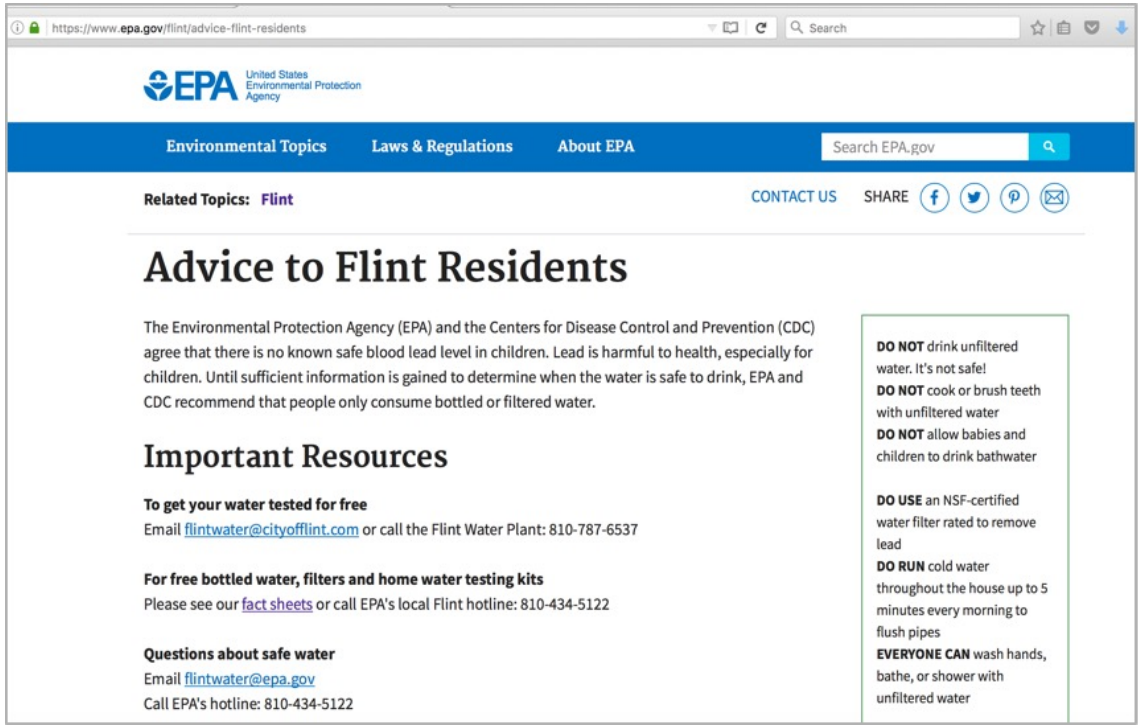
- May A.I. Help You?, https://www.nytimes.com/interactive/2018/11/14/magazine/tech-design-ai-chatbot.html
- M. McTear, Z. Callejas, and D. Griol. Conversational interfaces: Past and present. In The Conversational Interface. Springer, DOI: https://doi.org/10.1007/978-3-319-32967-3 4 , 2016.

Chatbots in Dynamic Environment

- Data changes, e.g. sensor data
- Groups of people, who come and go in environment
- Multi-modal interfaces, i.e., modes beyond conversation, like map, graphics and documents
- Dialog Management
  - Combination of learning and reasoning

S.No.	Dimension	Variety
1	User	1, multiple
2	Modality	only conversation, only speech, multi-modal (with point, map, ...)
3	Data source	none, static, dynamic
4	Personalized	no, yes
5	Form	virtual agent, physical device, robot
6	Purpose	socialize, goal: information seeker, goal: action delegate
7	Domains	general, health, water, traffic, ...

Current Practice of Water Advice



https://www.epa.gov/flint/advice-flint-residents

Search

EPA United States Environmental Protection Agency

Environmental Topics | Laws & Regulations | About EPA | Search EPA.gov

Related Topics: Flint | CONTACT US | SHARE

Advice to Flint Residents

The Environmental Protection Agency (EPA) and the Centers for Disease Control and Prevention (CDC) agree that there is no known safe blood lead level in children. Lead is harmful to health, especially for children. Until sufficient information is gained to determine when the water is safe to drink, EPA and CDC recommend that people only consume bottled or filtered water.

Important Resources

To get your water tested for free
Email flintwater@cityofflint.com or call the Flint Water Plant: 810-787-6537

For free bottled water, filters and home water testing kits
Please see our fact sheets or call EPA's local Flint hotline: 810-434-5122

Questions about safe water
Email flintwater@epa.gov
Call EPA's hotline: 810-434-5122

DO NOT drink unfiltered water. It's not safe!
DO NOT cook or brush teeth with unfiltered water
DO NOT allow babies and children to drink bathwater

DO USE an NSF-certified water filter rated to remove lead
DO RUN cold water throughout the house up to 5 minutes every morning to flush pipes
EVERYONE CAN wash hands, bathe, or shower with unfiltered water

Advisories to public for Flint Residents, MI, USA

Physical signage at a lake in Washington, USA

Decision-Support in Water: Problem and Objective

Guide every day people, who may be non-experts, with a multi-modal assistant to take data-based decisions specific to their needs, leveraging complex water quality data.

Audience

- General Public that wants to understand water quality at a specific location (e.g., swimming)
- Professionals with responsibility for regions (e.g., public health)

Before and After

Now: Static, non-interactive, non-contextual, lacks data details

Future: Anywhere, interactive, explain with data, contextual

Demo: Water Advisor

https://www.youtube.com/watch?v=z4x44sxC3zA

Jason Ellis, Biplav Srivastava, Rachel K. E. Bellamy, Andy Aaron, Water Advisor – A Data-Driven, Multi-Modal, Contextual Assistant to Help with Water Usage Decisions, at Proc. 32nd AAAI Conference on Artificial Intelligence (AAAI-18), New Orleans, Lousiana, USA, Feb 2-7, 2018. **[Demonstration, Water].**

AI Technical Issues in Collaborative Assistants for Water

Dimensions	General	Water Specific
Learning	Off-the-shelf trained intents	Water quality trends
Representation	Representation of raw data	Activity purpose and related parameters, water safety limits
Reasoning	Rule-based handling of missing values	Location and activity based regulation selection, interpreting safe limits for a parameter
Execution	Controlling interaction modules, asking questioning and parsing responses	Generating error rates, system confidence and usability rules
Human Usability Factors	Using error rates of conversation modules to control questioning strategy	Using missing data to control water advice in generated natural output.
Ethical Issues	Biases, adversarial examples, privacy violations, safety challenges and reproducibility concerns	Preference encoded in rules based on activities: recreation over drinking

