European Journal of Operational Research 254 (2016) 968–976

Contents lists available at ScienceDirect

European Journal of Operational Research

journal homepage: www.elsevier.com/locate/ejor

Decision Support

Approximate representation of the Pareto frontier in multiparty negotiations: Decentralized methods and privacy preservation☆

Youcheng Lou[a,b,*], Shouyang Wang[b]

[a] Department of Systems Engineering and Engineering Management, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong
[b] Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China

ARTICLE INFO

Article history:
Received 7 April 2014
Accepted 28 April 2016
Available online 6 May 2016

Keywords:
Multiparty negotiations
Decentralized methods
Privacy preservation
Pareto optimal solutions

ABSTRACT

Multiparty negotiations have drawn much research attention in recent years and an important problem is how to find a Pareto optimal solution or the entire Pareto frontier in a decentralized way. Privacy preservation is also important in negotiation analysis. The main aim of this paper is to find an approximate representation of the Pareto frontier in a decentralized manner and meanwhile, all parties' privacy can be effectively protected. In this paper, we propose a decentralized discrete-time algorithm based on a weight sum method and the well-known subgradient optimization algorithm, where a mediator works as a coordinator to help negotiators. The proposed algorithm is easily executable, and it only requires the mediator to compute a weighted average of the noisy estimates received from negotiators and negotiators to follow a subgradient optimization iteration at this weighted average. The proposed algorithm can generate an approximate Pareto optimal solution for one particular weight vector and an approximate representation of the Pareto frontier by varying appropriately weight vectors. The approximation error between the obtained approximate representation and the Pareto frontier can be controlled by the number of iterations and the step-size. Moreover, it also reveals that the proposed algorithm is privacy preserving as a result of the random disturbance technique and the weighted average scheme used in this algorithm.

1. Introduction

Negotiation analysis has drawn much research attention in last decades due to its wide applications in electronic commerce, artificial intelligence, economics and operations research. The development of powerful methods and decision tools for seeking Pareto optimal solutions (POSs) in negotiation analysis is interesting since the negotiators frequently fail to achieve efficient agreements in practice (Raiffa, 1982; Sebenius, 1992). This may be caused by the numerous issues to be negotiated over and the limited knowledge about the other negotiators' interests.

Many decentralized methods for computing POSs have been proposed in the literature (Ehtamo et al., 1999a; Ehtamo, Kettunen, & Hamalainen, 2001; Ehtamo, Verkama, & Hamalainen, 1999b; Heiskanen, 1999, 2001; Heiskanen, Ehtamo, & Hamalainen, 2001; Kitti & Ehtamo, 2007; Sehgal & Pal, 2005). A method is called decentralized if its use does not require the parties to know each others' value functions nor does any one outsider take the full knowledge of all the value functions. In decentralized Pareto-optimality seeking methods, typically an interactive procedure is designed between the negotiators and a mediator, who works as a neutral coordinator helping the negotiators to seek POSs.

Most of decentralized methods can be classified into two classes: constraint proposal methods (Ehtamo et al., 1999a; Ehtamo, Verkama, & Hamalainen, 1996; Heiskanen, 2001; Heiskanen et al., 2001; Kitti & Ehtamo, 2007; Teich, Wallenius, Wallenius, & Zionts, 1995; Verkama, Ehtamo, & Hamalainen, 1996) and improving direction methods (Ehtamo et al., 2001; Ehtamo et al., 1999b; Teich, Wallenius, Wallenius, & Zionts, 1996). The constraint proposal methods are based on the fact that under some mild convexity (concavity) assumptions on the objective functions, there exists a joint tangent hyperplane for negotiators' indifference curves at a POS. In the execution process, the mediator adjusts

☆ The authors are very grateful to the anonymous referees and Prof. Slowinski – the editor of this journal for their very helpful comments and suggestions. This research was partially supported by The National Natural Science Foundation of China under Grant 71401163, China Postdoctoral Science Foundation under Grant 2014M550098, Hong Kong Research Grants Council under Grants 414513, 14204514 and Hong Kong Scholars Program under Grant XJ2015049.

* Corresponding author: Tel.: +(852) 3943-4075.
E-mail address: louyoucheng@amss.ac.cn (Y. Lou).

http://dx.doi.org/10.1016/j.ejor.2016.04.060
0377-2217/

a hyperplane going through a given reference point following a numerical iteration scheme until the negotiators' most preferred points on the hyperplane (the optimal solutions of some optimization problem) coincide. The final coincident point is a POS. By varying the reference point, the constraint proposal methods can generate an approximation for the Pareto frontier. Teich et al. (1995), Ehtamo et al. (1999a, 1996) and Kitti and Ehtamo (2007) consider the two-party case, while Verkama et al. (1996), Heiskanen et al. (2001) and Heiskanen (2001) discuss the more general multiparty case. In joint improvement methods, a joint improving direction is searched from a tentative agreement and a POS will be obtained if a joint improving direction can no longer be found. The authors in Ehtamo et al. (1999b) showed that the improving direction method will converge in a two-party case provided proper conditions hold, while the method was generalized to multiple-party multiple-issue case in Ehtamo et al. (2001). The authors in Teich et al. (1996) proposed serval heuristic methods for seeking joint improvements and some extensions of the proposed methods for approximating the Pareto frontier in a two-party resource allocation negotiations.

The authors in Heiskanen (1999) proposed a decentralized method based on weight sum and decomposition technique to generate all the POSs of the Pareto frontier in multiparty negotiations, where the scalarized objective is decomposed by introducing a decision variable for each party and then applying the dual decomposition technique. The decomposition results in a separable problem which is solved iteratively with each party solving its individual optimization problem, whereas the mediator updates the parameters of the optimization problems according to the optimal solutions received from the parties. When the parties' optimal solutions converge, the common optimal solution is guaranteed to be Pareto optimal. Moreover, decentralized methods have also been proposed to solve other interesting problems, for instance, cooperative optimization (Fulga, 2007; Nedić & Ozdaglar, 2009; Nedić, Ozdaglar, & Parrilo, 2010), online learning (Yan, Sundaram, Vishwanathan, & Qi, 2013) and eigenvector computation (Pathak & Raj, 2011).

