WEBVTT

1

00:00:21.050 --> 00:00:21.515

Jisun An: Fine.

2

00:00:41.460 --> 00:00:44.620

Jisun An: Alright let's start.

3

00:00:45.060 --> 00:00:47.150

Jisun An: Thanks for joining today.

4

00:00:47.290 --> 00:00:51.910

Jisun An: Please pass code. Is memory. Please mark your attendance.

5

00:00:52.420 --> 00:00:55.860

Jisun An: I I wonder whether the spring will ever come.

6

00:00:56.921 --> 00:01:01.890

Jisun An: Hopefully, the weather gets better. Unfortunately, the weathercast doesn't say so.

7

00:01:02.200 --> 00:01:07.269

Jisun An: anyhow. So today's so we will continue the AI agent.

8

00:01:08.103 --> 00:01:09.410

Jisun An: Yeah. So

9

00:01:09.810 --> 00:01:23.970

Jisun An: same announcement, we have a practical assignment due by end of this week. Make sure that you are, and I changed the setting in the canvas. So now you should be able to submit the individual report. If there's any other issue, please let me know.

10

00:01:24.150 --> 00:01:29.539

Jisun An: And yeah, the exam. Next Thursday

11

00:01:29.930 --> 00:01:36.460

Jisun An: it will be around the 30 multiple choice questions. You may need to read a lot. So

12

00:01:37.170 --> 00:01:43.690

Jisun An: yeah, yeah, it covers from word representation to AI agent.

13

00:01:44.340 --> 00:01:48.729

Jisun An: And either. We close the book, we will use the canvas. Quiz.

14

00:01:50.034 --> 00:01:52.805

Jisun An: Yeah, more details coming up.

15

00:01:53.880 --> 00:01:56.720

Jisun An: on the day. But yeah, I think this is something.

16

00:01:57.970 --> 00:02:01.900

Jisun An: Any questions about p. 1 and the exam.

17

00:02:04.560 --> 00:02:05.320

Jisun An: Okay.

18

00:02:05.940 --> 00:02:11.550

Jisun An: Alright. Then let's move on right? So

19

00:02:13.070 --> 00:02:28.049

Jisun An: so we started with the think about how the AI agents can be applied in the real world, so how to be integrated into their system. And then, if you imagine, like a certain AI agents there it.

20

00:02:28.090 --> 00:02:48.630

Jisun An: I think what we have now and what you imagine. I think there are a lot big gap between the 2. So the day that you will see the actual AI agents that are true autonomy, that, like works by themselves, without any intervention, it will come in the very far, and we are in the progress, I think, to to get there.

21

00:02:49.060 --> 00:03:14.700

Jisun An: So the example that I'm sharing is the current status of the what we call as AI agents. And what we started was like ideal goal of the AI agent. So hopefully, in the next few years you will see more development. So I'm sorry that there are a bit of gaps between what we actually teach as a lecture versus what the AI agent actually should be. But I think just that's the ideal goal.

22

00:03:14.700 --> 00:03:21.629

Jisun An: And I'm just telling you different examples of different research that have been done on the AI agent.

23

00:03:22.410 --> 00:03:41.119

Jisun An: So, and at least I think people are trying to have a common sense of what is AI agents or Edm agents, and this is the conceptual framework that I find the most reasonable to me. So the AI agent or edit and base agents have these 3 different component brain perception and reactions.

24

00:03:41.240 --> 00:03:50.880

Jisun An: And so even the brain part is essentially is most important to be really autonomous, autonomous AI agents.

25

00:03:50.880 --> 00:04:12.609

Jisun An: And before the edit it was almost impossible. Right? Like usually these agents, they exist some agents, but they are basically run based on certain rules or based on the Rl. Algorithms. There were no way to actually think and act on it and etc. So Edm only made it possible to start of these rear AI agents that we are imagining now.

26

00:04:13.410 --> 00:04:38.590

Jisun An: So we start from this. And we talked about perceptions so like basically how they gather all the information about the external environment. And there could be different inputs like text input visual input, probably like the visual input include like images and the videos. And there could be audio inputs and maybe different senses of the environments like touch buildings and like taste

27

00:04:38.590 --> 00:04:46.640

Jisun An: smells or different environments, environmental senses like humidity, temperature, etc. So all this

28

00:04:47.440 --> 00:04:55.069

Jisun An: ways and sensors that enables to perceive the environment to be con, like part of this perception model.

29

00:04:55.210 --> 00:05:02.969

Jisun An: And the actions. There were 3 different actions that AI agents can do at the moment, which is the texture output.

30

00:05:03.000 --> 00:05:27.419

Jisun An: I mean, they can just talk. The Edm enables to do it. So we didn't talk much about it. The second one is the tool-based actions. So we talked about the tools and how they can actually implement this tool used in the and there are embodied actions. So these were the 3 different types of the actions. So I will finish up these two-based actions a little bit, and then I will move on to the brain, which is the major part of the AI based agent.

31

00:05:27.550 --> 00:05:39.609

Jisun An: But at the same time we actually already talked a lot about ability of the addms, and this brain part covers most of them. So I will just give you different examples and interesting papers that have been discussing about this issue.

32

00:05:40.734 --> 00:05:52.430

Jisun An: So the tool use. So we were here. The last slide was this one. So basically edit, them need to use the tools. And the simple way is, you can basically give

33

00:05:52.791 --> 00:06:16.619

Jisun An: like different tool tokens, which is tool tokens. And instead of predicting a the actual token. They, you can train the model to predict the tool tokens, so that whenever edit them face that particular tool tokens, then they can just execute a particular sort, that matching to that token. So that has been most common way to use the tools from the Edm. And then

34

00:06:17.090 --> 00:06:39.090

Jisun An: this tour former was, okay, there couldn't be many different tools. And why don't we just let edit them to learn what to use when? So what they did was they basically created a lot of data set looking like this. So they have some context. And then they have an input and output. And so when when they are in like generating these outputs like, they

35

00:06:39.280 --> 00:06:45.099

Jisun An: actually replaced the the true answer to, they replace it to a particular question.

36

00:06:45.140 --> 00:07:11.120

Jisun An: which is the actual tool use. So in this case the highlighted, the blue ones are they call the Qa Apis. So question and answer Api like search engines, and so, rather than they generate the token from their own model. They actually use the tool to fill this token. And the way that how they generate this data set is basically assuming that you have this one sentence with a particular answer.

37

00:07:11.120 --> 00:07:35.359

Jisun An: And so to fill that answer, they just had multiple potential Api calls. And here, basically, these are the Qas and different types of the questions. And then they just execute that Api course. And they found that which one actually get the correct answer. And then from that, they just generated a large amount of this data. So by replacing this actual widget as a tool.

38

00:07:35.360 --> 00:07:45.979

Jisun An: they just generate this big data. And then using this data, they train that again, and then they just the rest were the same as the other 2 edit thems are doing with the use of the tool.

39

00:07:46.870 --> 00:08:04.760

Jisun An: So in this way, basically, you don't need to give all the you don't need to give all the information when to use which tool, but basically, by doing so, they were able to match when for which token which tool actually was needed. So this was the way to learn for the tool. Use

40

00:08:05.435 --> 00:08:08.009

Jisun An: any questions about this particular.

41

00:08:09.030 --> 00:08:16.290

Jisun An: But okay, this morning update?

42

00:08:16.440 --> 00:08:24.840

Jisun An: Oh, no, it's just oh, oh, I I just added this this one slide, because just wanted to start from here. Yeah. But the rest are the same.

43

00:08:27.530 --> 00:08:46.649

Jisun An: Yeah. And then this one, I and also, you can also. Now, Openai also provide some way to define a function using the tools. And also you can send it all together. This tool information, together with the Gpt's user. Prompt.

44

00:08:46.680 --> 00:09:12.449

Jisun An: I mean, personally, I haven't used this. So I actually how I don't know how actually this working. But I mean, given that, it has a possibility that open AI also integrate with our different tools. I think there are, you can potentially use your own if you have your own kind of program to run, or particular Api calls that you can make, then you can define your own tool and then probably integrate that with that prompt.