Potential of Conversation Agents in Helping People

Characteristics and Potential

- Chatbots
  - Support a natural mode of interaction
  - Create a visible presence for an organization providing AI technology to users
  - Provide a sequential, slow mode of interaction (compared to the parallel, visual mode)
- Areas where people want help
  - Retrieve information
    - Contextual, user-specific, data access
    - Making data accessible to people with disability
  - Decision making: Helping choose among complex alternatives
  - Collaboration and mediation: among people making complex decisions

Everyday Scenarios - People

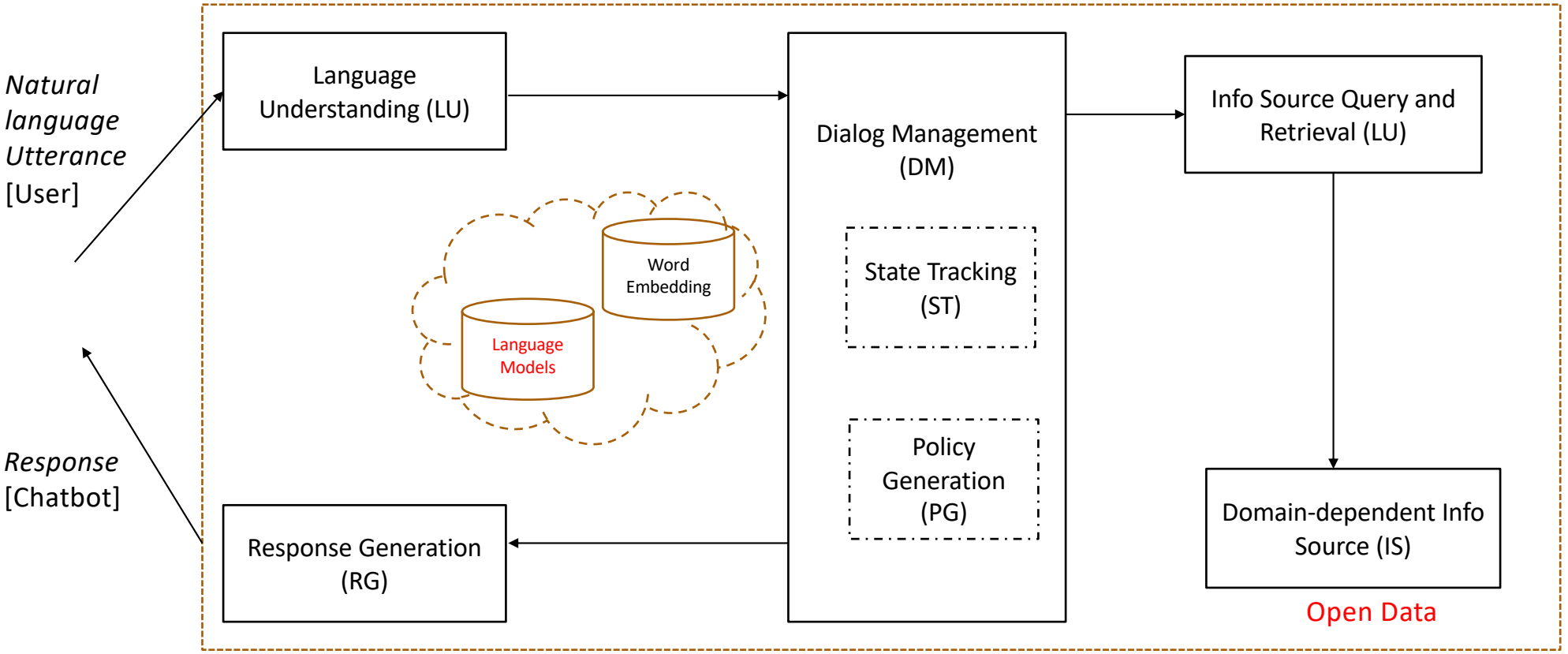
- Travel: “Which train can I take to office?”
  - Needs information about locations, train schedules and status, personal schedule
  - Category: information seeking
- Health: “Who can I see now for my pain in the stomach?”
  - Needs information about location, likely medical situation, medical specialties, doctors and health care providers in the vicinity, insurance and payment situation, availability of services
  - Category: information seeking, choosing among alternatives
- Social: “How do I meet my visiting friend with family at an evening?”
  - Needs information about schedule of friend’s family and mine, location of home and friend’s stay, capacity of home and restaurants in the area
  - Category: information seeking, choosing among alternatives, collaboration

Everyday Scenarios - Business

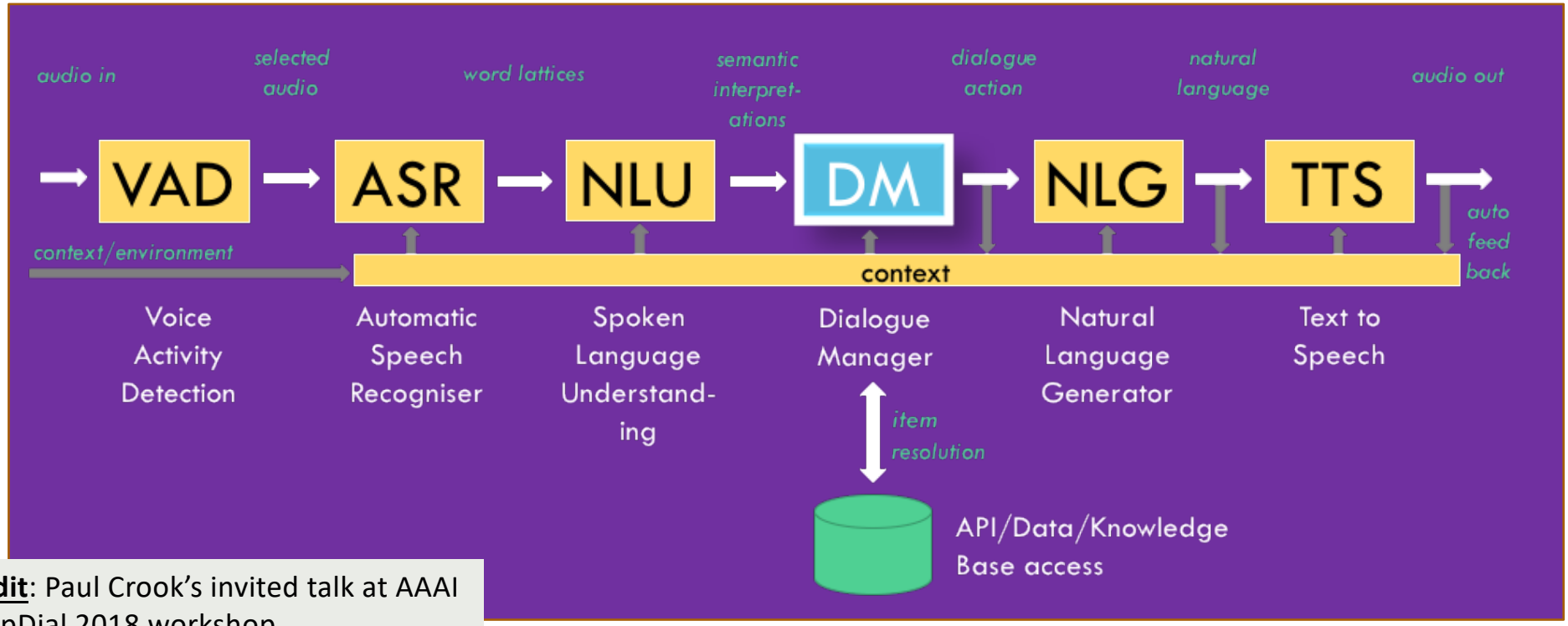
- Guidance
  - During data science
    - Rogers Jeffrey Leo John, Navneet Potti, Jignesh M. Patel, Ava: From Data to Insights Through Conversations. CIDR 2017
  - Skilling and professional development
- Collaboration and Mediation Decisions
  - Hiring a candidate
  - Scheduling an activity, e.g., medical operation
  - Merger and Acquisitions