Privacy preservation is an extremely important issue in negotiations. Negotiators desire to achieve an efficient agreement, but they are usually unwilling to disclose their private information to other negotiators because of some strategic reasons (Raiffa, 1982). However, most of the existing decentralized methods did not fully consider the privacy preservation problem. For instance, in constraint proposal methods and improving direction methods, the negotiators are required to report the optimal solutions of their own optimization problems to the mediator, or to answer the question which one of two available agreements they prefer to. These methods will lead to privacy disclosure inevitably in the sense that the mediator can infer some information about negotiators' objective functions based on the received information from negotiators.

In this paper, we consider the Pareto frontier approximate representation problem in multiparty negotiations. In our problem setup, we assume the negotiators can only exchange information with the mediator directly from the viewpoint of privacy preservation, and all parties including the mediator are semi-honest, that is, all parties follow the algorithm correctly but keep the record of all their computations. In this paper, we are interested in the following two problems: the first one is how to design an easily executable decentralized method to find an approximate representation of the Pareto frontier, and the second one is whether negotiators' privacy can be effectively protected during the algorithm execution.

Our proposed algorithm is discrete-time and based on a weight sum method and the well-known subgradient optimization algorithm. In each round of algorithm iteration, the negotiators first report their noisy estimates to the mediator and then the mediator takes a weighted average of all the estimates. Finally, the mediator reports this weighted value to negotiators and the negotiators update their estimates at the next step from the weighted average value along a negative subgradient direction. The proposed algorithm can generate an approximate POS for one particular weight vector with a geometric convergence rate and a discrete approximate representation of the Pareto frontier by systematically varying the weight vectors. The approximate error between the obtained approximation representation and the Pareto frontier can be characterized in terms of the system parameters such as the number of iterations and the (constant) step-size.

The proposed method is decentralized since it does not require any party to take the full knowledge of the multiparty negotiation problem. In fact, it only requires that each negotiator makes its own optimization iteration and the mediator computes the weighted average of the negotiators' estimates. Moreover, it is also privacy preserving observing that it can prevent the mediator from learning anything about negotiators' estimates due to the random disturbances in the transmitted estimates from negotiators to the mediator, and also prevent each negotiator from learning anything from other negotiators even though the received weighted average contains the information of other negotiators' estimates since all the negotiators do not know the weight taken by the mediator in the weighted average computation.

Compared with the constraint proposal methods and improving direction methods, our algorithm is easily executable and can save a lot of computations. In our algorithm, the negotiators are not required to report the optimal solutions of their own optimization problems and their most preferred points on constraint sets to the mediator, and only their estimates for POSs are required to be reported to the mediator. Compared with the methods in Yan et al. (2013), Nedić and Ozdaglar (2009), Nedić et al. (2010), Lou, Hong, Xie, Shi, and Johansson (2016) and Lou, Shi, Johansson, and Hong (2014), negotiators are not allowed to communicate with each other from the viewpoint of privacy preservation. Moreover, different from most of the existing algorithms, we fully consider the privacy preservation problem to avoid privacy disclosure because of the conflict of negotiators' interest.

The rest of this paper is organized as follows. The preliminaries on multiparty negotiation and problem formulation are presented in Section 2. A fully trusted decentralized POS generating algorithm and a modified privacy-preserving version are introduced in Section 3. Section 4 presents the proposed decentralized discrete approximate representation generating algorithm and the approximate error result. The numerical examples are given in Section 5. Some concluding remarks are given in Section 6.

2. Preliminaries and problem formulation

2.1. Preliminaries on multiparty negotiations

A multiparty negotiation problem (MNP) is usually described as

$$\begin{aligned} &\text{minimize} \;\; f(x) = \big(f_1(x), \ldots, f_n(x)\big) \\ &\text{subject to} \;\; x \in X_i, \; i = 1, \ldots, n. \end{aligned} \tag{1}$$

Here $n \geq 2$ is the number of negotiating parties; $X_i \subseteq \mathbb{R}^m$ and $f_i : \mathbb{R}^m \to \mathbb{R}$ are the closed convex constraint set and the convex value function of negotiator i, respectively, $i = 1, \ldots, n$; m is the number of negotiated issues. We assume throughout this paper that the constraint sets $X_i, i = 1, \ldots, n$ are bounded and have a nonempty intersection. The nonempty feasible set of MNP (1) is denoted as $X = \cap_{i=1}^{n} X_i$.

Let $\mathcal{X}_E$ denote the set of all Pareto optimal solutions (POSs) of MNP (1), i.e., $x^* \in \mathcal{X}_E$ if and only if $x^* \in X$, and there is no $x \in X$ such that $f_i(x) \leq f_i(x^*)$ for all i, and with strict inequality for at least one i. The set $\mathcal{X}_E$ is referred to as the Pareto frontier in the literature.

Let $\Delta_n = \{\omega | \omega = (\omega_1, \dots, \omega_n)', \omega_i \geq 0, \sum_{i=1}^n \omega_i = 1\}$ denote the unit simplex consisting of all nonnegative vectors with the sum of components equal to one, where $'$ denotes the transpose of a vector. The following lemma is important for the developed method to compute POSs, which is taken from Theorem 2 in Heiskanen (1999).

Lemma 2.1. *Suppose $f_i, i = 1, \dots, n$ are strictly convex. Then $x^* \in \mathcal{X}_E$ if and only if there is $\omega \in \Delta_n$ such that x^* is the (unique) optimal solution of optimization problem $\min_X \sum_{i=1}^n \omega_i f_i$.*

We know that each optimal solution of $\min_X \sum_{i=1}^n \omega_i f_i$ with positive vector $\omega \in \Delta_n$ ($\omega_i > 0$, $\forall i$) is properly Pareto optimal in the sense of Geoffrion (1968), and hence Pareto optimal. However, if the value functions are only convex (not necessarily strictly convex), the optimal solutions of $\min_X \sum_{i=1}^n \omega_i f_i$ for $\omega \in \Delta_n$ having zero as its component are only weakly Pareto optimal in general, and may be not Pareto optimal (referring to Ehrgott, 2000 for the definition of weak Pareto optimum).

