Finding Pareto-Optimal Frontier with Minimum Disclosure for Multi-Party Negotiations

Thesis Summary

Satish Kumar Sehgal
Indian Institute of Management Calcutta, 2005

Supervisor: Asim Kumar Pal

The concepts of multiple objective optimization, distributed computing and secure multi-party computation have been utilized to address the problem of finding pareto-optimal (***po***) frontier in a scenario requiring minimum disclosure of information among participating parties. The problem draws its inspiration from the domain of multi-party negotiation in general and e-negotiation in particular. The issue of availability of a mediator has been considered in formulating the algorithms. Both the cases of finite (discrete) and infinite (continuous) decision space have been attempted. In continuous decision space the parties are assumed to have linear and nonlinear (concave and nonconcave) value functions and constraints[†]. Trade-offs in communication and computation costs vis-à-vis information disclosure have been highlighted. New algorithms have been attempted for a few general problems in the in the area of cryptography and secure multi-party computation. These along with existing algorithms have been used to solve the privacy issues in finding po solutions.

Negotiation is an integral part of many human interactions. A desirable characteristic of the final agreement is its optimality (called *pareto-optimality*). Pareto-optimality of the solutions can be reached by first negotiating and finding an acceptable alternative and then applying the *method of improving directions*, in which the agents (i.e. parties) always move towards a better point[‡]. However, it has been observed that in most of the negotiations parties leave the joint gains on the table which could have been realized, even when they are informed about the joint gains (Raiffa, Richardson, & Metcalfe, 2002). Alternative to this procedure, agents first find the set of po points and then negotiate on them.

[†]The constraint set should be convex for linear and concave scenarios.
[‡]A point is better if it does not deteriorate the condition of any of the agents with at least one gaining.

The set of po points is called ***Pareto-Optimal Set or Pareto-Optimal Subset (POS)*** and the frontier formed by the points of the pareto-optimal set is called ***Pareto-Optimal Frontier (POF)***. The multi-objective literature refers to this as ***Non-Dominated Surface*** (Zeleny, 1982) and in database literature it is referred as ***Skyline*** (Kossmann, Ramsak, & Rost, 2002).

The thesis proposes algorithms for finding the pareto-optimal frontier in a variety of scenarios involving the characteristics of the objective functions and constraints which are 'private' to the participants. We assume that the parties have decided to find the po frontier first and then negotiate on that. We also assume the Partial Open Truthful Exchange (POTE) situations. The thesis explores a number of general algorithms in Secure Multiparty Computation too.

Building blocks : Negotiation can be viewed as Multiple Participant Multiple Criteria (MPMC) problem. Hipel, Radford, and Fang (1993) assert that Single Participant Multiple Criterion (SPMC) and Multiple Participant Single Criteria (MPSC) decision making can be treated in essentially the same way. They also state that in certain situations MPMC decision situations can be converted to MPSC. Thus, various techniques proposed in the literature of multiple criteria decision making can be used. This might be possible in the case where parties are ready to tell the complete truth i.e. Full, Open, Truthful Exchange (FOTE) (Raiffa et al., 2002), where the participants are willing to share the information with each other. This however would not be feasible especially in the case of negotiations where the amount of hostility is large and only Partial, Open, Truthful Exchange (POTE) (Raiffa et al., 2002) (i.e. complete truth is not told) can be assumed. Thus, the possible conversion of MPSC to SPMC is questionable and the existing algorithms in the multiobjective optimization cannot be used directly. These algorithms have to be adapted for the distributed scenario using distributed computing and secure multi-party computation.

Multiple Objective Optimization: Several techniques for finding the po points exist in multi-objective optimization. The techniques can be classified into no-preference methods, a posteriori methods, a priori methods and interactive methods (Miettinen, 1999). However, most of the methodologies assume the presence of a single agent with the multiple objectives. A multiple party scenario in this case is seen as a single agent having multiple objectives with complete disclosure of objective functions and constraints.

Finding po points in negotiation is different from the traditional multi-criteria optimization due to preservation of privacy of information, which necessitates the application of distributed computing concepts. In the thesis we adapt the

methodologies in the MCDM literature particularly the multi-objective simplex method and weighted criteria method to the negotiation scenario. We also derive from the works in the database literature on Skyline queries.

Secure Multi-party Computation (SMC): SMC is a method to compute *any* function on given inputs, in a distributed network where each participant holds one of the inputs, ensuring independence of the inputs, correctness of the computation, and that no more information is revealed to participants in the computation that can be computed from a coalition of participants' inputs and outputs (Goldwasser, 1997). The ideal solution to this problem would be to have a trusted center to which all the participants send their inputs and it calculates the output, however in the dissertation it is assumed that this is not possible. SMC employs techniques based on cryptography and stochastic uncertainty by introducing random noise, split, combination or permutation in data or in the computation procedure.