Building a Chatbot

General Architecture - Chatbot



Modular Building Approach – Speech Augmented



Credit: Paul Crook's invited talk at AAAI DeepDial 2018 workshop

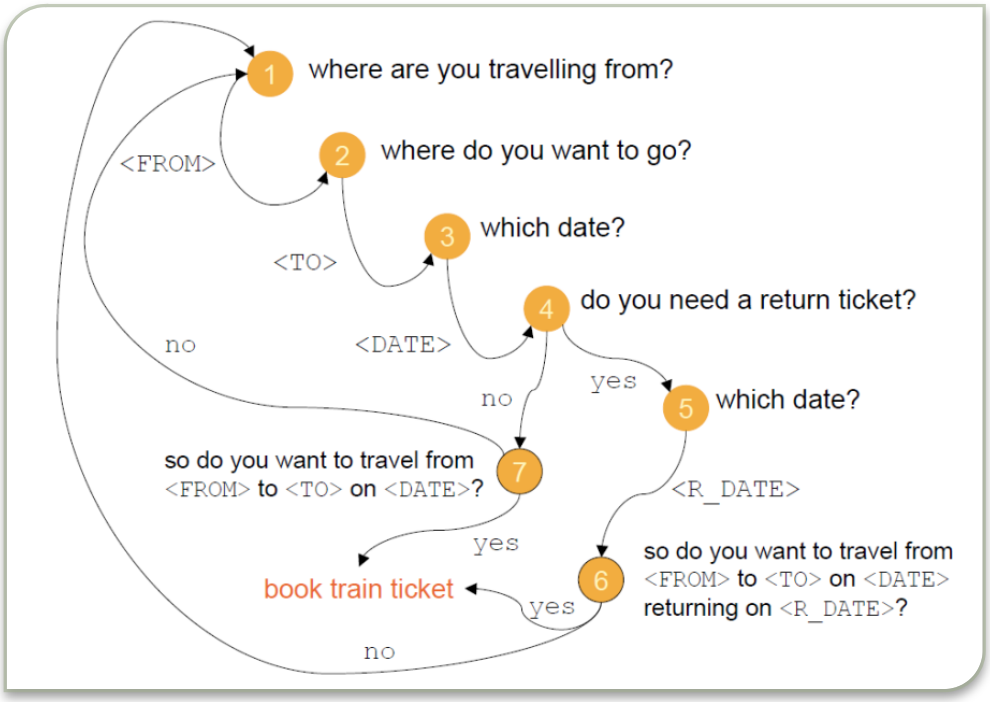
Open Source Tools

- Rasa – https://rasa.com/ // Primarily rules
- Open source LLM-based – e.g., Llama // Deep-learning based
- ParlAI - https://parl.ai/ // Flexible: Deep-learning / RL / rule-based
- MindMeld - https://www.mindmeld.com/ // Primarily rules
- Using a (open-source) LLM on ***chat*** task // Pre-trained deep-learning model

Type of Methods for Policy Generation

- Finite-state
- Frame-based
- Response-generation (including learning)
- Inference based (including planning)
- LLM-based
  - Prompting
  - Fine-tuning + prompting

Finite State DM / PG

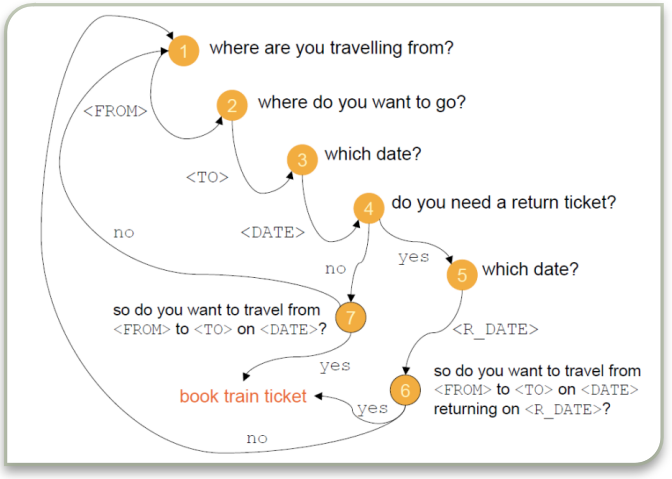


- Nodes both represent dialogue states and have associated output prompts by the system.
- Arcs represent expected user input. They lead to state transition.

Credit: Paul Crook's invited talk at AAAI DeepDial 2018 workshop

Finite State DM / PG

- The policy is a program at each node that the system executes if triggering conditions are met
- The set of possible paths in the flow diagram define the set of legal dialogues.
- The system has control over the conversation at all times.
- The user is assumed to be cooperative
  - Unexpected responses or extra information is usually ignored
  - System focused on the immediate / last user prompt.



Credit: Adapted from Paul Crook's invited talk at AAAI DeepDial 2018 workshop

Frame-Based DM/ PG

- A declarative, data-driven approach
- Frames consist of slots (variables), values and (system) prompts
  - Can be extended to capture ASR/NLU confidence scores, and grounding between the user and the agent
- A control algorithm determines what to say next based on the frame contents.
- The control specification can be as simple as *collect the first slot that has an unknown value*.
- Slots can be filled/refilled in any order and user responses can fill more than one slot.
  - Assumes an ASR and NLU models capable of interpreting multi-slot and out-of-expected-turn utterances.