45

00:09:12.520 --> 00:09:19.359

Jisun An: So I haven't explored it. But but I know that it's existence. So if you need it, this would be also a good option to use.

46

00:09:20.580 --> 00:09:37.299

Jisun An: Yeah. So this was the end of the tool. Use? So many of the actions are either done via this kind of Api course, which is tool use and even code generation. And everything is also pulled as a tool use. So it's also the broad term

47

00:09:37.677 --> 00:09:58.462

Jisun An: but I mean, obviously all the actions are done would be via either text generation or pulling this Apis. And the 3rd one is the embodied action. So now, assuming that these AI agents actually used for controlling for something else, then simply generating the text, how can we connect these 2? Right?

48

00:09:59.040 --> 00:10:18.489

Jisun An: so you can embodied action. You can imagine if the AI agent is there for controlling for the robots, or you build on like agents that are playing a game. So this particular game character is run by AI agents, and then they explore these open world games like Minecraft.

49

00:10:18.490 --> 00:10:35.890

Jisun An: and then they kind of do all the all like just playing these games. They just explore the world and see how what they are doing. So people haven't really interested in using a game as a platform to test the ability of the Edm agent

50

00:10:36.270 --> 00:10:59.410

Jisun An: and see what kind of actions they can actually do, and what are the goals that they can achieve, and to our certain extents, what are the extents that this can go right so human can probably do? Maybe all very, very complex things in the game. But then, can AI agents also can do so? And how? How can we make that make the agents to do more complex task. I think that has been a big question that people have been working on

51

00:10:59.660 --> 00:11:25.679

Jisun An: so and so. So I think games, actions which are now, this is different from like calling the Apis, even though these are like done with the code execution, it's still each of these actions are defined as a embodied action like thinking this as a person in the real world. And then we do different actions. And so these are kind of simulation of the real world version. So

52

00:11:25.990 --> 00:11:47.559

Jisun An: so this is the one type of the action that you can also think of. I will talk a little bit more about this game part later, but it's just yet the conceptual level. There are different actions of texture outputs and the tool use and the embodied action. So these are the 3 types of the action that currently the AI agents research has been working on.

53

00:11:48.560 --> 00:11:51.120

Jisun An: So I will move on to the brain.

54

00:11:52.060 --> 00:12:16.250

Jisun An: so the brain is the the core mechanism of the agents, and there are 5 different types of the operating mechanism. So you should be able to enable the agents to do like natural language interaction, it also should have like knowledge. It should have a reasoning and planning also have some memory, and also has need to have a transferability and generalizability.

55

00:12:16.560 --> 00:12:31.960

Jisun An: So so I think many of these concepts. We already talked because so if you see this these are like kind of criteria, and then the existence of the added M only possible to like fit all this, satisfy all these conditions.

56

00:12:32.650 --> 00:12:53.139

Jisun An: Natural linking interaction. So it should be. Agents should be able to do multi-tone interactive conversation, high quality, natural language, generation, and also have some intention and implication understanding. And I guess we now can agree that them can actually do all of the things, but I guess the intention and implication understanding has been challenging.

57

00:12:53.140 --> 00:13:04.479

Jisun An: But then, now, with the reasoning model, I think this also has been largely solved. So I think natural language interaction was almost done. Problem at this stage of as on as an Adm agents.

58

00:13:04.480 --> 00:13:25.360

Jisun An: and, secondly, the knowledge as well. Right? So Rrm. Is known to have a lot of knowledge so previously, before the reasoning models, I would say, we always say that Rrm. Has certain knowledge, but then they don't know how to think. But now I mean, there is a reasoning model. I think they also we kind of agree that Rrm also can think so. Knowledge, part, I think, is done

59

00:13:25.580 --> 00:13:48.959

Jisun An: has both linguistic knowledge, like grammars, obviously, and some common sense knowledge like like how the general word is working. And there has been a lot of extensive data set to test whether Edith actually has the common sense knowledge. There are different data set. People have been tested, and I think it is working relatively, performing very, very well on these kind of benchmark data sets.

60

00:13:48.960 --> 00:14:09.820

Jisun An: and also professional domain. Knowledge is like in different domains, programming, mathematics and medicines. Once again this has to used to be a challenging issues. But then, now I think over the advancement of the Rrm. I think we are pretty. We are at very close level of Edm. Is really working well even for this professional domains.

61

00:14:11.050 --> 00:14:29.059

Jisun An: some challenges would be I mean, obviously, because eventually the Edms are just trained models. So whatever information they are trained can be always outdated. And also there could be some hallucinations. So these are some challenges in keeping their knowledge. But we also talked about like way to

62

00:14:29.972 --> 00:14:35.610

Jisun An: basically, the rag has been one of the most go for options to tackle these issues.

63

00:14:36.630 --> 00:15:06.380

Jisun An: And the reasoning and planning we also like discussed about this a little bit. So basically the chain of thought and the chain of thought or self-consistency stuff. We find. These are all the methods, even though these are partial prompting methods. But they found that this prompting method was effective for them to lead to the reasoning. And now we also have a reasoning method based on these chain of thoughts inspired by this method. For the planning.

64

00:15:06.530 --> 00:15:19.530

Jisun An: There are 2 types of, I mean 2 steps of the planning. So plan, formulation and plan reflection. So the plan formulation is basically we we talked about like plan and solve a prompt where, if you have a larger task.

65

00:15:19.530 --> 00:15:42.770

Jisun An: then you need to like, think it through like, split them into small sub goals sub plans, and then tackle one by one like so problem. Decomposition is one way to do the plan formulation. And then, once you have a initial plan, then also you need to reflect them. Whether these plans are actually good, whether it's achievable or not. So you can do kind of giving some internal feedback on this mechanism, and then you can

66

00:15:42.850 --> 00:15:45.510

Jisun An: probably able to achieve the goal.

67

00:15:46.530 --> 00:15:54.599

Jisun An: So there was this particular study that are hinting at the reasonings. And these are

68

00:15:55.010 --> 00:16:19.719

Jisun An: some interesting idea. So I mean, it's 1 of the like. Quite insightful paper on on the reasoning part. So before going through this example, so so react is the combination of reasoning and act. So it's a short for react. So the idea was very simple. So can we make the editing to think or I mean.

69

00:16:20.140 --> 00:16:48.049

Jisun An: before doing any action, can we make the edit them to think before act. I think that was like the really like a simple idea. And if you think about how human would do any actions, then we actually think first, st and we act on it, and then we observe, and then, based on that observation, we rethink and then act, and then observing once again. So we are repeating this process right? So the react was the idea that can we just ask, edit them to do exactly the same thing?

70

00:16:48.690 --> 00:17:03.819

Jisun An: so so basically given a task that we are given edit, and we'll just think and then suggest certain action and then get some observation and then edit them things again, and then do the actions and etc. So they will just repeat this.

71

00:17:03.930 --> 00:17:17.930

Jisun An: So these were the actual 0 shot reactor prompt. So, for example, you are on agents that answer questions by using 2 actions like Search Google, search the curry and then finish. Return the answer.

72

00:17:18.460 --> 00:17:30.479

Jisun An: and then you your answer. So you now you're generate in the following format, where, like thoughts, what would be the analyze? Given the observations? And then what would be your actions?

73

00:17:31.100 --> 00:17:36.680

Jisun An: And then the question right? So I mean, this was very, very simple, prompt. But then

74

00:17:37.840 --> 00:17:46.770

Jisun An: they found that this was very effective in achieving and like beating many of the benchmark data set for planning scenarios.

75

00:17:47.850 --> 00:17:50.730

Jisun An: So, for example, this is one example of the react.

76

00:17:52.940 --> 00:17:58.377

Jisun An: So the question was, I think they were, they wanted to find a

77

00:17:59.790 --> 00:18:03.629

Jisun An: The the question was, I think, whether they can buy the

78

00:18:04.204 --> 00:18:13.600

Jisun An: if you have certain number of money, then, whether you can buy, or the apple and media and the Microsoft so, given that question, Adam, start to think.