Now we introduce a lemma about strongly convex functions. Let $|\cdot|$ denote the Euclidean norm of a vector. A function $\varphi(\cdot) : \mathbb{R}^m \to \mathbb{R}$ is said to be strongly convex on closed convex set K with parameter $\lambda > 0$, if for any $0 \leq \alpha \leq 1$, $\varphi(\alpha x + (1-\alpha)y) \leq \alpha\varphi(x) + (1-\alpha)\varphi(y) - \frac{1}{2}\lambda\alpha(1-\alpha)|x-y|^2$, $\forall x, y \in K$ or, equivalently,

$$\varphi(y) \geq \varphi(x) + \langle y - x, g \rangle + \frac{1}{2}\lambda |x - y|^2, \ \forall x, y \in K, \tag{2}$$

where $g \in \partial\varphi(x)$ with $\partial\varphi(x)$ denoting the set of all subgradients of φ at x. The following conclusion is important for the coming lemma and can be obtained from (2) by noticing that $0 \in \partial\varphi(x^*)$: for strongly convex function $\varphi(\cdot) : K \to \mathbb{R}$ with parameter $\lambda > 0$, we have

$$\varphi(z) \geq \varphi(z^*) + \frac{1}{2}\lambda |z - z^*|^2, \ \forall z \in K, \tag{3}$$

where z^* is the unique optimal solution of $\min_{z \in K}\varphi(z)$.

Define mapping $\hat{x} : \Delta_n \to \mathcal{X}_E$ with $\hat{x}(\omega)$ the unique optimal solution of $\min_X \sum_{i=1}^n \omega_i f_i$. Clearly, mapping $\hat{x}$ is surjective according to Lemma 2.1. The following lemma plays an important role in characterizing the approximate error between the generated discrete approximate representation and the Pareto frontier. Its proof is summarized in Appendix A.

Lemma 2.2. *Suppose $f_i, i = 1, \dots, n$ are strictly convex. Then*

(i) *Mapping $\hat{x}$ is continuous on Δ_n;*
(ii) *Furthermore, if f_i is strongly convex on X_i with parameter $\sigma_i > 0$, $i = 1, \dots, n$, then for $\omega^\ell = (\omega_1^\ell, \dots, \omega_n^\ell)' \in \Delta_n$, $\ell = 1, 2$,*

$$|\hat{x}(\omega^1) - \hat{x}(\omega^2)| \leq 2\sqrt{\frac{B\sum_{i=1}^n |\omega_i^1 - \omega_i^2|}{\sigma_{min}}},$$

where $B = \sup_{i, x \in X_i} f_i(x)$, $\sigma_{min} = \min_{1 \leq i \leq n} \sigma_i$, $L = \sup_{z \in \cup_{i, x \in X_i} \partial f_i(x)} |z|$.

Note that both B and L are finite numbers due to the boundedness of $X_i, i = 1, \dots, n$ and the continuity of convex functions $f_i, i = 1, \dots, n$. In the sequel of this paper, we assume that each value function f_i in the considered MNP (1) is strongly convex on X_i with parameter $\sigma_i > 0$, $i = 1, \dots, n$.

2.2. Problem formulation

We consider the multiparty negotiation problem (1), where n negotiators are negotiating over m continuous issues. The objective of the negotiators is to achieve an efficient agreement in POSs or the Pareto frontier. As the decentralized setting in the literature, there is a neutral mediator helping negotiators to find the desired agreement. Each negotiator i only knows its individual constraint set X_i, value function f_i, but does not know other constraint sets X_j and value functions f_j, $j \neq i$. Each negotiator is unwilling to disclose her/his private information to other negotiators and the mediator due to some strategic reasons. We make the following two assumptions for the parties in our problem setup.

- *In order to prevent the potential privacy disclosure, each negotiator is unwilling to communicate directly with other negotiators. Each negotiator is only willing to exchange information directly with the mediator.*
- *All negotiators and the mediator are semi-honest. A semi-honest agent follows the algorithm properly but it keeps a record of all its computations (Goldreich, 1998). All parties are assumed to follow the protocol correctly, but they may record and analyze the data obtained in the process of following the protocol in order to gain as much information as possible about other parties.*

Unlike the settings in Nedić and Ozdaglar (2009), Nedić et al. (2010), Lou et al. (2016) and Lou et al. (2014) for decentralized computation, here the negotiators are unwilling to communicate with each other to avoid the potential disclosure of private information. In fact, the first assumption has been widely used in the decentralized negotiation analysis, see Ehtamo et al. (1999a); Ehtamo et al. (2001, 1999b), Heiskanen et al. (2001), Teich et al. (1996), Heiskanen (1999); 2001) and Kitti and Ehtamo (2007). The second assumption on semi-honesty of parties has also appeared in the literature, which motivates the research on designing privacy preserving methods to accomplish various tasks, for instance, eigenvector computation (Pathak & Raj, 2011), belief propagation (Kearns, Tan, & Wortman, 2007), POS computation (Sehgal & Pal, 2005).

In this paper, we are concerned with the following problems:

- How to design an easily executable decentralized algorithm to find an approximate representation of the Pareto frontier? How to characterize the approximate error between the obtained approximate representation and the Pareto frontier?
- Is the designed decentralized algorithm privacy preserving in the sense that any party (including the negotiators and the mediator) cannot obtain other parties' private information based on the exchanged information in the negotiations?

For the first problem, in Sections 3 and 4 we will first introduce a discrete-time iterative decentralized algorithm to generate an approximate POS based on the well-known subgradient optimization algorithm for one particular weight vector and then an approximate representation generating algorithm to generate an approximate representation of the Pareto frontier by systematically varying the weight vectors in the unit simplex. The result shows that the approximate error between the obtained approximate representation and the Pareto frontier can be characterized by systems parameters. For the second problem, we give the positive answer and reveal that the designed algorithm is privacy preserving by employing a random disturbance technique.

3. An approximate Pareto optimal solution

In this section, we first introduce a fully trusted decentralized algorithm to generate an approximate POS, and then develop a modified version taking privacy preservation into account by introducing a random number in the exchanged estimates between the negotiators and the mediator.