Credit: Adapted from Paul Crook's invited talk at AAAI DeepDial 2018 workshop

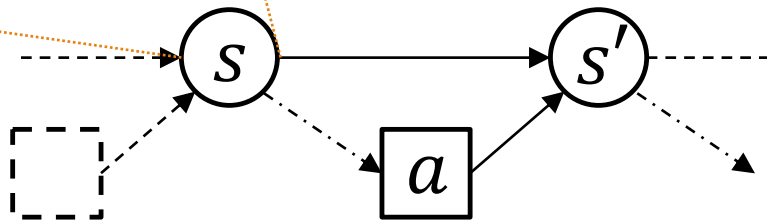
Example Frame

slot	value	prompt
ORIGIN	unknown	From which city are you leaving?
DESTINATION	unknown	Where are you travelling to?
DATE	unknown	When do you want to travel?

Frame-Based DM/ PG

Assuming the frame contains all the information required for the control algorithm to act optimally, the control task maps onto a Markov Decision Process (MDP).

slot	value	prompt
ORIGIN	unknown	From which city are you leaving?
DESTINATION	unknown	Where are you travelling to?
DATE	unknown	When do you want to travel?



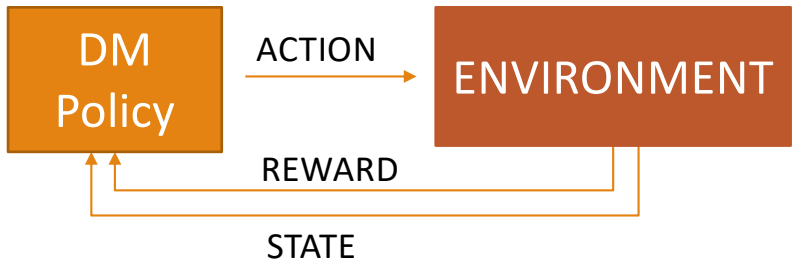
A MDP is defined as a tuple $\langle S, A, \mathrm{T}, \mathrm{R} \rangle$.
Established approaches exist for learning optimal policies.

Credit: Adapted from Paul Crook's invited talk at AAAI DeepDial 2018 workshop

Reinforcement Learning for DM

Given a MDP, techniques such as Reinforcement Learning (RL) can be applied to optimize the policy through trial and error.

RL framework:



Needs:

- Dialog data for training
- Variation: Partially observable MDP

Credit: Adapted from Paul Crook's invited talk at AAAI DeepDial 2018 workshop

Comparing Approaches

Credit: Adapted from Paul Crook's invited talk at AAAI DeepDial 2018 workshop

Finite-State DM

Procedural

Advantages:

- Easy to understand; many designers and developers familiar with procedural approaches
- Precise control of dialogue paths allows:
  - easy constraint of the dialogue when required (e.g. account payment processing)
  - risk adverse designs/simplified ASR & NLU
  - easier scripting of intelligent sounding prompts; e.g. accounting for pragmatics

Disadvantages:

- Ridged dialogues can frustrate users
- Flow-diagrams quickly become complex

Frame-Based/IS DM

Typically Declarative

Advantages:

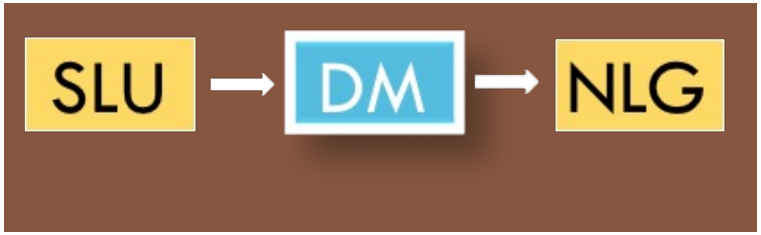
- Easy to author slot filling dialogs
- Allows for flexible, user directed and mixed initiative dialogues

Disadvantages:

- Scripting good system prompts is more challenging – need sophisticated NLG to avoid sounding robotic or repetitious (and to encode pragmatics)
- Imposing constraints on the dialogue paths can be complicated, e.g. developers less comfortable with declarative programming

Response Generation DM/ PG

- Response-Generation approaches collapse the user understanding to generation process by learning a direct input to output function

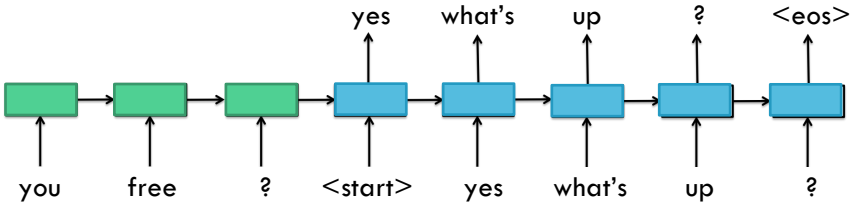


- They are appealing in that they
  - eliminate the manual design of internal ML features (especially Seq-2-Seq models),
  - are end-to-end trainable from unannotated NL "query-response" pairs,
  - have been shown to generate surprising engaging dialogues,
  - can capture human conversational norms like politeness, etc.

Credit: Adapted from Paul Crook's invited talk at AAAI DeepDial 2018 workshop

Response Generation Methods

- Information Retrieval / ranking query-response pairs.
  - [Filter, rank, and transfer the knowledge: Learning to chat. S. Jafarpour et al., NIPS, 2009]
  - [NPCEditor: Creating virtual human dialogue using information retrieval techniques. A. Leuski and D. Traum, AI Magazine 2011]
- Phrase-based Machine Translation.
  - [Data-driven response generation in social media. A. Ritter et al., EMNLP, 2011]
- Seq-2-Seq models.
  - [Neural responding machine for short-text conversation. L. Shang et al., ACL, 2015]
  - [A neural conversational model. O. Vinyals and Q. Le, ICML Deep Learning Workshop, 2015]
  - [A neural network approach to context-sensitive generation of conversational responses. A. Sordoni et al., NAACL HLT, 2015]



Credit: Adapted from Paul Crook's invited talk at AAAI DeepDial 2018 workshop

Inference-Based DM/PG

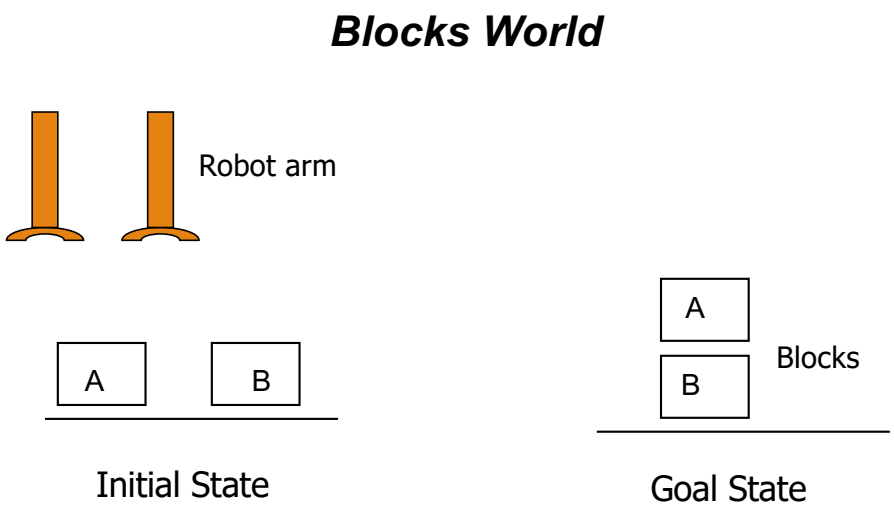
- Inference-Based DM considers dialogue as a planning task.
- The DM has a set of goals and axioms and is equipped with plan-based reasoner, e.g. a theorem prover.
- Dialogue acts are instances of goal-orientated *action schema*; typically specified in terms of constrains, preconditions, goals and effects, e.g.

