Student's affirmation: I certify that I have neither taken help in completing this exam nor helped anyone else with this exam. I have never discussed this exam with anyone other than the instructor and TA.

(Signature) _____

Mandatory: Affirmation and signature on the first page; name on every page; submission as PDF.
If you make assumptions about any problem, state them, but be prepared to justify why they were necessary.

Problem	1	2	3	4	Total
Points:	34	25	15	26	100
Score:					

This exam has 4 problems, for a total of 100 points.

Throughout, I prefer that you think afresh but if you come across a source on which you base your answer, please be sure to cite it. (Some problems ask for a specific author or source.)

1. (34 points) Mark the following statements `true` or `false`. Provide a short explanation of about 10–20 words. You can and should provide a source where appropriate. Where the statement is about a paper, please specify the corroborating part of the paper (e.g., "Page 32, second para, lines 4–6").

   A. (According to Mark Granovetter) Heider's theory of *cognitive balance* provides a basis for triad closure of strong ties on grounds of the congruence that people expect between their feelings and those of their friends about others

   B. Kleinfeld makes the case that, despite the fame of the six degrees of separation studies by Travers and Milgram, these studies are not reliably replicated

   C. Ian McCulloh describes a study wherein subjects could be influenced to provide a description of something that they themselves didn't believe

   D. If you have a weak tie to someone, chances are high they have high betweenness centrality in the social network

   E. According to Law and von Ahn, to be repeatable, a human computation algorithm must be sequential

   F. In the ring-based construction defined by Watts and Strogatz, a graph constructed with $p = 0.5$ is more like a small-world graph than a (traditional, Erdős-Rényi) random graph

   G. Watts and Strogatz state that though a small-world network may differ a random network, the two types of network display the same ratio of characteristic path length and clustering coefficient

   H. Tversky and Kahneman define the representativeness bias as arising due to the retrievability of instances

   I. The outcome of the Linda problem tells us that people are pretty good reasoners because though they may order the bank teller options incorrectly, they got everything else right

   J. Under autonomy, if a message m_1 is causally prior to a message m_2, then if m_1 occurs, m_2 will eventually occur as well

   K. In designing a communication protocol, we would like to set up as many request-response pairs as we can to ensure that the various agents remain as closely in sync as possible

   L. A shortcoming of sequence diagrams is that they can convey greater certainty about what is specified than what is physically realizable

   M. A finite-state machine representation of a protocol provides clarity on the choices of the agents participating in the protocol that would lead to the protocol being completed

   N. An agent that participates in, i.e., plays a role in, a communication protocol has no choice but to comply with the expectations that other participants in the protocol have of it

O. The fundamental idea behind protocols is that given a safe and live protocol, agents who conform to the roles in the protocol are guaranteed to be able to interoperate

P. The third-price sealed-bid auction for the sale of a single item would be incentive compatible for buyers

Q. The third-price sealed-bid auction for the sale of a single item ensures efficiency

2. Consider an enterprise crowdsourcing setting wherein you seek to query the staff of an enterprise to determine whether and how much to bid on a large project. For specificity, assume the project is to build a healthcare IT system for Madagascar and it involves software development based on legal regulations and user needs, deployment, day-to-day operations, and maintenance in light of revised regulations.

   The idea would be obtain information from the staff and to aggregate it so as to make a decision based on the best of what the enterprise's knowledge is.

   (a) (5 points) Building on the discussions between Galton and those who responded to his articles (such as Hooker), describe one possible objection someone may raise (i.e., about the challenges or risk of error) to the results you may obtain from querying enterprise staff.

   Use about 30–50 words.

   (b) (10 points) From a reading of Tverksy & Kahneman's Heuristics and Biases paper, describe two possible ways in which enterprise staff may produce biased information.

   Use about 30–50 words per objection.

   (c) (10 points) Building on the debate between Tverksy & Kahneman and Gigerenzer, describe one possible rephrasing or reframing that would capture Gigerenzer's response to dealing with one of the previous biases (specify which one).

   Use about 30–100 words for this part.

3. This problem concerns Pareto optimality. A finite set of goods is initially allocated among participants Alice, Bob, and Charlie, each of whom has a nonzero valuation for possessing each possible subset of goods. The valuation is nondecreasing: a superset never has a lower valuation than a subset. Each participant has enough money to buy all the above goods, if need be.

   (a) (5 points) Does a Pareto optimal allocation of the goods necessarily exist? If not, explain why not. If so, explain how to find one. Use about 20–40 words.

   (b) (5 points) Suppose there is a case with two Pareto optimal allocations. Will these allocations necessarily have the same total valuation (summed over the participants)? Explain your answer in about 30 words.

   (c) (5 points) Suppose we happen to begin from a Pareto optimal allocation and another Pareto optimal allocation exists. Is it possible to go from the first allocation to the second in a way that is respectful of each participant's valuation? Explain your answer in about 30 words.

4. (26 points) The following protocol is based on the purchase setting that we have used before. This protocol seeks to achieve these important requirements:

   - It should be possible for the BUYER and SELLER to concurrently send *payment* and *goods*, respectively, to each other
   - It should be possible for the SELLER to send a *withdraw* message after sending *offer*. If a BUYER is cooperative in this regard, it will not send *pay* if it receives *withdraw* before sending *pay*. However, the protocol handles the case where the *pay* and *withdraw* messages may cross. Thus, the protocol provides a *refund* message: if the SELLER receives *pay* once *withdraw* has gone out, the SELLER may send *refund*.
   - This protocol (eventually) completes in any of the following cases:
     - when both *payment* and *goods* have been sent
     - when both *refund* and *pay* have been sent
     - when *withdraw* has been sent and *pay* has not been sent

Note that a message name can be repeated with different schemas. The message names are not involved in the causality and integrity constraints in BSPL so we could choose them arbitrarily. However, it is good practice to use the same names for messages that have the same meaning in the protocol. That is why we repeat *allDone* below, each time with a slightly different schema.

```
protocol OfferPayGoodsRefundWithdraw {
  roles Buyer, Seller
  parameters _____
  private _____

  Seller ↦ Buyer: offer [out ID, out item, out price]

  Buyer ↦ Seller: pay [in ID, in price, out pDone, _____]

  Seller ↦ Buyer: withdraw [in ID, _____, out rescind]

  Seller ↦ Buyer: goods [in ID, in item, _____, out gDone]

  Seller ↦ Buyer: refund [_____]

  Buyer ↦ Seller: allDone [in ID, _____]

  Buyer ↦ Seller: allDone [_____, out outcome]

  Buyer ↦ Seller: allDone [_____, out outcome]
}
```

The above protocol listing is a partial solution. Modify the above listing by inserting any necessary parameters and messages so that the resulting protocol satisfies the above requirements and in addition is *safe* and *live*.

If you like, you may use the verification tool to verify that your solution is safe and live. Here's a plain text version to facilitate editing: https://www.csc2.ncsu.edu/faculty/mpsingh/local/Social/f25/wrap/SocDAI-protocols/OfferPayGoodsRefundWithdraw-blanks.bspl

Therefore, your main effort will be in

- Ensuring it meets the requirements with minimal modifications
- Explaining that it meets the requirements
- Explaining why you need each modification

Please submit the entire protocol as your solution, highlighting the parts that you inserted or modified.