3.1. A fully trusted decentralized algorithm

Raising from large-sized resource allocation in computer networks and the estimation in sensor networks, decentralized or

Algorithm 1 Decentralized Pareto optimal solution generating algorithm.

Input: The nonnegative weight vector $\omega = (\omega_1, \ldots, \omega_n)' \in \Delta_n$; number of iterations T; the constant step-size α; initial conditions $x_i^{\omega}(0) \in \mathbb{R}^m$, $i = 1, \ldots, n$.
Output: $\bar{x}^{\omega}(T)$.

The mediator delivers the step-size α to all negotiators.
for $k = 0 : T$ **do**
1: Each negotiator i transmits its current local estimate $x_i^{\omega}(k)$ to the mediator;
2: The mediator computes the weighted average $\bar{x}^{\omega}(k) := \sum_{i=1}^n \omega_i x_i^{\omega}(k)$ of negotiators' estimates and then reports $\bar{x}^{\omega}(k)$ to all negotiators;
3: **if** $k \le T - 1$
Each negotiator i updates its current estimate and uses

$$x_i^{\omega}(k+1) = P_{X_i}\left(\bar{x}^{\omega}(k) - \alpha g_i(k)\right) \tag{4}$$

as the estimate at the next step, where $g_i(k) \in \partial f_i(\bar{x}^{\omega}(k))$, $P_{X_i}(\cdot) : \mathbb{R}^m \to X_i$ denotes the convex projection operator onto closed convex set X_i.
else Each negotiator i gets $\bar{x}^{\omega}(T)$ as the final estimate.
end for

distributed optimization problems have been studied widely in the literature (Fulga, 2007; Lou et al., 2016; Lou et al., 2014; Nedić & Ozdaglar, 2009; Nedić et al., 2010). The main advantage of these algorithms compared with the conventional centralized ones is that they do not require any agent in the network knows other agents' value functions. Here is the proposed decentralized Pareto optimal solution generating algorithm (see Algorithm 1).

Here we first distinguish our algorithm with the existing decentralized POS generating algorithms in multiparty negotiations. In constraint proposal methods (Ehtamo et al., 1999a; Ehtamo et al., 1996; Heiskanen, 2001; Heiskanen et al., 2001; Kitti & Ehtamo, 2007; Teich et al., 1995; Verkama et al., 1996) and the methods in Heiskanen (1999) and Sehgal and Pal (2005), in each round of iteration the negotiators are required to exactly solve their own optimization problems. However, this will incur a lot of computations and the computation cost may be prohibitively high, especially for complicated objective functions. Instead of solving whole optimization problems, our algorithm is discrete-time iterated, relatively simple to execute and only the computations of weighted average and subgradient optimization are needed.

The discrete-time iterative Algorithm 1 is based on the well-known subgradient algorithm. In each iteration step, the negotiators first report their estimates to the mediator truthfully and then the mediator takes a weighted average of the received estimates. Finally, the mediator transmits this weighted average to all negotiators and negotiators update their estimates following a negative subgradient direction of their own value functions.

The following theorem establishes the relation between the generated estimates and the exact POS corresponding to the weight vector taken in the weighted average step in terms of the number of iterations T, the step-size α and some other system parameters. The proof is given in Appendix B. Recall that $\hat{x}(\omega)$ is the unique optimal solution of $\min_X \sum_{i=1}^n \omega_i f_i$, $\omega = (\omega_1, \ldots, \omega_n)' \in \Delta_n$.

Theorem 3.1. *Consider decentralized Pareto optimal solution generating Algorithm 1. Suppose the step-size α satisfies $0 < \alpha < 1/\sum_{i=1}^n \omega_i\sigma_i$. Then*

$$|\bar{x}^{\omega}(T) - \hat{x}(\omega)|^2 \le \left(1 - \alpha \sum_{i=1}^n \omega_i\sigma_i\right)^T |\bar{x}^{\omega}(0) - \hat{x}(\omega)|^2 + \frac{\alpha L^2}{\sum_{i=1}^n \omega_i\sigma_i}. \tag{5}$$

Theorem 3.1 shows that the average of agents' estimates will converge to the (unique) minimizer of the weighted sum value function $\sum_{i=1}^n \omega_i f_i$ at a geometric rate until reaching an error $\frac{\alpha L^2}{\sum_{i=1}^n \omega_i\sigma_i}$. Clearly, for any initial condition we can obtain an approximate POS by executing Algorithm 1 with sufficiently small step-size α and sufficiently large iteration number T. A surprising feature of Algorithm 1 is that the weight vector in the weighted sum value function (or the scalarized single objective) to be minimized is exactly the one taken in the weighted average step. This feature lays foundation for generating many POSs or a discrete approximate representation of the Pareto frontier by systematically varying the weight vectors in the unit simplex, as that developed in the next section.

A straightforward application of Theorem 3.1 gives

Corollary 3.1. *When*

$$0 < \alpha < \min\left\{\frac{1}{\sum_{i=1}^n \omega_i\sigma_i}, \frac{\varepsilon \sum_{i=1}^n \omega_i\sigma_i}{2L^2}\right\},$$
$$T \ge \frac{\ln \frac{\varepsilon}{2D}}{\ln\left(1 - \alpha \sum_{i=1}^n \omega_i\sigma_i\right)},$$

$|\bar{x}^{\omega}(T) - \hat{x}(\omega)| \le \varepsilon$. In fact, the above two conditions suffice to ensure both the two terms on the right-hand side of (5) not greater than $\varepsilon/2$, respectively. Here $D = \sup_{z \in \cup_i X_i} |\bar{x}^{\omega}(0) - z|^2$ is a finite number due to the boundedness of X_i, $i = 1, \ldots, n$.