$\mathbf{BOOK}(S, U, T)$
`Constraints:` $System(S) \wedge User(U) \wedge Ticket(T)$
`Goal:` $Booked(S, U, T)$
`Preconditions:` $Knows(S, Origin(T)) \wedge Knows(S, Dest(T)) \wedge ...$
`Effects:` $Booked(S, U, T)$

$\mathbf{INFO\_REQUEST}(A, B, P)$
`Constraints:` $Speaker(A) \wedge Addressee(B) \wedge Prop(P)$
`Goal:` $Know(A, P)$
`Preconditions:` $\neg Know(A, P) \wedge Desire(A, Know(A, P) \wedge Believe(A, Know(B, P)) \wedge ...$
`Effects:` $Believe(B, Desires(A, Know(A, P)))$

Credit: Adapted from Paul Crook's invited talk at AAAI DeepDial 2018 workshop

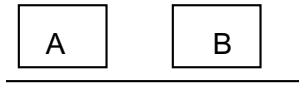
Reasoning Illustration - Planning Example



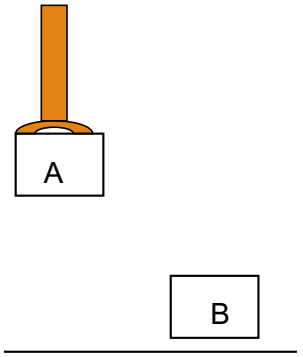
All robots are equivalent

Reasoning Illustration - Representation

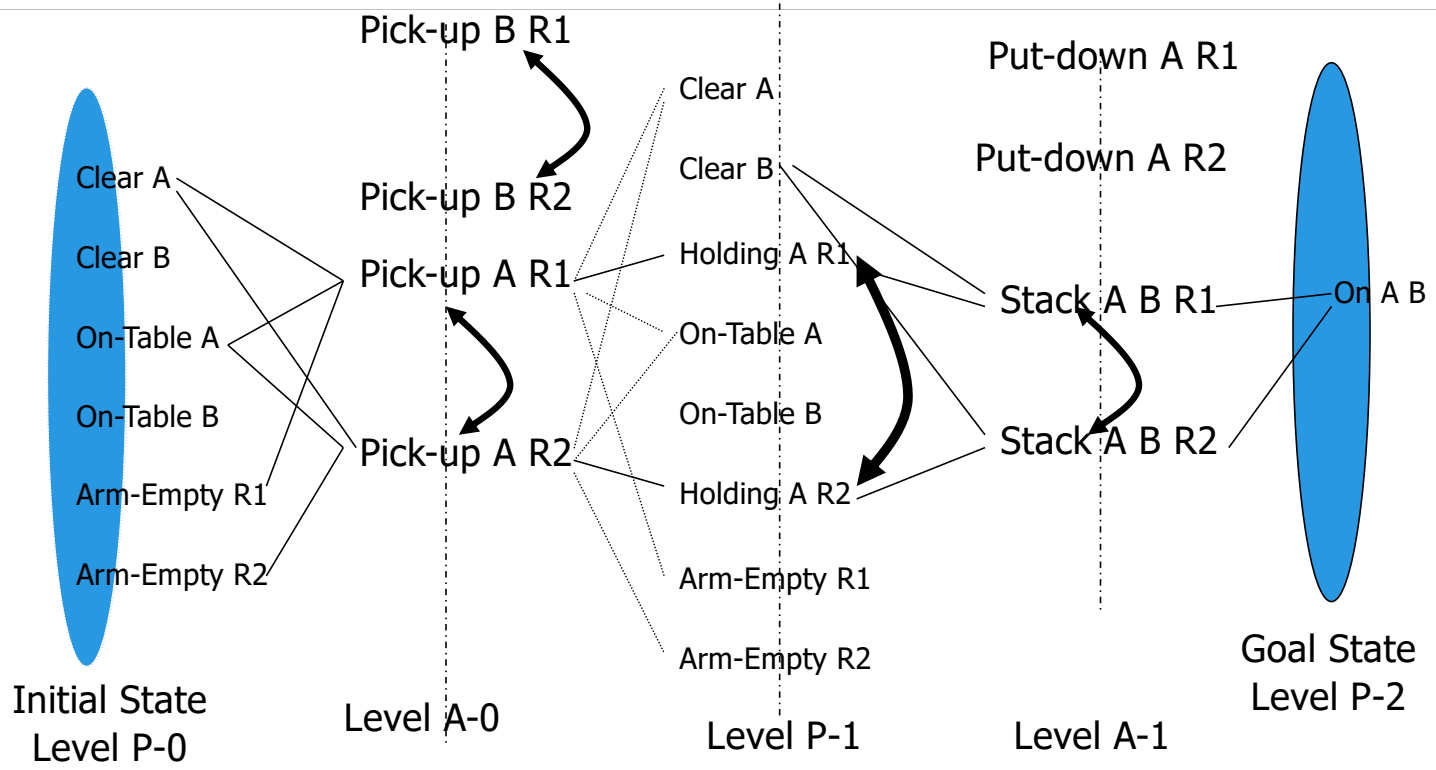
States: ((On-Table A) (On-Table B) …)



Actions: ((Name: (Pickup ?block ?robot)
Precondition: ((Clear ?block)
(Arm-Empty ?robot)
(On-Table ?block))
Add: ((Holding ?block ?robot))
Delete: ((Clear ?block)
(Arm-Empty ?robot)))…)