79

00:18:13.600 --> 00:18:38.870

Jisun An: and then they need to find the current market capitalization. So they do search for those value. And then this was the result from the Google. And based on this observation, they think again, what would be the market cap for the company, and then add them together, and to add them, they were using some computation, and they were using just a search again, which I mean, if you just Google it, you can just get the computation. So it was the

80

00:18:39.462 --> 00:18:50.547

Jisun An: whether some of these 3 market cap would be enough with the 7 trillion dollars. The observation was basically computing. And so it is not almost good enough.

81

00:18:54.580 --> 00:18:55.840

Jisun An: so I, yeah.

82

00:18:59.170 --> 00:19:07.380

Jisun An: So the answer is now, like, you need an additional 600 billion dollars to be by to be able to buy all 3 companies.

83

00:19:07.380 --> 00:19:30.659

Jisun An: So yeah, so this was the basic idea of the react. And once again, even though this was a very, very simple idea, this was working far better than in compared with like standard or the cot, basically like less thing, step by step, or act, only without any thinking. So this was one of the 1st approach that how the agent should be looked like. So they should have.

84

00:19:31.095 --> 00:19:40.410

Jisun An: I mean, if they by having ability to think, which is the reasoning their action was basically getting much better. And they actually performed quite well.

85

00:19:44.668 --> 00:19:47.239

Jisun An: Yeah, any questions about the react?

86

00:19:52.960 --> 00:19:56.530

Jisun An: Yeah. The distribution. I know action is something like

87

00:19:56.670 --> 00:20:04.390

Jisun An: the model. Search the question, timeline. And what is the observation? Is the return from the search?

88

00:20:04.590 --> 00:20:07.429

Jisun An: Yep, in in this case? Yeah.

89

00:20:08.590 --> 00:20:37.499

Jisun An: But then so this was the only the example based on like web based, or this kind of like reasoning based test. But the react was also tested on finding, like new chemical composition for particular disease. And then they also found that react has working far better on those tests as well. So since it was appeared that this particular technique has been applied to different types of tests. And yeah, surprisingly, it has been working quite well.

90

00:20:38.210 --> 00:20:46.119

Jisun An: So still, even though it was only prompting based this was really resulting in a good performance.

91

00:20:47.212 --> 00:21:00.197

Jisun An: And then another way would be the global planning. So I think we had this paper before when we were talking about the prompt promptings so these are plan and sober prompting. So rather than just

92

00:21:00.530 --> 00:21:25.189

Jisun An: doing the cot, basically, we asked to. Let's 1st understand the problem and devise a plan to solve the problem and let's carry out the plan and solve the problem step by step. So, using this prompt, they were able to split a task into the smaller tests, and they were just so you can see in the in the below. Example is the plan and sober prompting, and they

93

00:21:25.240 --> 00:21:31.490

Jisun An: split the plan into multiple steps, and they are solving one by one. And this has been also effect effective.

94

00:21:32.050 --> 00:21:34.760

Jisun An: This is one way to plan things

95

00:21:35.320 --> 00:21:57.380

Jisun An: and since there were this like react or the planning, you may also need to. I mean, how about to have a better plan you probably need to check for the errors, and maybe reflect and just recover if there's any error. So this was the reflection is also another insightful very well known paper in this reasoning and planning area.

96

00:21:57.380 --> 00:22:20.890

Jisun An: Once again the idea was very simple, so like, rather than just simply thinking and act and observe, they just added this one additional steps, evaluation. So after you have tests and some trajectory of the action and observation, thought, action, and observation, you also evaluate internally, see whether whatever action they taken was actually correct or not.

97

00:22:20.920 --> 00:22:25.017

Jisun An: And if based on that, you just like change the plans

98

00:22:25.520 --> 00:22:54.421

Jisun An: and based on that reflection, you are doing the elections again. So once again, this sounds very easy, but there are always the 1st person who have done, and they also prove that the way that we actually do planning and the reasoning is also effective to the agents as well. And I think that's the like. The key and the interesting findings of these works. So whatever intuition that you may have like, why, you are working with the edit them, it probably it may actually work.

99

00:22:55.190 --> 00:22:57.100

Jisun An: So this was the reflection.

100

00:22:57.310 --> 00:23:18.480

Jisun An: and then and this was the the last one in this planning and the reasoning. So the co-act is some relatively new work. And here, now this one. So before all the other work was, we assume that there are single agents, and this one is now have a multi multiple agents. At least we have a at least 2

101

00:23:19.031 --> 00:23:42.900

Jisun An: And agents. So one is the global planner and the other is the local agent. So the global planner kind of plan everything. And basically they are splitting the task and give the task to the local agents. And now local agents like work, each sub tasks and and plan, and they also the local agents, has the way to get the feedbacks and evaluate.

102

00:23:42.900 --> 00:24:04.100

Jisun An: and the replant etc, and then they do each of the phase, and then they collect all the Richards and then get back to the Globe. So I haven't read this paper properly. I just know the concept. So if you are interested in like, check this paper as well. But I think there are now many research that are trying to

103

00:24:04.100 --> 00:24:29.849

Jisun An: adapt to the multi agent system in different problems, and that can have some pros and cons and and I will talk more about this multi agent thing later. But I think this was one of such a case, where, by introducing, separating as a like global planable managing across the entire task and having an agent that is focusing on one particular specific task. This has been also improved. The performance on overall

104

00:24:29.990 --> 00:24:31.959

Jisun An: and the reasoning and the planning tasks.

105

00:24:33.610 --> 00:24:48.390

Jisun An: Yeah, yeah, I mean, I don't know. These are interesting papers. So I think some of your teams are also interested in building a AI agent. So all this, some of this work may be helpful for dig deeper and see how they actually implemented all this.

106

00:24:50.275 --> 00:24:57.040

Jisun An: So I will move. Oh, any any questions here, planning and the reasoning

107

00:24:59.380 --> 00:25:06.970

Jisun An: right? So now to the memory, memory is So

108

00:25:08.200 --> 00:25:27.450

Jisun An: so for an agent to to act or react properly, they need to have a memory which is basically stores all the past observations and for test behaviors. So this could help to ensure proficiency handling of a sequence of the consecutive tests.

109

00:25:27.730 --> 00:25:53.329

Jisun An: and also revisit and apply same strategies when face the complex problem. I mean once again, these are the reason that why we have a memory. Right? So I think really many approaches that people have been attempting with the Edith agents is how human works so, having, like, we have, like long term, memory, short term, memory. So there has been different ideas. How to implement this with the Edith agents, and I will

110

00:25:54.080 --> 00:25:56.469

Jisun An: talk on that

111

00:25:57.120 --> 00:26:05.200

Jisun An: but challenge. So there has been 2 particular challenges in developing, or let the edit them to have the memory. So

112

00:26:05.540 --> 00:26:14.750

Jisun An: 1st would be basically, it requires a method for better memory capability. And so

113

00:26:14.880 --> 00:26:16.962

Jisun An: I mean the edit M has, like

114

00:26:17.720 --> 00:26:27.840

Jisun An: context length so, even though for a prompt, there are particular limited length of context that you can provide. So

115

00:26:27.940 --> 00:26:28.880

Jisun An: if

116

00:26:28.930 --> 00:26:38.820

Jisun An: the easy way or the good way would be. If Editor just has a larger context window. Then you can provide more input and that can solve a few problems.

117

00:26:38.820 --> 00:27:03.780

Jisun An: So there has been this long context transformers which we haven't talked much about it. But it has been just one of the efforts that are trying to make this memory capability be better. And another way to have this is now summarizing the memory right? So even though so, the agents may not be able to remember everything, or maybe there would be only specific memory that actually needed is very important.

118

00:27:03.780 --> 00:27:11.279

Jisun An: So rather than keeping every all the memory they can just summarize and then just summarize. Remember, it would be enough for

119

00:27:11.750 --> 00:27:13.840

Jisun An: Consider the next actions.

