

CLAIMS

1. A computer-implemented method for performing counterfactual regret minimization (CFR) for strategy searching in strategic interaction between two or more parties by solving an imperfect information game (IIG), wherein the IIG represents resource allocation, cyber-attack prediction and/or prevention, and /or traffic routing, the method comprising:

identifying N1 possible actions of a first party in a first state of the first party;

sampling a possible action out of the N1 possible actions in the first state of the first party with a first sampling probability;

identifying N2 possible actions of the first party in a second state of the first party, wherein the first state of the first party is closer to a beginning state of the IIG representing resource allocation, cyber-attack prediction and/or prevention, and /or traffic routing than the second state of the first party;

sampling a possible action out of the N2 possible actions in the second state of the first party with a second sampling probability, wherein the first sampling probability is less than the second sampling probability; and

performing the CFR based on the possible action out of the N1 possible actions in the first state of the first party and the possible action out of the N2 possible actions in the second state of the first party.

2. The method of claim 1, wherein performing the CFR based on the possible action out of the N1 possible actions in the first state of the first party and the possible action out of the N2 possible actions in the second state of the first party comprises:

calculating a regret value of the possible action out of the N1 possible actions in the first state of the first party;

calculating a regret value of the possible action out of the N2 possible actions in the second state of the first party;

updating a first strategy of the first party in the first state based on the regret value of the possible action out of the N1 possible actions; and

updating a second strategy of the first party in the second state based on the regret value of the possible action out of the N2 possible actions.

3. The method of claim 1, further comprising:
sampling k_1 possible actions out of the N_1 possible actions in the first state of the first party, wherein each of the k_1 possible actions is sampled with the same first sampling probability; and

sampling k_2 possible actions out of the N_2 possible actions in the second state of the first party, wherein each of the k_2 possible actions is sampled with the same second sampling probability.

4. The method of claim 3, further comprising:
performing CFR based on the k_1 possible actions out of the N_1 possible actions in the first state of the first party and the k_2 possible actions out of the N_2 possible actions in the second state of the first party.

5. The method of claim 3, wherein the first sampling probability is k_1/N_1 , and the second sampling probability is k_2/N_2 .

6. The method of claim 3, wherein $2 \leq k_1 \leq N_1$ and $2 \leq k_2 \leq N_2$.

7. The method of claim 3, wherein $k_1 = k_2$.

8. The method of claim 1, further comprising:
identifying M_1 possible actions of a second party in a first state of the second party;
sampling a possible action out of the M_1 possible actions in the first state of the second party with a third sampling probability;

identifying M_2 possible actions of the second party in a second state of the second party, wherein the first state of the second party is closer to a beginning state of the IIG representing resource allocation, cyber-attack prediction and/or prevention, and /or traffic routing than the second state of the second party; and

sampling a possible action out of the M_2 possible actions in the second state of the first party with a fourth sampling probability, wherein the third sampling probability is less than the fourth sampling probability.

9. The method of claim 1, further comprising:

identifying M1 possible actions of a second party in a first state of the second party, wherein the first state of the first party is closer to a beginning state of the IIG representing resource allocation, cyber-attack prediction and/or prevention, and /or traffic routing than the first state of the second party; and

sampling a possible action out of the M1 possible actions in the first state of the second party with a third sampling probability, wherein the third sampling probability is larger than the first sampling probability.

10. The method of claim 1, wherein the first state of the first party comprises a history of information provided by a second party, and the N1 possible actions of the first party comprises N1 possible actions in response to the history of information provided by the second party for providing product-service recommendations to customers.

11. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations for a method for performing counterfactual regret minimization (CFR) for strategy searching in strategic interaction between two or more parties by solving an imperfect information game (IIG), wherein the IIG represents resource allocation, cyber-attack prediction and/or prevention, and /or traffic routing, the operations comprising:

identifying N1 possible actions of a first party in a first state of the first party;

sampling a possible action out of the N1 possible actions in the first state of the first party with a first sampling probability;

identifying N2 possible actions of the first party in a second state of the first party, wherein the first state of the first party is closer to a beginning state of the IIG representing resource allocation, cyber-attack prediction and/or prevention, and /or traffic routing than the second state of the first party;

sampling a possible action out of the N2 possible actions in the second state of the first party with a second sampling probability, wherein the first sampling probability is less than the second sampling probability; and

performing a counterfactual regret minimization (CFR) based on the possible action out of the N1 possible actions in the first state of the first party and the possible action out of the N2 possible actions in the second state of the first party.