Reasoning Illustration - Planning Process



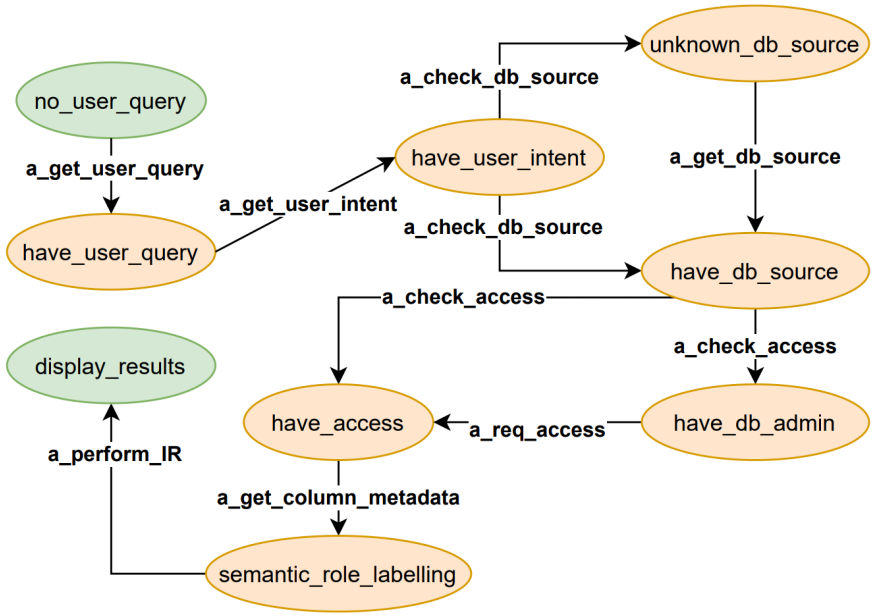
Inference-Based DM/PG

```
(:action no_db_source
    :parameters (?x ?y)
    :precondition (and
      (have_user_intent ?y)
      (not (have_db_source ?x))
    )
    :effect (and (no_db_source ?x))
)
```

a. An action in the domain file

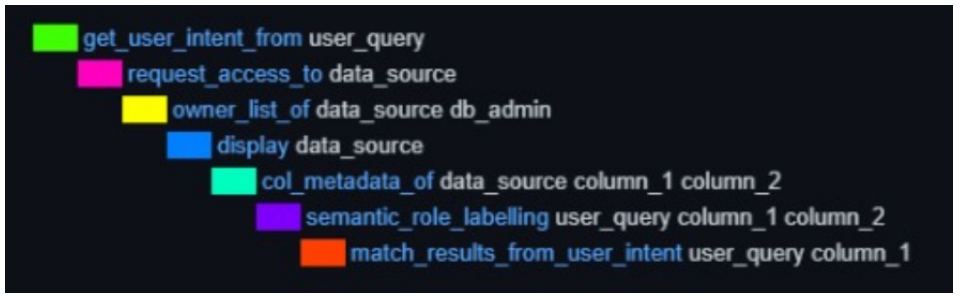
```
(:goal (and
{% if data.DB_present %}
    (get_user_intent {{data.user_query}})
    {% for db in data.DataBase %}
        (open {{db.name}})
        {% for col in db.content %}
            (get_col_metadata {{col}})
            (role_labelled {{data.user_query}} {{col}})
        {% endfor %}
        (display {{db.content[0]}})
    {% endfor %}
{% else %}(no_db_source {{data.if_not_present}})
{% endif %}
))
```

b. Goal description of the problem file



Induced State Transition Diagram

Dialog Plan



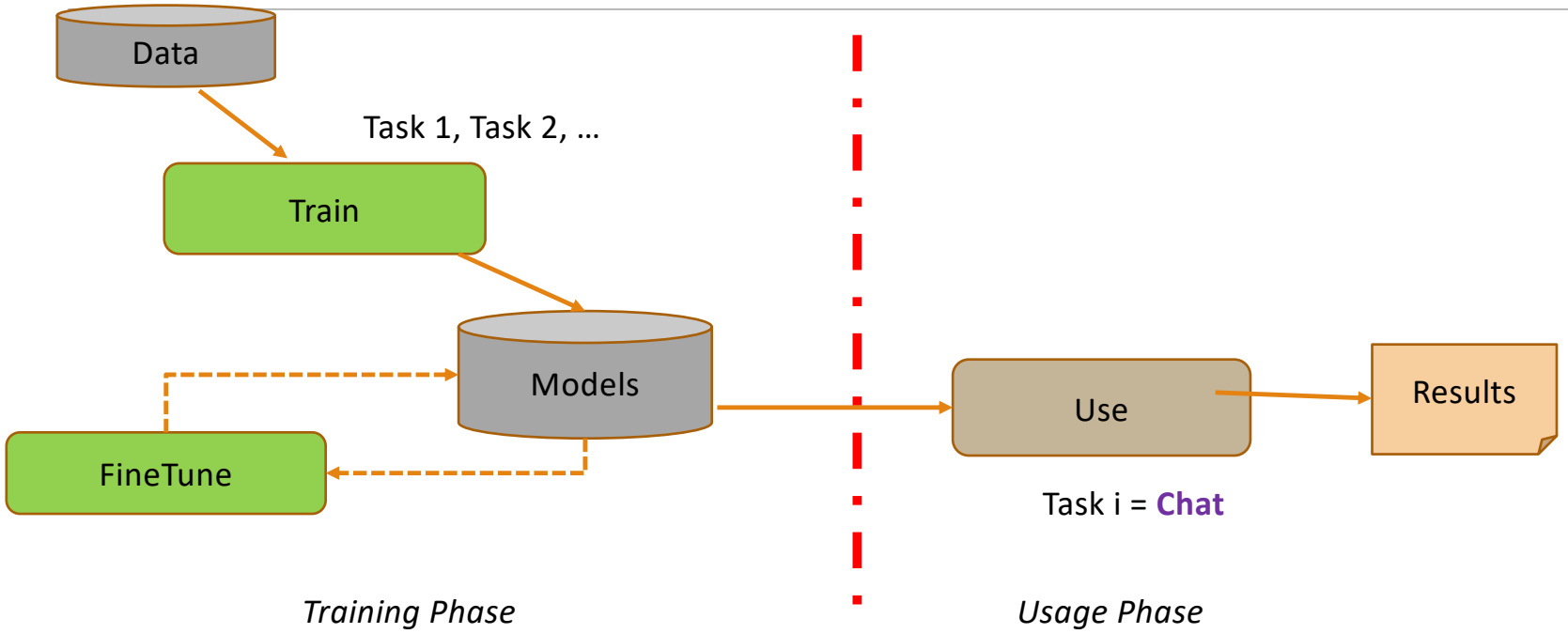
References: Inference Based DM

- A Generic Dialog Agent for Information Retrieval Based on Automated Planning Within a Reinforcement Learning PlatformV Pallagani, B Srivastava, Bridging the Gap Between AI Planning and Reinforcement Learning (PRL), 2021
- Botea, A.; Muise, C.; Agarwal, S.; Alkan, O.; Bajgar, O.; Daly, E.; Kishimoto, A.; Lastras, L.; Marinescu, R.; Ondrej, J.; Pedemonte, P.; and Vodolan, M. 2019a., Generating Dialogue Agents via Automated Planning. In https://arxiv.org/abs/1902.00771.
- Cohen, P. R. 2018. Back to the future for dialogue research: A position paper. On Arxiv at: https://arxiv.org/abs/1812.01144
- Chp.16 “Computational Models of Dialogue”, Ginzburg and Fernández, in The Handbook of Computation Linguistics and Natural Language Processing, 2010]