120

00:27:14.850 --> 00:27:33.949

Jisun An: and also like using the rack or kind of external database also has been a way to go. Go ahead with this issue. So just compress the memories and changing it to the vectors or particular data structure, and then you just retrieve it whenever you need it. So this has been another way

121

00:27:34.310 --> 00:27:42.720

Jisun An: and those that there should be some method for memory retriever. And we've already talked about this retriever issues within the Reg. So

122

00:27:43.822 --> 00:27:57.418

Jisun An: but then here, because these memories are there for determining, I mean best. But what would be the best memory for determining the best actions? Right? So that was the question. So

123

00:27:57.990 --> 00:28:22.762

Jisun An: rather than simple, like similarity, retriever based there could. There has been some work that are developed a particular new metric called a memory score. And so because so what memory would be most useful for determining the next action, they thought there could be 3 different components of recency relevance, and the importance. So given these 3 values, they kind of

124

00:28:23.390 --> 00:28:47.009

Jisun An: simply did a weighted average of these 3 different components. And this so out of all the actions and experience that you had before using these 3 matrices, you extract the memory and then keep that as a prompt, I mean context in the prompt together, and that will kind of determine, modify the next actions, so that these are some of the things that have been done. In the memory space

125

00:28:48.433 --> 00:28:54.500

Jisun An: and I will introduce now a few cases in in the memory. So so this.

126

00:28:54.770 --> 00:29:18.770

Jisun An: this one basically argued that having a memory that are containing the workflow will help for the agents to get be better and performing on a particular issue. And here the test that they tested was based on the web arena that we talked about last week. So web arena was the the simulation environment for the web device web environments.

127

00:29:18.770 --> 00:29:45.030

Jisun An: So we have this a shopping website, and then the task was like, Can you check for the when my last order will be arrived? So given this query the agents needed to navigate different web pages, so go to like, click the account, click the orders and check the particular products, and they needed to see the arrival, dates and etc. So these were the task that they were tested on.

128

00:29:45.650 --> 00:30:14.280

Jisun An: And here this, basically the simple idea was, they now have this one particular memory where those workflow that needed to the success action will be stored in this memory. And I mean once again, it sounds very easy. But this, having this memory, and then using this as for the general. So they did this induction part where they try to find the

129

00:30:14.920 --> 00:30:29.447

Jisun An: the the like, the the high level workflow out of all this the actual workflow, and then they kept it in the memory, and that has been very useful for facilitating any new actions. So

130

00:30:30.230 --> 00:30:38.069

Jisun An: basically, if you remember successful workflow, then that just helps for the performing for many different tasks.

131

00:30:40.110 --> 00:30:47.947

Jisun An: and then so the memory is one part. But then, like, if you can just do something that

132

00:30:49.301 --> 00:30:53.069

Jisun An: I mean memory may not be the only

133

00:30:54.900 --> 00:31:19.749

Jisun An: So memory means that you are doing the same. I mean, if you have the memory, and if you follow the action based on your memory, then you will always do the same thing right. But then, if you think about the agents or our lives, the exploration is also the important, like finding the new path or doing different actions to explore the world. So for certain scenario the exploration is also very important. So there has been people have been. Think about, how

134

00:31:19.750 --> 00:31:29.059

Jisun An: can we make the model to explore the environment or to do some action that is not depending on your only the past experience, but something for

135

00:31:29.210 --> 00:31:38.779

Jisun An: the better explore the environment. So how can we let the model to have the curiosity was the some of the concerns that people also have been had.

136

00:31:38.780 --> 00:32:02.310

Jisun An: and traditionally, people have been using the reinforcement learning and having some particular reward function, where, if you just explore, not not doing the expected action. But if you are doing some action that is not expected to do, then you are having like higher reward. So the Ra used this kind of reward method to be able to let agents do the actions that is not expected to do

137

00:32:03.240 --> 00:32:17.150

Jisun An: so. The similar approach has been also applied in different work. So here this one particular ethic research called platform a bay. Good platform

138

00:32:17.680 --> 00:32:20.760

Jisun An: here. They had like

139

00:32:21.450 --> 00:32:45.179

Jisun An: they had Adam agents, and then Adam labelers. So these Adam agents are doing some actions. So if you have a particular environment, and there are like force of the actions that you can do. Then these agents were just doing some random sequence of the actions. And then these Adam labelers. They actually label that particular action, what that action lead it to?

140

00:32:45.782 --> 00:33:08.929

Jisun An: In natural language. And then and then they just repeat this. So basically, they are kind of generating the data like right, the sequence of the actions based on the atoms ability, and and see whether the instruction given that instruction, whether that particular action was the optimal or not. So they were evaluating that in the second stage.

141

00:33:09.400 --> 00:33:27.200

Jisun An: So in this way, right? So you don't need to like. Let Adam knows every possible actions to do every things in this platform. But Adam was able to explore all possible actions and click everything in the particular environment. And we're able to

142

00:33:27.572 --> 00:33:40.597

Jisun An: complete their task by their own. So this was one way to actually learn the agents to, I mean, enable the agents to learn about the environment automatically. So this was the one way by

143

00:33:41.120 --> 00:33:43.120

Jisun An: enforcing the exploration.

144

00:33:43.889 --> 00:34:08.820

Jisun An: And similarly, this voyager was also another way of like lifelong learning kind of idea of lifelong learning. So here they have an agents that are playing the Minecraft, and obviously Minecraft now has an even larger action space. Right? So you really cannot create a rules, or ask the agents to do all these different actions.

145

00:34:09.310 --> 00:34:29.300

Jisun An: So then, how can we enable the agents to learn to explore the Minecraft, and then play different games. And the way that they did was so they basically use the Gpt-four to so given a particular scene of the Minecraft game. So I mean, in a particular situation, you will see what resources you have

146

00:34:29.300 --> 00:34:56.920

Jisun An: currently and what environment you are facing. Right? So given. So you are giving this information to the Gpt. And the Gpt. Were generating this auto curriculum like. So what this Minecraft player can do? And then, so that answer which they coded as automatic curriculum was coming back to the agents, and that agents were actually executing it, and then see whether that execution was possible or not, and then and then they also, I mean

147

00:34:57.430 --> 00:35:18.569

Jisun An: so like, add all these actions to the memory, and they updating so whenever they were success subsetting in doing something. They add this, this skill library. So, using the combination of the skill library when given the environment, they can all like, gradually create like more complex tasks.

148

00:35:18.630 --> 00:35:31.120

Jisun An: And they were repeating this process so that the agents can gradually explore larger world and also doing more complex things within this Minecraft.

149

00:35:32.540 --> 00:35:48.689

Jisun An: So once again, this was the approach to enable the agents to explore the world, and also being more autonomous right by giving an ability to learn about the environment by themselves rather than rather than we are giving our rules or the way to act.

150

00:35:50.630 --> 00:36:01.280

Jisun An: yeah, any any questions on like I. I know it's a lot, and I'm just giving you a very high level information about it. But any any questions

151

00:36:06.740 --> 00:36:18.479

Jisun An: right? But pick big pick. So these are the games, and these are all. So the the actual action is actually run with a code.

152

00:36:18.670 --> 00:36:28.190

Jisun An: So you ask to create something. And then, if they were not able to create something that it will return the error. So these are, I mean, yeah, I mean, so basically you can.

153

00:36:29.640 --> 00:36:43.349

Jisun An: Oh, right? Right, I mean. So I I guess they may not be able to tell whether that something was more efficient or not. And and the feedback level of the feedback may not be as good as you wish to, but I mean the game. We're

154

00:36:43.820 --> 00:36:57.940

Jisun An: give you some feedback. Whether something was possible or not, at least, or maybe you cannot do it because you are lacking this particular resources. How many of them are lacking? So this kind of feedback is coming from the game itself.

155

00:36:58.170 --> 00:36:58.840

Jisun An: Yep.