3.2. A modified privacy preserving decentralized algorithm

Privacy preserving is an extremely important issue in negotiation analysis. Clearly, it is desirable that on one hand, the negotiators can achieve an efficient agreement, while on the other hand, their private information can be effectively protected in the interactions between the negotiators and the mediator. However, most of the existing decentralized algorithms did not consider the privacy preservation problem. In the improving direction methods (Ehtamo et al., 2001; Ehtamo et al., 1999b; Teich et al., 1996), the negotiators are required to answer the question which one of two available agreements they prefer to. In constraint proposal methods (Ehtamo et al., 1999a; Ehtamo et al., 1996; Heiskanen, 2001; Heiskanen et al., 2001; Kitti & Ehtamo, 2007; Teich et al., 1995; Verkama et al., 1996) and the method in Heiskanen (1999), the negotiators are required to report the optimal solutions of their own optimization problems to the mediator. These methods may lead to privacy disclosure inevitably in the sense that the mediator can infer some information about negotiators' objective functions based on the received information from negotiators and some additional information.

The fully trusted algorithm described in last subsection can generate an approximate POS with a geometric convergence rate within any pre-specified approximate error by adjusting the algorithm parameters. However, it is not somehow privacy preserving from the view that the mediator can infer some information about negotiators' value functions $f_i, i = 1, \ldots, n$ based on the estimates received from negotiators. In fact, from (4) we can find that in the special case when there is no constraint, i.e., $X_i = \mathbb{R}^m$, and the objective functions are differentiable, the mediator can obtain the gradients of negotiators' value functions at all the weighted average points and maybe further infer some information about negotiators' value functions based on some additional information. In fact, a strategically equivalent objective function in the neighborhood of weighted average points can be constructed based on the obtained gradients (Sehgal & Pal, 2005). We next present a modification to Algorithm 1 so that the negotiators' private information cannot be disclosed.

We keep Algorithm 1 unchanged except the following parts:

---

for $k = 0 : T$ **do**
All negotiators reach an agreement about some random vector $\mathbf{r}_k \in \mathbb{R}^m$
1': Each negotiator i transmits its noisy estimate $x_i^{\omega}(k) + \mathbf{r}_k$ to the mediator;
2': The mediator computes the weighted average $\bar{x}^{\omega}(k) = \sum_{i=1}^n \omega_i (x_i^{\omega}(k) + \mathbf{r}_k)$ of negotiators' noisy estimates and then reports $\bar{x}^{\omega}(k)$ to all negotiators;
3': **if** $k \le T - 1$
Each negotiator i updates its estimate and uses $x_i^{\omega}(k+1) = P_{X_i}\left(\bar{x}^{\omega}(k) - \mathbf{r}_k - \alpha g_i(k)\right)$ as the estimate at the next step, where $g_i(k) \in \partial f_i(\bar{x}^{\omega}(k) - \mathbf{r}_k)$;
else Each negotiator i gets $\bar{x}^{\omega}(T) - \mathbf{r}_T$ as the final estimate.
end for

We now illustrate that the above modified algorithm is privacy preserving. Clearly, since the mediator does not know the random vector $\mathbf{r}_k$, from the noisy estimate $x_i^{\omega}(k) + \mathbf{r}_k$ it is almost impossible to obtain $x_i^{\omega}(k)$ and then cannot get further information about negotiators' constraint sets and value functions. Notice that the above modification does not change the actual estimate update. Therefore, the algorithm remains as valid as the fully trusted one and the negotiators can prevent the disclosure of their private information. Moreover, it may be observed that negotiators might derive some information about other negotiators from the weighted average vector $\sum_{i=1}^n \omega_i x_i^{\omega}(k)$ (or $\sum_{i=1}^n \omega_i (x_i^{\omega}(k) + \mathbf{r}_k) - \mathbf{r}_k = \sum_{i=1}^n \omega_i x_i^{\omega}(k)$ in the modified version). However, this is also impossible since the negotiators do not know the weights taken by the mediator in the weighted average vector.

4. Approximate representation of Pareto frontier

In some practical situations, the negotiators may not be satisfied with some particular POS but want to find serval ones and then negotiate over them (Ehtamo et al., 1999a). In this section, we provide a systemic method to generate serval approximate POSs, which forms a discrete approximate representation (DAR) of the Pareto frontier. The proposed method is to first make a discretization of the whole nonnegative stochastic vector set, and then generate approximate POSs corresponding to the weight vectors in the discretization subset by applying the modified privacy preserving version of Algorithm 1. The strong convexity of value functions ensures that the obtained DAR is well dispersed over the Pareto frontier.

4.1. Relations with multiobjective optimization

Multiparty negotiations is closely related with the multiobjective optimization. Multiobjective optimization problems have also been widely investigated in last decades (Hwang & Masud, 1979; Karasakal & Köksalan, 2009; Klamroth & Miettinen, 2008; Masin & Bukchin, 2008; Sayin, 2003; Steuer, 1986). In negotiation analysis, multiple negotiators negotiate over many issues, where each negotiator has its individual value function, which is not known by other negotiators. In contrast to negotiation analysis, in multiobjective optimization problems there is usually one authority, for example, the manager in a large factory, who has multiple objectives to be optimized simultaneously and has the ability to take the full knowledge of all the objectives.

Similar to negotiation analysis, an important problem in multiobjective optimization is to find a discrete approximate representation of the Pareto frontier in the decision space or the nondominated set in the outcome space. Various methods have been proposed to generate an approximate representation (Karasakal & Köksalan, 2009; Klamroth & Miettinen, 2008; Masin & Bukchin, 2008; Sayin, 2003). In these methods, since the authority takes the full knowledge of the considered problem, the global information can be utilized, for instance, the whole nondominated set or the rough shape of the nondominated set to generate the desired representation, which is totally different from the decentralized methods in negotiation analysis.

4.2. Discretization of unit simplex Δ_n

In this subsection, we present a discretization subset of the unit simplex Δ_n with pre-specified discretization error ϵ. In fact, we can easily construct one as follows. Let $\epsilon^* = 1/\lceil \frac{\sqrt{n}}{\epsilon} \rceil$, where $\lceil b \rceil$ denotes the least integer not less than b. Clearly, $\epsilon^* \le \frac{1}{\sqrt{n}}\epsilon$. It is not hard to find that

$$\Omega_\epsilon := \left\{ \omega \middle| \omega_i = \kappa_i \epsilon^*, \kappa_i \text{ is a nonnegative integer}, \sum_{i=1}^n \kappa_i = \frac{1}{\epsilon^*} \right\}$$

is a discrete representation of $\triangle_n$ with discretization error $\sqrt{n}\epsilon^*$ $(\le \epsilon)$. That is,

$$\sup_{y \in \triangle_n} \inf_{z \in \Omega_\epsilon} |y - z| \le \epsilon.$$

The following lemma gives the cardinality of Ω_ϵ. The proof is given in Appendix C.