References

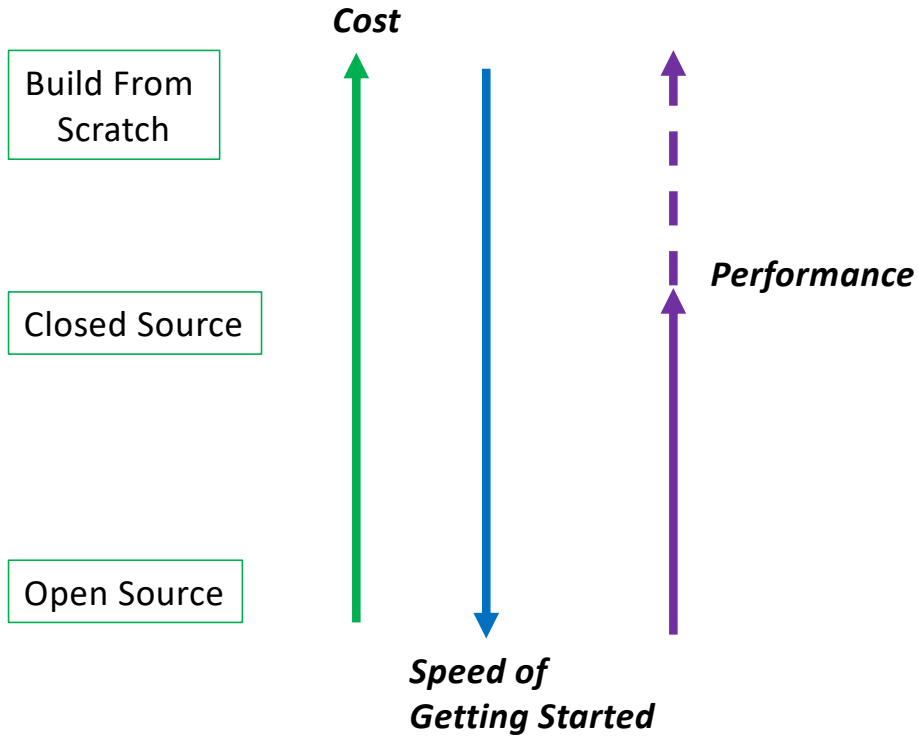
- Review paper - Santos Teixeira, M., Dragoni, M. A Review of Plan-Based Approaches for Dialogue Management. Cogn Comput 14, 1019–1038 (2022). https://doi.org/10.1007/s12559-022-09996-0 (PDF: https://link.springer.com/content/pdf/10.1007/s12559-022-09996-0.pdf)
- Yunfeng Zhang, Q. Vera Liao, and Biplav Srivastava. 2018. Towards an Optimal Dialog Strategy for Information Retrieval Using Both Open- and Close-ended Questions. In Proceedings of the 23rd International Conference on Intelligent User Interfaces (IUI '18). Association for Computing Machinery, New York, NY, USA, 365–369. https://doi.org/10.1145/3172944.3172998

Large Language Models (LLMs) based Chatbot



Practical Considerations

- How much can you pay?
  - Free open-source models, i.e., weights are available for download (Llama, Mistral, …) v/s Closed models (GPT, Gemini, Claude, …)
- Can you afford to share your data? Yes/ No
- Will others be using your model? Yes / No



Options

- Assumption: Already tried a pre-trained model and know performance on one's tasks
- Option 1: Fine-tune a pretrained model
- Option 2: Use someone-else's pretrained model
  - Creating mini-GPT (OpenAI): https://help.openai.com/en/articles/8554397-creating-a-gpt
- Option 3: Build one's own on specialized data, tasks and optimizing performance metrics of interest