12. The non-transitory, computer-readable medium of claim 11, wherein performing the CFR based on the possible action out of the N1 possible actions in the first state of the first party and the possible action out of the N2 possible actions in the second state of the first party comprises:

calculating a regret value of the possible action out of the N1 possible actions in the first state of the first party;

calculating a regret value of the possible action out of the N2 possible actions in the second state of the first party;

updating a first strategy of the first party in the first state based on the regret value of the possible action out of the N1 possible actions; and

updating a second strategy of the first party in the second state based on the regret value of the possible action out of the N2 possible actions.

13. The non-transitory, computer-readable medium of claim 11, the operations further comprising:

sampling k1 possible actions out of the N1 possible actions in the first state of the first party, wherein each of the k1 possible actions is sampled with the same first sampling probability; and

sampling k2 possible actions out of the N2 possible actions in the second state of the first party, wherein each of the k2 possible actions is sampled with the same second sampling probability.

14. The non-transitory, computer-readable medium of claim 13, the operations further comprising:

performing CFR based on the k1 possible actions out of the N1 possible actions in the first state of the first party and the k2 possible actions out of the N2 possible actions in the second state of the first party.

15. The non-transitory, computer-readable medium of claim 13, wherein the first sampling probability is k_1/N_1 , and the second sampling probability is k_2/N_2 .

16. The non-transitory, computer-readable medium of claim 13, wherein $2 \leq k_1 \leq N_1$ and $2 \leq k_2 \leq N_2$.

17. The non-transitory, computer-readable medium of claim 13, wherein $k_1 = k_2$.

18. The non-transitory, computer-readable medium of claim 11, the operations further comprising:

identifying M1 possible actions of a second party in a first state of the second party;

sampling a possible action out of the M1 possible actions in the first state of the second party with a third sampling probability;

identifying M2 possible actions of the second party in a second state of the second party, wherein the first state of the second party is closer to a beginning state of the IIG representing resource allocation, cyber-attack prediction and/or prevention, and /or traffic routing than the second state of the second party; and

sampling a possible action out of the M2 possible actions in the second state of the first party with a fourth sampling probability, wherein the third sampling probability is less than the fourth sampling probability.

19. The non-transitory, computer-readable medium of claim 11, the operations further comprising:

identifying M1 possible actions of a second party in a first state of the second party, wherein the first state of the first party is closer to a beginning state of the IIG representing resource allocation, cyber-attack prediction and/or prevention, and /or traffic routing than the first state of the second party; and

sampling a possible action out of the M1 possible actions in the first state of the second party with a third sampling probability, wherein the third sampling probability is larger than the first sampling probability.

20. The non-transitory, computer-readable medium of claim 11, wherein the first state of the first party comprises a history of information provided by a second party, and the N1 possible actions of the first party comprises N1 possible actions in response to the history of information provided by the second party for providing product-service recommendations to customers.

21. A computer-implemented system for performing counterfactual regret minimization (CFR) for strategy searching in strategic interaction between two or more parties by solving an imperfect information game (IIG), wherein the IIG represents resource allocation, cyber-attack prediction and/or prevention, and /or traffic routing, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

identifying N1 possible actions of a first party in a first state of the first party;

sampling a possible action out of the N1 possible actions in the first state of the first party with a first sampling probability;

identifying N2 possible actions of the first party in a second state of the first party, wherein the first state of the first party is closer to a beginning state of the IIG representing resource allocation, cyber-attack prediction and/or prevention, and /or traffic routing than the second state of the first party;

sampling a possible action out of the N2 possible actions in the second state of the first party with a second sampling probability, wherein the first sampling probability is less than the second sampling probability; and

performing a counterfactual regret minimization (CFR) based on the possible action out of the N1 possible actions in the first state of the first party and the possible action out of the N2 possible actions in the second state of the first party.

22. An apparatus for performing counterfactual regret minimization (CFR) for strategy searching in strategic interaction between two or more parties by solving an imperfect information game (IIG), wherein the IIG represents resource allocation, cyber-attack prediction and/or prevention, and /or traffic routing, comprising:

- a first identifying module for identifying N1 possible actions of a first party in a first state of the first party;

- a first sampling module for sampling a possible action out of the N1 possible actions in the first state of the first party with a first sampling probability;

- a second identifying module for identifying N2 possible actions of the first party in a second state of the first party, wherein the first state of the first party is closer to a beginning state of the IIG representing resource allocation, cyber-attack prediction and/or prevention, and /or traffic routing than the second state of the first party;

- a second sampling module for sampling a possible action out of the N2 possible actions in the second state of the first party with a second sampling probability, wherein the first sampling probability is less than the second sampling probability; and

- a processing module for performing the CFR based on the possible action out of the N1 possible actions in the first state of the first party and the possible action out of the N2 possible actions in the second state of the first party.