156

00:37:04.770 --> 00:37:06.979

Jisun An: great any other question.

157

00:37:09.500 --> 00:37:14.660

Jisun An: Right? So I also want to introduce this work, which is

158

00:37:15.010 --> 00:37:19.291

Jisun An: one of the phenomenal work that I've seen in

159

00:37:20.120 --> 00:37:30.270

Jisun An: 2023. So these are now has everything like multi agents AI agents, multi agents and memories and behavior and everything. So.

160

00:37:31.455 --> 00:37:34.229

Jisun An: So this work is has

161

00:37:34.710 --> 00:37:53.249

Jisun An: right. After they had gpt 3.5, they imagined that this can be used to simulate a world that we are living or human behavior. So they built this small village. They call this a Smallville, and this is the also game kind of interface.

162

00:37:53.940 --> 00:38:11.980

Jisun An: And here they had the 25 different agent, and each of them had their own personas, so names and their like all all possible description, like their family relationship, their friends. Relationships what? What they are, work on, what is their personality and etc.

163

00:38:12.590 --> 00:38:22.110

Jisun An: So they are in this village. There are 25, these agents, and they stimulate, and then the base.

164

00:38:22.340 --> 00:38:30.054

Jisun An: the editing determines which actions each of these agents will actually do on each of the day. So, for example,

165

00:38:31.170 --> 00:38:55.319

Jisun An: And once again the profile include their all the relationship as well. So who they know and who they actually do not know. And and the simulation was going on, starting from the day, and so after the day started, a particular agents woke up. So all these informations were created in natural language, and also stored in a particular memory.

166

00:38:56.823 --> 00:38:58.150

Jisun An: And so

167

00:38:59.120 --> 00:39:24.326

Jisun An: so you can imagine these. Each agents are each agents, and they hold their actions are determined by the additive, and they want to see whether there are actual the human interaction happening. SIM, really, simply by these add items and they also tested. How the information actually spreads within this community as well. So as they start. So

168

00:39:25.060 --> 00:39:42.700

Jisun An: So they evaluate various things, so given that so each agent has their own personal, and each agent also has their own memory stream which I may have. Yeah, this is the architecture for individual agent. So the way that how they determine what action to do was.

169

00:39:42.700 --> 00:40:12.250

Jisun An: so they perceive, so they can perceive all possible things going on in the environment. So what happened to them or to them, and also to their neighbors like nearby. So these are the perceptions, so all these actions, them, their actions themselves, and also the other sections are going to this. Memory streams. All these experience are stored in the memory stream, and then, before they are taking action, they retrieve the some of the memories from this memory stream.

170

00:40:12.830 --> 00:40:23.972

Jisun An: and then based on those memories they act, and these retrieve memories also help to plan and also reflect, which I will talk a little bit later. So

171

00:40:24.780 --> 00:40:48.819

Jisun An: so basically they, I mean when they wake up. Then they would just go to wash their teeth or take a shower, eat something and go out. So so these agents were actually showing a very human like behaviors on like, based on their personas, and whenever they are meeting to each other, then they now start to talk to each other, and when they are talk to each other they also use these memory streams, and

172

00:40:48.820 --> 00:41:00.300

Jisun An: the recent and important memories, to decide what topics to talk to this particular person. It also determined by whether the person knows this person or not knowing this person.

173

00:41:00.850 --> 00:41:08.969

Jisun An: and but they so based on this architecture, they just did a 2 day simulations and see what kind of conversations were there among these 25 people.

174

00:41:09.640 --> 00:41:29.969

Jisun An: Oh, yeah. So once again. And then, in retrieving this memory, they found that these 3 value, the recency importance and the relevance are the most important. So to determine their next action, they for each of these experience, they had an important important score.

175

00:41:30.230 --> 00:41:38.709

Jisun An: and the recency was just like based on the time. And then they have the decay function. And the relevance was basically the similarity between the

176

00:41:39.060 --> 00:42:07.234

Jisun An: the query that they received versus the each of the sentences in the embedding space, the similarity between the 2 sentences. So by combining weighted some of these 3 vectors, they had a value for each of the experience, and they retrieve the memory that has a highest score. And they these memories went to the prompt together and given the whatever query that they had, and the prompt, the retrieve memory. The next conversation was

177

00:42:07.920 --> 00:42:28.400

Jisun An: during it. So in this case, like Isabella, has been thinking about having a valentine Valentine's party at her cafe. So, after considering all these factors, this was the given the question, What are you looking forward to the most right now, Isabella was asking. I mean answering to that

178

00:42:29.962 --> 00:42:59.540

Jisun An: and there was one extra. So once again, these memories, I mean, if you are looking at this memory stream. These are really like the details like, but so it is all about environment like. So desk is idle. Bed is idle, closet is idle refrigerator is idle. Isabella is stretching. So these are like all kind of experiments, experience. So they also had this reflection session, where basically they kept all the memory that is important. So they summarize, and they try to

179

00:42:59.540 --> 00:43:03.800

Jisun An: profile this particular person from the experience themselves.

180

00:43:04.200 --> 00:43:12.449

Jisun An: So these were collected also, and this reflection also be part of their memory stream as well. So this was the also one thing

181

00:43:12.790 --> 00:43:30.439

Jisun An: and the within this simulation. So what what they found is that these 25 agents were using the actions. And they analyzed the conversation between the agents. And they found that, yeah, there were I mean, basically, it really showed like a human like behavior.

182

00:43:30.440 --> 00:43:46.969

Jisun An: And they also did an end to end experiment, which is how the information actually diffuses. So as a simulation started. The Isabella was planning this Valentine Day party, and then they they kind of at the end of the simulation they observed, if

183

00:43:46.970 --> 00:44:07.370

Jisun An: who knows about this Valentine party, and then they basically found that some of them who's Isabel's friends. They were heard from Isabel directly, and then some of them also heard from others as well. So you can kind of see that this information also, like spreading through these the networks of these human.

184

00:44:08.010 --> 00:44:10.240

Jisun An: So this.

185

00:44:10.440 --> 00:44:28.309

Jisun An: Oh, yeah. So the Edm based agents has enabled to simulate the human behavior. And this was one of the 1st study that are trying to replicate or build these agents that are and and simulate how how they would actually behave. And it turns out it was quite human-like.

186

00:44:28.660 --> 00:44:37.120

Jisun An: It's a very interesting paper, and I highly recommend you to read any questions here.

187

00:44:40.370 --> 00:44:41.170

Jisun An: Okay.

188

00:44:41.993 --> 00:44:53.390

Jisun An: and then transportability and general liability is the last components of the brain. And this one is also we already talked about. Can the Rrm. Work for unseen tasks

189

00:44:53.998 --> 00:45:19.440

Jisun An: we talked about like the larger language model, had suddenly had this emergent ability where, even though they were instructed with a task, a certain type of set of tasks, they were also performing well on the test. That was not part of this instruction data. So T. 5 was the 1st model that were showing this emergent ability and being able to work better on the unseen tests.

190

00:45:19.840 --> 00:45:34.169

Jisun An: And the in-context learning is also another possibility for generalizing this work. So by simply rather than fine tuning the model by giving a few examples that, and also can do many of the work. And also there are many work

191

00:45:34.200 --> 00:45:55.330

Jisun An: that are trying to do this continual learning. The challenge. Here is the catastrophic forgetting. So catastrophe, catastrophic forgetting is basically if you train the model with a new set of tasks, then basically, the model is likely to forget, like whatever they learned before. So how can we prevent that is the

192

00:45:55.420 --> 00:46:06.179

Jisun An: a challenge. And I think one of the team working actually on this one. So I hope we can hear something interesting ideas on this at the end of the term.

193

00:46:06.470 --> 00:46:17.439

Jisun An: So yeah, I also do not exactly know. What's the particular solution for that. But this is a challenge. And I think there are many people working on on that.