Lemma 4.1. *Let* $|\Omega_\epsilon|$ *denote the cardinality of* Ω_ϵ*. Then* $|\Omega_\epsilon| \le n^{\lceil \frac{\sqrt{n}}{\epsilon} \rceil}$.

Let $\nu = |\Omega_\epsilon|$. We sort the elements of Ω_ϵ in lexicographic order (also referring to Chapter 5 of Ehrgott, 2000 for lexicographic multiobjective optimization):

$$\left(\Omega_\epsilon = \{\omega^1, \ldots, \omega^\nu\}, <_{lex} \right). \tag{6}$$

Suppose $\omega^j = (\kappa_1^j \epsilon^*, \ldots, \kappa_n^j \epsilon^*)'$. Then $\omega^{j_1} <_{lex} \omega^{j_2}$ if and only if $\kappa_p^{j_1} < \kappa_p^{j_2}$, where $p = \min\{i | \kappa_i^{j_1} \ne \kappa_i^{j_2}\}$. We can find that any two elements in Ω_ϵ sorted in lexicographic order is contiguous if and only if the two elements have only two different components and the two different components are contiguous. It is easy to see that $\sum_{i=1}^n |\omega_i^j - \omega_i^{j+1}| = 2\epsilon^*$ for $1 \le j \le \nu - 1$.

4.3. An approximate representation generating algorithm

In this subsection, we first introduce an Approximate Representation Generating Algorithm based on the modified privacy preserving algorithm given in Section 4.2 and the discretization technique developed in last subsection, and then present the approximate error between the obtained DAR and the Pareto frontier $\mathcal{X}_E$. As the following theorem shows, the final approximate error is caused by two factors: the optimization algorithm just executes finite step iterations and the constructed discretization set Ω_ϵ is only a subset of the unit simplex $\triangle_n$. The proposed approximate representation generating algorithm is as follows (see Algorithm 2).

Here is the approximate error result, and its proof is presented in Appendix D.

Theorem 4.1. *Let* $\epsilon > 0$ *be any pre-specified discretization error and* Ω_ϵ *the discrete representation of* $\triangle_n$ *given in (6). Suppose the stepsize* α *satisfies* $0 < \alpha < n/\sigma_{max}$*, where* $\sigma_{max} = \max_{1 \le i \le n} \sigma_i$*. Then*

$$\sup_{x \in \mathcal{X}_E} \inf_{z \in \Theta} |x - z| \le \sqrt{\frac{2Bn\epsilon}{\sigma_{min}}} + \sqrt{C\left(1 - \frac{\alpha \sigma_{min}}{n}\right)^T + \frac{\alpha L^2}{\sigma_{min}}}, \tag{7}$$

where $C = \max_{1 \le j \le \nu} |\bar{x}^{\omega^j}(0) - \hat{x}(\omega^j)|^2$*. In other words, the generated set* Θ *in Algorithm 2 is a DAR of the Pareto frontier* $\mathcal{X}_E$ *with the number on the right-hand side of (7) as an upper bound of approximate error.*

Algorithm 2 Approximate representation generating algorithm (ARGA).

Input: The discretization $\Omega_\epsilon = \{\omega^1, \dots, \omega^\nu\}$ with lexicographic order (6); number of iterations T and the step-size α; initial conditions $x_i(0) \in \mathbb{R}^m$, $i = 1, \dots, n$;
Initialization: $\Theta = \emptyset$;
Output: The discrete approximate representation (DAR) Θ

for $j = 1 : \nu$ **do**
1: Execute the modified privacy preserving algorithm in Section 3.2 with inputs: weight vector ω^j, number of iterations T,step-size α and initial conditions $x_i^{\omega^1}(0) = x_i(0)$ for $j = 1$;$x_i^{\omega^j}(0) = x_i^{\omega^{j-1}}(T)$ for $j \geq 2$.
2: Obtain an approximate POS $\bar{x}^{\omega^j}(T)$ and let $\Theta := \Theta \cup \bar{x}^{\omega^j}(T)$.
end for

Theorem 4.1 gives the approximate error between the generated DAR and the Pareto frontier $\mathcal{X}_E$. Note that the approximate error in (7) depends only on the constraint sets X_is, the value functions f_is, the number of negotiators n, the number of iterations T and the step-size α, but not the weight vectors in Ω_ϵ. This provides the possibility of the existence of the uniform iteration steps to achieve the desired approximate error specified in advance. In the following, we will present some discussions on the choice problem of the number of iterations and discretization error to reach the pre-specified approximate error and the improving computation efficiency problem, respectively.

4.3.1. Achieve pre-specified approximate error ε

Clearly, we can find a discrete representation Ω_ϵ of Δ_n with sufficiently small discretization error ϵ and execute the modified Algorithm 1 with sufficiently small step-size α and sufficiently large iteration steps T to generate a DAR of $\mathcal{X}_E$ with any pre-specified approximate error. The following corollary is straightforward from Theorem 4.1.

Corollary 4.1. *When*

$$0 < \epsilon \leq \frac{\varepsilon^2 \sigma_{min}}{8cn}, \quad 0 < \alpha < \min\left\{\frac{n}{\sigma_{max}}, \frac{\varepsilon^2 \sigma_{min}}{8L^2}\right\},$$

$$T \geq \frac{\ln\left(\frac{\varepsilon^2}{8D}\right)}{\ln\left(1 - \frac{\alpha \sigma_{min}}{n}\right)},$$

$\sup_{x \in \mathcal{X}_E} \inf_{z \in \Theta} |x - z| \leq \varepsilon$. *In fact, under the above sufficient conditions, both the two terms of approximate error in (7) are not greater than $\varepsilon/2$, respectively, and hence the generated set Θ in Algorithm 2 is a DAR of $\mathcal{X}_E$ with approximate error ε.*

4.3.2. Improve computation efficiency

In ARGA, the initial conditions for executing j-th ($j \geq 2$) round Algorithm 1 are set to be negotiators' estimates $x_i^{\omega^{j-1}}(T)$ obtained in $(j-1)$-th round. The motivation of this choice of initial conditions comes from that it is expected that the information gained in previous rounds can be used to generate other approximate POSs in the coming rounds and then improve the computation efficiency.