Distributed computing: Distributed computing algorithms enable the solution of a problem which is either inherently distributed or which is computed distributed to exploit the unused distributed computing power leading to faster solutions. With the advancement of computer network technologies as well as the concepts of cryptography the distributed computing techniques can be exploited very well to the requirements of remote accesses as well as for preserving the privacy of information. ***Agent based systems*** can be employed not only to adapt the algorithms developed in the thesis but also to develop more intelligent versions of algorithms where autonomous agents can take many decisions by themselves. Some existing distributed optimization algorithms have been extended to tackle the security issues confronted in this thesis. Since, the value functions are distributed the algorithms for separable problems especially can be employed (Heiskanen, 1999; Bertsekas & Tsitsiklis, 1989).

Problem scenarios : The following categories of pareto-optimization have been attempted in the thesis:

1. Discrete decision space: The decision space for each decision making agent (DMA), i.e. party, is finite consisting of elements which are known a priori.

2. Continuous decision space: Here value functions that each decision maker optimizes (maximizes) are categorized into:
   (a) Linear value functions (with linear constraints)
   (b) Nonlinear value function
      i. Concave value function
      ii. Nonconcave value function

Availability of mediator agent (MA) brings another dimension to the problem. The two cases possible are:

1. MA not available
2. MA available
   (a) Honest MA
   (b) Semi-honest MA
   (c) Malicious MA

We do not consider the case of Honest MA and Malicious MA. If an honest MA is available there is no need for any distributed and secure algorithm. All the DMAs can give their value functions and the constraints to the MA. The MA can find the po frontier and inform them. However, getting such an MA is difficult. The case of malicious MA is not considered as all the algorithms for semi-honest can be converted to an equivalent algorithm for the malicious model, i.e. macros can be introduced which force the parties to behave either in a semi-honest manner or be detected leading to abortion of algorithm (Goldreich, 1998).

For discrete decision space we first find the feasible set from the decision set of all the DMAs and then find the po set from this set. For both the subproblems the SMC techniques are used to reduce disclosure. Numerous algorithms in the ***vector optimization*** literature exists to find the po frontier where the DMAs have linear value functions. For this we solve the Phase-I (i.e. finding a feasible basis) of the linear multi-objective optimization or vector optimization algorithm (Simplex based method) (Steuer, 1986; Armand, 1993) using distributed computing algorithms and for the rest of the phases we plug the loop holes in the existing algorithm to impose restrictions on disclosure using SMC.

The continuous case comprises concave and nonconcave scenarios (for the maximization problem). ***Weighting method*** which operates in the ***value space*** is one of the most adopted method in multiple objective optimization for concave case. The distributed weighting method is modified to reduce disclosure. We also propose algorithms which operate in the ***decision space***. In addition we give alternative solutions for the ***method of improving directions***. For the nonconcave case we propose a geometrical solution which enables considerable reduction in the possible po region starting from the complete feasible space.

Algorithms in SMC: In the process we also come up with a few general algorithms for SMC for both discrete and continuous spaces which are utilized in various optimization

algorithms mentioned above. These general algorithms are for finding intersection of finite sets, multi-party comparison of a pair of alternatives, finding the minimum and finding the sum of a set of values.

In sum, the primary contribution of the thesis is in utilizing methodologies from diverse fields of multiple objective optimization, distributed computing, databases, secure multi-party computation and agent based systems, for finding the pareto-optimal frontier, with an application in the field of negotiations. Algorithms have been devised considering a wide range of scenarios.

Keywords : Multiple criteria decision making, Vector optimization, Multi-objective optimization, Simplex, Linear Programming, Nondominated solutions, Efficient frontier, Privacy preseving, Skyline, Secure multi-party computation, Cryptography, Network security, Information security, Multi-agent systems, Distributed computing, E-negotiation.

References

Armand, P. (1993). Finding all maximal efficient faces in multiobjective linear programming. *Mathematical Programming*, *61*, 357–375.

Bertsekas, D. P., & Tsitsiklis, J. N. (1989). *Parallel and distributed computation* (2 ed.). Prentice–Hall International Editions.

Goldreich, O. (1998). *Secure multi-party computation.* ((working draft) Version 1.1, `http://www.wisdom.weizmann.ac.il/~oded/pp.html`, accessed on 10 February 2004)

Goldwasser, S. (1997). Multi party computations: past and present. In *Sixteenth annual ACM symposium on principles of distributed computing* (pp. 1–6). ACM Press.

Heiskanen, P. (1999). Decentralized method for computing pareto solutions in multiparty negotiations. *European Journal of Operational Research*, *117*, 578–590.

Hipel, K. W., Radford, K. J., & Fang, L. (1993, July/August). Multiple participant-multiple criteria decision making. *IEEE Transactions on Systems, Man and Cybernetics*, *23*(4), 1184–1189.

Kossmann, D., Ramsak, F., & Rost, S. (2002). Shooting stars in the sky: An online algorithm for skyline queries. In *Twenty-eighth VLDB conference.* Hong Kong, China.

Miettinen, K. M. (1999). *Nonlinear multiobjective optimization.* Kluwer Academic Publishers.

Raiffa, H., Richardson, J., & Metcalfe, D. (2002). *Negotiation analysis: The science and art of collaborative decision making.* The Belknap Press of Harvard University Press.

Steuer, R. E. (1986). *Multiple criteria optimization: Theory, computation and application.* John Wliey & Sons, Inc.

Zeleny, M. (1982). *Multiple criteria decision making.* McGraw-Hill Book Company.