194

00:46:18.750 --> 00:46:34.760

Jisun An: Then, yeah, so these were 3 components. Once again, brain perception, and the actions and various efforts in different domains. On these add images. I know that it may feel like these are like all of the sudden different examples, but

195

00:46:34.820 --> 00:46:50.870

Jisun An: it is the reality, I think, at the moment. Edit images is a term that is hot and used by many different in different subdomains. But hopefully, in in the near future there will be more common sense out of this.

196

00:46:51.209 --> 00:47:05.139

Jisun An: Agents and the more clear kind of taxonomy or the categorization of these agents. But I think these all are interesting, and each of them have some learning points. So I wanted to just introduce all these these work

197

00:47:06.310 --> 00:47:15.770

Jisun An: right? So I have just few more. right? So move on to types of the agent system. So

198

00:47:16.080 --> 00:47:26.189

Jisun An: if now that, assuming that we have an AI agents and there could be depending on their interaction types, we could have 3 different types of the agents, so single agents

199

00:47:26.190 --> 00:47:51.259

Jisun An: or the the system where there are multiple agents and they are communicating each other. Or we could have a system where the humans are interacting with the agents so single agents would be I mean the ones that we've seen. I mean, the Internet itself will be considered as a single agent as well, and also I don't know how many of you knows. But then the auto Gpt was introduced in 2023, I think anyone have heard or.

200

00:47:52.640 --> 00:48:19.250

Jisun An: yeah. So auto Gpt was something, use the Gpt to do a test. So basically, these were like a 1st demonstration of, can we use the simple prompting to do complete a more complex task. So rather than simple like question, and answering, this was the 1st demonstration to write a long, prompt, and see whether they can actually achieve a more complex course. So

201

00:48:20.420 --> 00:48:34.189

Jisun An: so auto gpt, but back then it looked like a quite magic. So you just enter one prompt. And then they collect all the information, and then they just did a job. And then these are extra the problems that people were

202

00:48:36.370 --> 00:48:40.999

Jisun An: So these were not exposed by the auto Gpt. But they I think they were just

203

00:48:41.330 --> 00:48:47.940

Jisun An: somehow compile this prompt and replicate what is it called like the

204

00:48:48.630 --> 00:48:53.860

Jisun An: did a back engineering. to get this prompt

205

00:48:55.046 --> 00:49:15.280

Jisun An: and yeah, so basically, they had the long prompt. These are full slides just for the one prompt. So they have a goal. Write a short story about the flowers, and then they have all these constraints like, because back then we didn't have the long context. So the memory. Given the memory, you should have only 4,000 word limit.

206

00:49:16.290 --> 00:49:33.609

Jisun An: and then there are a few tools that you can use. So these are like a different comment. And then also there are different resources. And then you can also how to evaluate the performance and how you should response, using this Json format.

207

00:49:34.910 --> 00:49:44.180

Jisun An: And then and then also they had like ensure. The response can be parsed by the Json dot load. So so this was like.

208

00:49:44.909 --> 00:50:03.799

Jisun An: one of the 1st example that are trying to create a like single agents, and then and then try to, rather than simple question and answering, just do a complete job. And what all the AI agents that we are seeing is like stemming from this, I think. Auto gpt.

209

00:50:04.570 --> 00:50:24.389

Jisun An: I don't know whether it's still running or not. But I guess now we have like other platforms that would be more useful. But this was something that started from, and then, like the react and reflection, these are all kind of considered as a single agents, that they can do their own like planning and reasoning.

210

00:50:25.340 --> 00:50:27.559

Jisun An: So the single agents

211

00:50:29.120 --> 00:50:40.560

Jisun An: they they can do actually a lot. And there are also researchers are trying to create like generalized general list of the agents. But then they may get lost in complex tests.

212

00:50:41.590 --> 00:50:47.490

Jisun An: So single agent would be still useful for small clear tests.

213

00:50:48.023 --> 00:50:55.870

Jisun An: And then maybe more complex things can be addressed with the human AI collaboration or the multi agent collaborations

214

00:50:56.520 --> 00:51:19.330

Jisun An: so human and AI agent system. This is a huge topic, especially in the Hci domain, and I have only one slide, but because I cannot really handle all of them, and there are a lot a lot of research about what is the best way to human collaborate with the Asian agents and ais, and I just cannot cover everything. But here are from the survey paper.

215

00:51:19.330 --> 00:51:29.620

Jisun An: These are like the 2 particular paradigm, whether the humans are like like playing a role as an instructor, and the agents, like working as an executor

216

00:51:29.840 --> 00:51:47.956

Jisun An: versus whether they have like equal partnership. So I think there are like 2 different paradigms, and they consider how the collaborations kind of we go but once again. These are really like a simplified version of it. There's like tons of new this is like particular research domain that I cannot cover in one

217

00:51:48.440 --> 00:51:49.340

Jisun An: lecture.

218

00:51:49.880 --> 00:52:03.179

Jisun An: So so just just know that there are existence of these human AI interactions. But I will probably like mostly skip it. I will focus more on the multi-agent system because it's, I think, more Nfp communities are more interested in

219

00:52:03.180 --> 00:52:26.870

Jisun An: and my personally also interested in so multi agent system is. Now, we already have seen some examples like the voyagers or the correct not actually had a 2 agents, and the social simulation already had, like 25 different agents. So if we have a system that has a multi agents interacting with each other, so how can we make a multi agent system. Better

220

00:52:27.460 --> 00:52:56.600

Jisun An: so, why do we need a multi agent systems? Maybe by having being able to have multiple agents, we may define different problem structures. And also it may provide a right knowledge at the right time. And also you, you can like switch between, edit them at like, based on their requirements. And also you may be able to provide the security or safety so certain edit them can access to certain Dv. And certain may not

221

00:52:57.170 --> 00:53:07.070

Jisun An: And also, maybe you should you. You'll be able to like, simulate human instructions. The one example that I showed the small building example. You see that particular example.

222

00:53:07.400 --> 00:53:14.789

Jisun An: So I will also share a few research papers about what has been done in this multi agent system.

223

00:53:16.930 --> 00:53:18.759

Jisun An: and the or these are

224

00:53:19.100 --> 00:53:35.229

Jisun An: for either visiting or for like web arena. So these are based on all the like texture, input on the web. But I assume that in the future we will see more examples of the embodied actions, and how the multi multi agent system will be integrated into it.

225

00:53:36.050 --> 00:53:58.439

Jisun An: So here this is one of the 1st paper dealing with the multi agents. And the idea is basically they inspired by the idea of the society of mind. So rather than thinking individually. If we just combine the ideas, then maybe it will better lead to better decisions.

226

00:53:59.130 --> 00:54:18.468

Jisun An: So like what they did was very simple. So if they have all 2 different agents then given the same. Given a particular query in the 1st round, both agents are just giving the answer, and then they combine this so in this particular platform they just share the other agents.

227

00:54:18.840 --> 00:54:34.270

Jisun An: answers to the as a part of the prompt for the second round. So basically, in the second round, they will have. They will get the answers from the other agents, and then, based on that, they will think about whether their answer is correct or not.

228

00:54:34.970 --> 00:55:01.539

Jisun An: and then they just repeat this like few rounds. So in this particular example, they did a 3 different round and then the expected scenario was, and then, at the end of the round, they just simply take the majority voting of their answers out of these agents, and then they get the answer, and they evaluate the performance on different regionally benchmark data set. So the example here shows that basically the 1st agent

229

00:55:01.920 --> 00:55:08.380

Jisun An: they did not have the correct answers, but then, having by by knowing the other agents,

230

00:55:08.890 --> 00:55:29.890

Jisun An: answers, it helped to correct their answers and then eventually they got it correct. And this actually helped a lot, and they showed there's some performance improvement in there. So you can see that when there are different agents, and there could be different way to how to make them interact with each other. And this was one of the simplest way to start with

231

00:55:30.860 --> 00:55:41.919

Jisun An: the next study. I think this one is more popular discord. As a I mean, the name is literally the same multi-asian debate, but now they call them as a Med. So these are the med structure.