We next give an estimate for $C = \max_{1 \leq j \leq \nu} |\bar{x}^{\omega^j}(0) - \hat{x}(\omega^j)|^2$. Notice that $\bar{x}^{\omega^1}(0) = \bar{x}(0)$, $\bar{x}^{\omega^j}(0) = \bar{x}^{\omega^{j-1}}(T)$ for $2 \leq j \leq \nu$. Fix $j \geq 2$. Then

$$\begin{aligned} |\bar{x}^{\omega^j}(0) - \hat{x}(\omega^j)| &= |\bar{x}^{\omega^{j-1}}(T) - \hat{x}(\omega^j)| \\ &\leq |\bar{x}^{\omega^{j-1}}(T) - \hat{x}(\omega^{j-1})| + |\hat{x}(\omega^{j-1}) - \hat{x}(\omega^j)| \\ &\leq |\bar{x}^{\omega^{j-1}}(T) - \hat{x}(\omega^{j-1})| + \sqrt{\frac{4\sqrt{2}B\epsilon}{\sigma_{min}}}, \end{aligned} \quad (8)$$

where in the second inequality we use the estimate inequality in Lemma 2.2 (ii) and the fact that $\sum_{i=1}^n |\omega_i^j - \omega_i^{j-1}| = 2\epsilon^* \leq \sqrt{2}\epsilon$.

Notice that the number of iterations T in Algorithm 1 is required to be uniform for different weight vectors. However, this may be not necessary in practical situations. In fact, from the estimate (8) it is easy to see that when the discretization error is small enough and the iteration number T in the $(j-1)$-th round is large enough, the term $|\bar{x}^{\omega^j}(0) - \hat{x}(\omega^j)|$ can be sufficiently small. Therefore, when Algorithm 1 is executed for weight vectors ω^j, $j \geq 2$, the needed number of iterations T may be not necessarily as large as that for ω^1 (the scalar $|\bar{x}(0) - \hat{x}(\omega^1)|$ may be large).

4.4. General convex functions

We have shown that a DAR of the Pareto frontier can be generated by the proposed method for strongly convex value functions. Here we discuss the feasibility of applying the proposed method to the more general convex value function case. In fact, the following example shows that when the value functions are only convex (not strongly convex), generally it is almost impossible to generate a DAR of $\mathcal{X}_E$ by the proposed method.

Example 4.1. In $\mathbb{R}^2$, let $X = X_1 = X_2 = \{(x_1, x_2)' | 0 \leq x_1, x_2 \leq 10, \sqrt{2}x_1 + x_2 \geq 2\}$. The value functions $f_i : \mathbb{R}^2 \to \mathbb{R}$ are $f_i(x_1, x_2) = x_i, i = 1, 2$. We can find that the Pareto frontier of the biobjective optimization problem is $\mathcal{X}_E = \{(z, 2 - \sqrt{2}z)' | 0 \leq z \leq 1\}$. Then the weight sum method is used to solve the following scalarized problem $P(\gamma)$ $(0 \leq \gamma \leq 1)$:

$$\begin{aligned} &\text{minimize} \;\; \gamma f_1(x_1, x_2) + (1 - \gamma) f_2(x_1, x_2) \\ &\text{subject to} \;\; (x_1, x_2) \in X. \end{aligned}$$

By some simple calculations, we can find that when $\gamma \in [0, \frac{\sqrt{2}}{\sqrt{2}+1})$, the unique optimal solution of $P(\gamma)$ is $(\sqrt{2}, 0)'$; when $\gamma \in (\frac{\sqrt{2}}{\sqrt{2}+1}, 1]$, the unique optimal solution of $P(\gamma)$ is $(0, 2)'$, and when $\gamma = \frac{\sqrt{2}}{\sqrt{2}+1}$, the optimal solution set of $P(\gamma)$ is $\{(z, 2 - \sqrt{2}z)' | 0 < z < \sqrt{2}\}$. We can see that the proposed method in this paper is impossible to generate a DAR of $\mathcal{X}_E$ for any sufficiently large iteration steps T and any sufficiently small discretization error ϵ.

5. Examples

In this section, we first present two practical examples to demonstrate that the proposed method is applicable in these situations and then an example to numerically compute the approximate error between the approximate representation obtained by the proposed method and the Pareto frontier.

Example 5.1.

(1) (Resource allocation negotiations Teich et al., 1996) We consider a two-party resource allocation negotiation problem, in which there is a single resource that must be allocated among multiple completing programs $p = 1, \dots, m$. Each party i prefers more resource to less and wants to maximize its own value function $g_i(x_1, \dots, x_m)$, where $x_p \geq 0$ is the amount allocated to program p. There is a shared resource constraint $\sum_{p=1}^m x_p = c$ with $c > 0$ the total available funding. Moreover, each x_p also has an upper bound, denoted as c_p, indicating that program p is fully funded at this level. Without loss of generality, $\sum_{p=1}^m c_p > c$ is assumed. This implies that the total funding c is insufficient to fund all programs fully.
The approximate POS computation problem of the above two-party resource allocation negotiations can be solved by the method proposed in this paper by setting

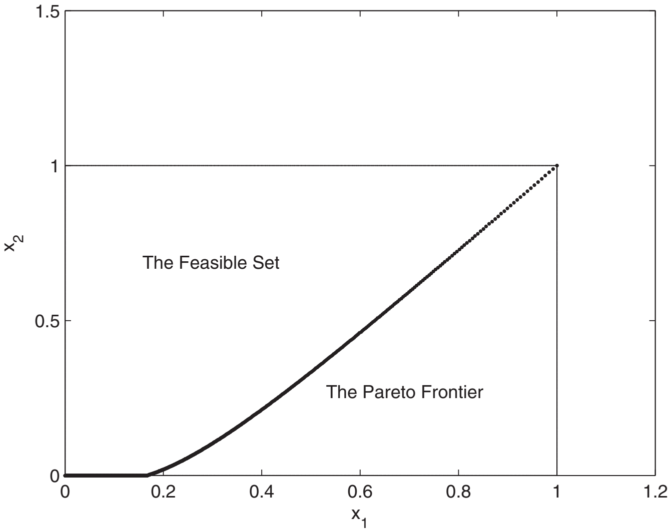

Fig. 1. The feasible set ($[0, 1] \times [0, 1]$) and the Pareto frontier (the black dotted line).