Ethical Issues – A Preview

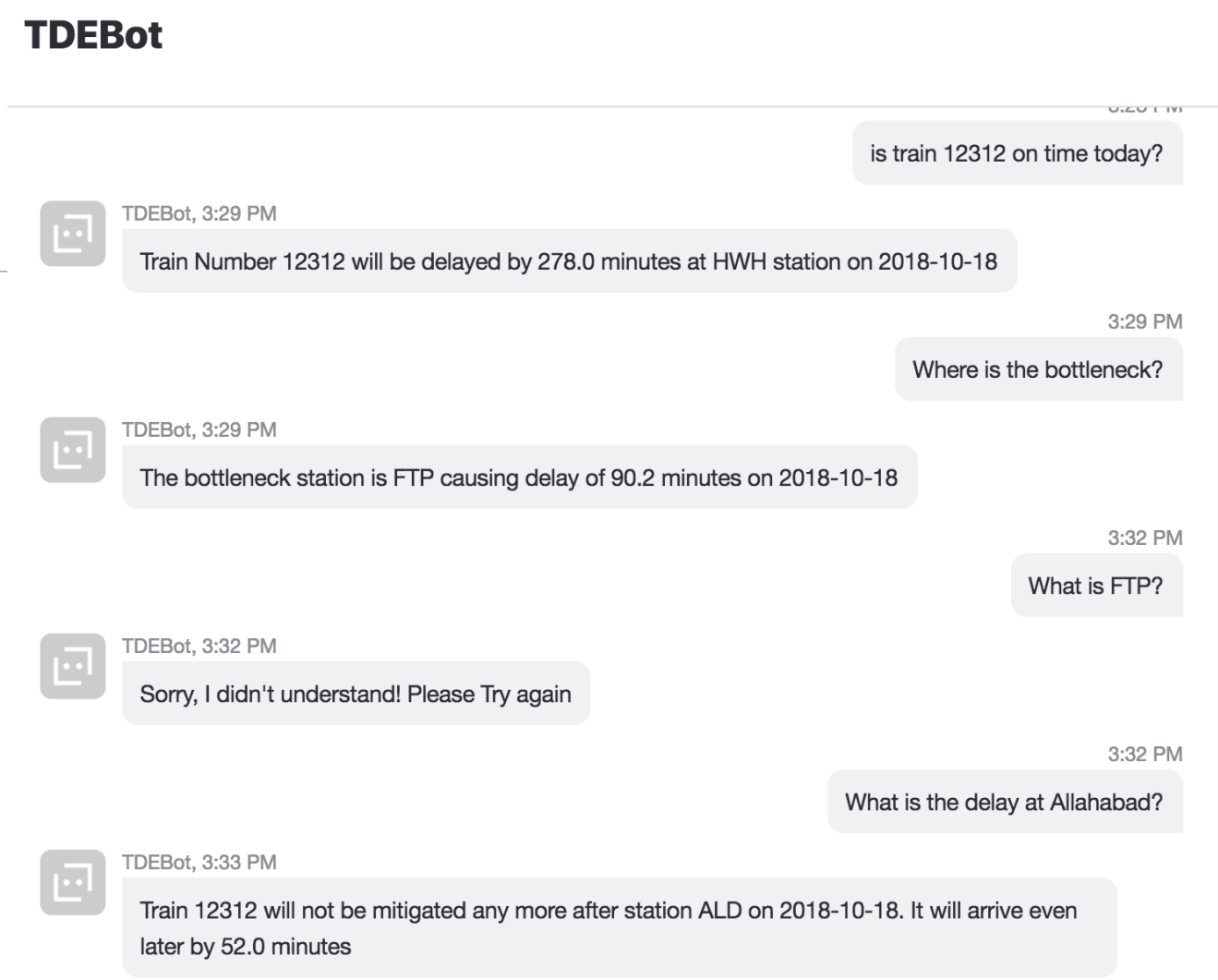
Impact of Chatbots: Creativity

- Blog: https://theconversation.com/asking-chatgpt-vs-googling-can-ai-chatbots-boost-human-creativity-242584
  - Paper: https://www.nature.com/articles/s41562-024-01953-1, 2024
- Method
  - Five experiments, asking participants to use ChatGPT (GPT-3.5) to generate creative ideas for **- choosing a creative gift for a teenager, making a toy, repurposing unused items and designing an innovative dining table**.
  - External judges, unaware of the participants' assigned instructions, rated each idea for creativity. Averaged the judges' scores to provide an overall creativity rating.
- Found that
  - ChatGPT increased the creativity of the generated ideas compared with
    - Humans not using any technology or
    - Humans using a conventional Web search (Google).
  - ChatGPT doesn't generate truly novel ideas; but leveraging (e.g., combinations across) existing ideas

Illustration: A Seemingly Innocuous Chatbot

Potential Issues

- Leak information
- Abusive language
- Complex response



References:
1.Ramashish Gaurav, Biplav Srivastava, Estimating Train Delays in a Large Rail Network Using a Zero Shot Markov Model, IEEE International Conference on Intelligent Transportation Systems (ITSC). On Arxiv at: https://arxiv.org/abs/1806.02825, June 2018 [Train delay, prediction]
2.Himadri Mishra, Ramashish Gaurav, Biplav Srivastava, Train Status Assistant for Indian Railways, On Arxiv at: https://arxiv.org/abs/1809.08509, Sep 2018, Video: https://www.youtube.com/watch?v=a-ABv29H6XU [Chatbot, Train delay assistant]

Lecture 24: Concluding Comments

- Different types of chatbots
- Potential for using them
- Different ways of building them
  - Rule based methods
  - (Deep) learning based methods
- Applications
- Ethical Issues

Concluding Segment

Course Project

Discussion: Course Project

Theme: Analyze quality of official information available for elections in 2024 [in a state]

- Take information available from
  - Official site: State Election Commissions
  - Respected non-profits: League of Women Voters
- Analyze information
  - State-level: Analyze quality of questions, answers, answers-to-questions
  - Comparatively: above along all states (being done by students)
- Benchmark and report
  - Compare analysis with LLM
  - Prepare report

- Process and analyze using NLP
  - Extract entities
  - Assess quality – metrics
    - Content – *Englishness*
    - Content – *Domain* -- election
  - … other NLP tasks
  - Analyze and communicate overall

Major dates for project check

- Sep 10: written – project outline
- Oct 8: in class
- Oct 31: in class // LLM
- Dec 5: in class // Comparative

Obtaining Election Data

Here are a few things to do:
A) **Official data** backed by laws: state election commission
a) Find the state's election commission
b) Find the Q/As they provide. They may be as FAQs or on different web pages.
c) Collect the Q/A programmatically

B) **Secondary data** sources: non-profit
a) Find Q/As from Vote 411 which is supported by the non-profit: LWV.

For reference, for SC,
A) Official - https://scvotes.gov/voters/voter-faq/
B) Secondary - https://www.vote411.org/south-carolina

For extraction, one or more approaches:
- Manually annotating
- BeautifulSoup,
- Tika
- or other open source libraries.

Election Q/A for Your State

- Format in .json; name file as "**xy**_qa.json", where xy is the two-character US state acronym
- Fixed attributes in .json
  - state: xy
  - num_questions: **a**, where a is the number of questions
  - num_answers: **b**, where b is the number of answers
  - contributor: student name
- questions: List of Q/As with attributes for each it:
  - q // question
  - a // answer
  - s // source url from where the information is taken
  - t // time when the information is taken – UTC format
- Store it in your github repo; put in sub-dir like "project/data"
- Instructor will keep it in common place inside course github repo and share.

Election Q/As for Multiple States

- Instructor will keep it common place inside course github repo and share.
- You will be able to access Q/As of all states from common location
  - To compare data across all states

Discussion

- How will you use a LLMs for election data analysis ?
- When and Why? (conversely, not)

Project Report Guidelines

- Use template of ACM Computing Surveys – Latex or Word - https://www.acm.org/publications/authors/submissions
- Consider your report as a paper. Sections to have will be similar
  - Abstract: 1-line each on what, how, result // Optional
  - Introduction: motivation for the work // Optional
  - **Problem** // Clearly state input and output
  - **Related Work** // What are closely related work?
  - **Approach** // How does your solution/ code work?
  - **Evaluation** // How is the result better than a baseline? What better could have been done ?
  - **Discussion** // About results, what more could be done, anything else interesting
  - **Conclusion** // Optional
  - **References**

About Next Lecture – Lecture 25

Lecture 25 Outline

- Ethical Issues with computer processing of natural languages
- Stateless services – translators, sentiment, …
- Stateful services – chatbots
- Mitigation methods

18	Oct 22 (Tu)	Entity extraction, linking
19	Oct 24 (Th)	Events extraction, spatio-temporal analysis
20	Oct 29 (Tu)	Topic Analysis
21	Oct 31 (Th)	PROJ REVIEW
	Nov 5 (Tu)	
22	Nov 7 (Th)	NLP Task: Sentiment
23	Nov 12 (Tu)	NLP Task: Summarization
24	Nov 14 (Th)	Conversation Agents
25	Nov 19 (Tu)	Ethical Concerns with NLP, Trusted AI and Societal Impact
26	Nov 21 (Th)	Working with LLMs for NLP Tasks - programming, Quiz