232

00:55:42.250 --> 00:56:06.639

Jisun An: and here they tackle this idea of the problem of the degeneration of the thoughts in the self-reflection. So the degeneration of thoughts is basically once added, them has determined their thoughts, then it is not easily change it. So it is not very easy to change their thoughts.

233

00:56:07.050 --> 00:56:28.340

Jisun An: So what it means is that even though the answer is wrong, once they answer to it, they were not going to change it. So this is the definition of the degeneration of thought. So they were thinking, maybe using the multi agent system actually can tackle this dot problem, and I think it actually quite makes sense

234

00:56:29.015 --> 00:56:44.790

Jisun An: so their idea when they had the 2 different agents then they initially enforce a 1 agents to say, like yes to a question, and the other agents to know to that particular question, and then debate to each other, and then get the final answers.

235

00:56:45.090 --> 00:57:14.530

Jisun An: So here's the the the the actual example, and not just. They have the 2 agents that are discussed each other. But then, so there are this consensus, I mean how to make the decision, the final decision. Right? So in the previous example, we simply took the majority voting. But in this case they had a separate edit them. So you see, edit them as a judge. So based on the debates between these 2 agents, the final judge were making the final decision on to the answer.

236

00:57:15.200 --> 00:57:25.000

Jisun An: So here, basically, you had 2 different agents that are the endure and the devils and they just mate to.

237

00:57:25.680 --> 00:57:31.427

Jisun An: So I think the structure wise is the same. So both agents were answered to the question, and then

238

00:57:31.860 --> 00:57:48.790

Jisun An: They were their answer to copy back to the others. I don't exactly remember whether it was a sequential conversation, whether it was like like mesh conversation. But it. The example looks like it was a sequential conversation, but

239

00:57:49.120 --> 00:57:54.654

Jisun An: what I read it was different from it. But anyhow, that was the basic idea of

240

00:57:55.180 --> 00:58:09.030

Jisun An: yes. So the interesting part here is basically you are enforcing it to to think certain way, so that within the system you have some diverse opinions, and that actually helps to eventually solve the problem.

241

00:58:10.777 --> 00:58:23.759

Jisun An: The 3rd application. So these are now structure, wise, more or less similar. But the reconcile has the little difference in my understanding, even though, after reading it.

242

00:58:23.810 --> 00:58:42.930

Jisun An: it was not very clear. What's the big difference here? But one definite difference was that the now each agent, when they are answering, they are giving the confidence themselves. So like. So they are like 40% confident in this answer, like 90 5% or 50%

243

00:58:43.360 --> 00:58:55.270

Jisun An: and then here they argue that they are using like the different models as on different agents. So rather than you have 3 different instance on the same model. Here they were using like 3 different

244

00:58:55.430 --> 00:59:09.519

Jisun An: edited models, but the 1st one actually also, it was only the framework, so they can also use different models. So I don't think that was the their contribution. But the obvious difference was that they asked confidence when the answering, and then

245

00:59:10.010 --> 00:59:24.580

Jisun An: so when so eventually, the communication is happening, as you're copying one's agents to the others right and and giving that response to the others, and they will just consider their action based on these. Their answers.

246

00:59:24.850 --> 00:59:44.230

Jisun An: And then the confidence was kind of help like, whether to what extent they should believe their answers or not. So so this reconcile also helped in now estimating how much I should incorporate the others opinion. So that was some new thing that this reconcile proposed.

247

00:59:47.260 --> 00:59:51.849

Jisun An: e, any questions about these 3?

248

00:59:55.670 --> 00:59:56.460

Jisun An: Hmm.

249

00:59:59.810 --> 01:00:01.129

Jisun An: they they did. Yeah.

250

01:00:02.420 --> 01:00:07.794

Jisun An: yeah, yeah, it's just I mean, big, big. So they wanted to discuss, based on those

251

01:00:08.370 --> 01:00:11.969

Jisun An: based on those response of the other models.

252

01:00:13.340 --> 01:00:33.130

Jisun An: no, no matter how the confident they are. Yeah, but but because they have a confidence value. They probably know that okay, this values is not as trustworthy as so so in the they are in. They are one of the example actually show that. So eventually the confident answers were able to convince the other 2, which was less confidence.

253

01:00:33.600 --> 01:00:42.850

Jisun An: But then, once again, the experiment was I think it's. It's not easy to hardly argue that this was convincing. But but that's that's what they

254

01:00:43.670 --> 01:00:44.410

Jisun An: yeah.

255

01:00:44.780 --> 01:00:56.130

Jisun An: But I think it's it's a it's a it makes sense right. The knowing, the confidence can tell how much I should adapt that answers incorporate, that when I'm generating my own answer.

256

01:01:01.750 --> 01:01:07.370

Jisun An: so in a way. This would be like weighted majority voting based on the confidence

257

01:01:08.372 --> 01:01:19.249

Jisun An: so that was the another one and the more recent system. Now they this one is the chain of agent. So.

258

01:01:19.420 --> 01:01:23.960

Jisun An: yeah, so this was

259

01:01:24.632 --> 01:01:39.534

Jisun An: so this, this tackles a slightly different problem, and they tackles the long question, if I understand correctly. So what they found is that when? If so, if this is not a like simple question and answer,

260

01:01:41.430 --> 01:01:54.433

Jisun An: even though it's a simple catch on. And answer problem, if the reasoning requires multiple steps, they found that the agents tend to lost in the middle so they basically

261

01:01:55.610 --> 01:02:02.740

Jisun An: try to split the oh

262

01:02:03.680 --> 01:02:12.099

Jisun An: the tests, and then using multiple agents and go like step by step and see whether that will improve the

263

01:02:12.540 --> 01:02:13.305

Jisun An: performance.

264

01:02:15.780 --> 01:02:39.179

Jisun An: But I should be really honest. I added this in the last minute, and I don't think I fully understand how they split the task. So I I thought the idea was interesting, because all the other work were doing more meshed communication, and this one using more like hierarchical or like one way direction

265

01:02:39.210 --> 01:02:50.487

Jisun An: communication. Thought that would be kind of interesting, but I don't know why I'm talking. It doesn't make much sense, so I'm sorry I leave it to you to read the paper if you're interested.

266

01:02:51.470 --> 01:02:59.390

Jisun An: yeah, I'm I'm sorry I I forgot to recheck the paper, so I cannot really explain it. Well, at the moment

267

01:02:59.910 --> 01:03:03.697

Jisun An: I'm sorry so I will move on.

268

01:03:04.340 --> 01:03:09.610

Jisun An: I think this was the last example. And here

269

01:03:10.212 --> 01:03:28.860

Jisun An: so now this was one of few paper that are working with the embodiedm agent. So the Minecraft, one voyagi, and this one, I think, is the only 2 that are trying to create agents that are learning different actions in the like game environment.

270

01:03:29.790 --> 01:03:54.570

Jisun An: And here they what they found is that when they, when there are multi agents, explore the space and do some work, they found that they have unnecessary messages. They just talk random things, even though they can just decide by themselves. They unnecessarily talk to the other agent, and then, just that this disrupt the other agents actions and that made just redundancy messages. And that's what they found.

271

01:03:54.570 --> 01:04:19.619

Jisun An: So what they did was they basically had the leaders. So they now use the structure of leader and the team members and the leader basically give all the action instructions to others. So basically, all the other team members report back to the leader so that leader can decide each agents what to do, where to look for, what to look for, and

272

01:04:19.870 --> 01:04:43.890

Jisun An: this has been helpful to reduce the redundant message. So I think the performance wise in it may not be increasing as much. But then they found that the communication efficiency was far better to have the leader in this kind of exploration in the multi agent system. So I think that was the interesting finding. So I brought that idea here.

273

01:04:44.850 --> 01:04:46.190

Jisun An: Oh, so

274

01:04:46.470 --> 01:05:12.868

Jisun An: and okay, we have few more, and this one I will. I will just quickly go through and if you're interested in that, you can just look into more. And this is also an interesting, and it was looking from more psychological perspective. So if you give a particular like personality to an agent, would it help to make decisions? Or I mean, they were not interested in like having better performance. But actually, they were interested in how they

275

01:05:13.480 --> 01:05:18.839

Jisun An: how they are actually interact with each other. So they have a 2 particular.

276

01:05:19.280 --> 01:05:43.260

Jisun An: There are many factors, but important thing is, they had 2 different agents which are over confident, overconfident versus easygoing. And so, and they they use like 3 different agents to talk to each other to solve one thing, and they see like. So they have, like different society, where all 3 agents are overconfident, or 3 are easy going, and in between the combination of the 2,

277

01:05:43.480 --> 01:05:49.369

Jisun An: and see actually what happened, and they go through this debate and reflections around each of the round

278

01:05:49.880 --> 01:05:53.879

Jisun An: and some. So there were. No.

279

01:05:54.330 --> 01:05:59.977

Jisun An: I don't remember which communication was the best. But one thing that I remember is that

280

01:06:00.820 --> 01:06:19.319

Jisun An: basically if if everyone's are easy going, then the consensus were faster, and if everyone's are like overconfident. Then consensus will never happen. I mean something that you expect from the human. It also happened in the human in the, in the among the AI agents.

281

01:06:19.610 --> 01:06:21.980

Jisun An: and also oh.

282

01:06:22.620 --> 01:06:43.719

Jisun An: the these traits were also lost in the middle of the conversation as well, so initially you are set as overcompetent. But then, while you are talking, you are also kind of persuaded, and then getting less overconfident, so yours. They also observe the changes of this property as well, so these were, I think, some of the interesting aspects of building this AI agents

283

01:06:45.190 --> 01:07:06.429

Jisun An: right? So so out of all these examples we can think of. If you in the future ever create multi agent team, then there could be different considerations. So there would be like individual attributes. So when you are building the agents. Whether you want to add any particular traits, like demographics or personalities, or roles, or the occupations.

284

01:07:06.610 --> 01:07:18.040

Jisun An: And then there are there could be like a team structure, whether it would be hierarchical or flat or hybrid. So this will determine who will communicate with whom? Who will interact with whom?

285

01:07:18.650 --> 01:07:26.224

Jisun An: And then, lastly, the 3rd component would be decision making process which I don't didn't talk much about it. But these are also something.

286

01:07:26.850 --> 01:07:50.830

Jisun An: so once you have all the responses from the agents, how you will make the final decision, whether it be Missouri voting, or whether you will have like a judge who will determine it, or whether you be based on the consensus, or whether you will like randomly select. So there could be different decision making process. So these are different components to think about, and maybe different combination of that would work better for building better multi agency

287

01:07:52.712 --> 01:08:17.189

Jisun An: and the auto gen is the one of the popular platform that I believe that people have been using. I mean, at least you can develop different agents and also the interaction communication patterns are supported by this this platform. So, yeah, if you are interested in this multi system agency, I think definitely, it's worth it to check this particular platform.

288

01:08:19.899 --> 01:08:22.510

Jisun An: Yeah, any questions up to here?

289

01:08:25.490 --> 01:08:32.334

Jisun An: I, yeah, I'm yeah. I I think I'm doing just lecturing today. But I hope some of these informations are useful.

290

01:08:32.899 --> 01:08:58.039

Jisun An: so last couple of things about the agent evaluation. And this is the area where it's the mostly lack of the research. And, in other words, this is the area that are most of the research are doing at the moment. I think someone is actually doing it, as we hasn't been published yet. So how can we actually evaluate these agents, or has been on very interesting, challenging questions?

291

01:08:58.760 --> 01:09:26.800

Jisun An: And obviously you can. I mean, if I mean, for every evaluation you could have some subjective evaluation like human can basically evaluate for each of the agents. Actions and behaviors. How appropriate they are. But then this will just cost a lot, and you can also have some discrimination based evaluation, whether whether the agents outputs are, how good they are in. Compare with the human outputs. This is also.

292

01:09:26.800 --> 01:09:34.830

Jisun An: and in particular, whether human actually can distinguish between the 2 outputs. And this is also called as a Turing test.

293

01:09:34.850 --> 01:09:35.680

Jisun An: But

294

01:09:36.170 --> 01:09:59.450

Jisun An: anything that are involving human is expensive and costly. So I think the researchers tend to go to focus on the automatic way to evaluate these agents. So some key criteria for evaluating these are these are the 4 key criteria, usefulness, social capability, value and ethics and evolvability.

295

01:09:59.870 --> 01:10:19.740

Jisun An: Usefulness is obviously given a particular task. Whether the agents were able to complete the task. It's relatively easier to evaluate right. But then these agents also, and also it depends on whether it's the multi agent system or human AI system. So for human AI system, maybe the social capability or the value

296

01:10:20.580 --> 01:10:39.527

Jisun An: social capability may be more important. Maybe among the multi agent system. This actually may not be important right, even though they are talking some alien language. Who cares right as long as they perform well. But these are, I think, in mind that any kind of AI agents that are potentially interact with us.

297

01:10:40.030 --> 01:10:55.069

Jisun An: social capability, whether they how, how well how, what kind of social behavior they are kind of showing whether they are willing to collaborate, whether they are willing to negotiate, whether they actually stick to their role, whether they keep their personal, etc.

298

01:10:55.360 --> 01:11:23.530

Jisun An: And then the value and the ethics. I mean, these are like something, some criteria across for all the items, and also whether they learn continuously, they can set the goals and adapt to the changing environment and etc. So these are some of the key criteria and accept the usefulness. All 3 are easily defined. So in the I hope that in the future there will be more work that are more better social grounded evaluation metrics is coming up.

299

01:11:24.380 --> 01:11:47.399

Jisun An: and these are some of the data set that have introduced, especially for this 1st one, the usefulness. So the agent bench. I mean, you can imagine this is similar to what we've seen in the web arena. So they define this different real world challenges. And then this has been used for benchmarking across different methods.

300

01:11:47.950 --> 01:11:56.745

Jisun An: It include, like, whether they can operate the ubuntu systems, how well they can extract the

301

01:11:58.230 --> 01:12:06.150

Jisun An: oh, yeah, extract the information from the database and like card games or

302

01:12:07.074 --> 01:12:15.555

Jisun An: like thinking puzzles, web shopping and web browsing. So these are similar to the web arena, and these were mainly

303

01:12:16.260 --> 01:12:18.010

Jisun An: targeting the single agents

304

01:12:18.370 --> 01:12:28.230

Jisun An: and then back. I mean, this was 2023, and since then I mean Gpt. 4, obviously had the best features, and you can see the performance differences.

305

01:12:29.410 --> 01:12:53.016

Jisun An: And then, recently, very recently, in 2025, this new paper about the Multi agent bench has just published. So once again, these are really the current research, the most up to date research going on. And they now try to create a benchmark data for multi agent system, and and this one also. I haven't read it till the end. So I need to look for it.

306

01:12:53.340 --> 01:13:05.380

Jisun An: But I guess just wanted to let you know that there are some ongoing research on creating different benchmark data set for this and many of the actual criterias evaluations are missing and lacking.

307

01:13:06.410 --> 01:13:10.800

Jisun An: I think this is the last slide. Any questions?

308

01:13:14.040 --> 01:13:22.740

Jisun An: Okay, so so so I decided to exclude the AI agent from the exam.

309

01:13:22.890 --> 01:13:52.149

Jisun An: So the exam will be until the Rec. Because I mean AI. Agent. I found that most of the thing actually we already talked about. And then these are just different examples in different applications. And and these are very lengthy and not very technical. So I think it may not be really worth it for a exam, so I will. It's this will not be covered by the exam, so the exam will be from the word representation to the Rec.

310

01:13:53.480 --> 01:14:01.799

Jisun An: Okay. If you have any other questions, please let me know, and I will see you next Tuesday. Yeah, thanks. A lot

311

01:14:02.150 --> 01:14:03.809

Jisun An: have a great weekend