Table 1
The weight vector ω and the needed number of iterations T.

ω_1	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
T	32	33	33	35	37	40	43	43	60	143	335

$X_1 = X_2 = \{x | x = (x_1, \ldots, x_m)', 0 \le x_p \le c_p, \sum_{p=1}^m x_p = c\}$, $f_i = -g_i, i = 1, 2$.

(2) (Cournot games Ehtamo et al., 1996; Verkama et al., 1996). The Cournot game describes an oligopoly market in which two firms produce a homogeneous product. The two firms' decision variables are given by their product outputs, which are denoted as $x_i \in [0, c_i]$, $i = 1, 2$, respectively, where $c_i > 0$ denotes the capacity constraint of firm i. The market price $q(\cdot)$ is given by the industry inverse demand curve and the cost function of firm i is denoted by $g_i(\cdot)$. Then the profit function π_i are given by

$$\pi_i(x) = q(x_1 + x_2)x_i - g_i(x_i), i = 1, 2, x = (x_1, x_2).$$

The approximate POS computation problem of the above Cournot games can be solved by the method proposed in this paper by setting $X_1 = [0, c_1] \times [0, c]$, $X_2 = [0, c] \times [0, c_2]$, $f_i = -\pi_i, i = 1, 2$. Here $c > \max\{c_1, c_2\}$ is an upper bound of the two firms' capacity constraints and is known by the two firms.

Example 5.2. We consider the following bilateral negotiation problem:

$$f_1(x_1, x_2) = \frac{1}{5}\left(2(x_1 - 1)^2 + x_2^2 - 2x_1(x_2 - 1)\right),$$

$$f_2(x_1, x_2) = \frac{2}{5}\left(2x_1^2 + (x_2 + 1)^2 + (x_1 - 2)x_2\right),$$

where the decision sets are $X_1 = \{(x_1, x_2)' | -1 \le x_1 \le 1, -1 \le x_2 \le 1\}$, $X_2 = \{(x_1, x_2)' | 0 \le x_1 \le 2, 0 \le x_2 \le 2\}$. Then the feasible constraint set $X = X_1 \cap X_2 = \{(x_1, x_2)' | 0 \le x_1 \le 1, 0 \le x_2 \le 1\}$ and f_1, f_2 are strongly convex with parameters $\sigma_1 = \frac{3-\sqrt{5}}{5}$ and $\sigma_2 = \frac{6-2\sqrt{2}}{5}$, respectively. It is easy to see that $\sigma_{min} = \sigma_1$, $\sigma_{max} = \sigma_2$ and an upper bound of subgradients of f_1, f_2 on X is given by $L = \frac{12}{5}$.

Fig. 1 shows the feasible set and the Pareto frontier of the bilateral negotiation problem.

Table 1 shows the numbers of iterations T required by Algorithm 1 with initial condition $x_1(0) = x_2(0) = (5, -5)'$ and step-size $\alpha = 0.1$ for weight vectors $\omega = (\omega_1, 1 - \omega_1)', \omega_1 = 0, 0.1, \ldots, 0.9, 1$ to guarantee that the approximate error between the obtained estimate in Algorithm 1 and the exact POS $\arg\min_X(\omega_1 f_1 + (1 - \omega_1)f_2)$ is not greater than 0.01. That is, T is the smallest positive integer such that $|\bar{x}^\omega(T) - \hat{x}(\omega)| \le 0.01$.

Table 2
The discre. error ϵ and the discre. appro. error E_d.

ϵ	1/10	1/20	1/50	1/100	1/200	1/500	1/1000
E_d	0.2978	0.1935	0.0942	0.0507	0.0264	0.0108	0.0054

Table 3
The discre. error ϵ and the numer. appro. error E_f.

ϵ	1/10	1/20	1/50	1/100	1/200	1/500	1/1000
E_f	0.0336	0.0219	0.0108	0.0064	0.0064	0.0064	0.0064

Table 4
Weight vectors, corresponding approximate POSs generated by Algorithm 2, POSs and the Euclidean metric between generated approximate POSs and POSs.

Weights vectors	Generated approximate POSs	POSs	Euclidean metric
(0, 1)'	(1.7085e-15, 0)'	(0, 0)'	1.7085e−15
(0.1, 0.9)'	(0.0263, 1.1633e-04)'	(0.0263, 0)'	1.1888e−04
(0.2, 0.8)'	(0.0556, 5.4915e-04)'	(0.0555, 0)'	5.5672e−04
(0.3, 0.7)'	(0.0881, 0.0015)'	(0.0882, 0)'	0.0015
(0.4, 0.6)'	(0.1248, 0.0032)'	(0.1250, 0)'	0.0032
(0.5, 0.5)'	(0.1667, 0.0064)'	(0.1667, 0)'	0.0064
(0.6, 0.4)'	(0.2165, 0.0309)'	(0.2165, 0.0309)'	1.1435e−08
(0.7, 0.3)'	(0.2826, 0.0870)'	(0.2826, 0.0870)'	1.0486e−07
(0.8, 0.2)'	(0.3810, 0.1905)'	(0.3810, 0.1905)'	1.4561e−06
(0.9, 0.1)'	(0.5562, 0.4045)'	(0.5562, 0.4045)'	3.1200e−05
(1, 0)'	(0.9993, 0.9989)'	(1, 1)'	0.0013

E_d	E_f	A upper bound of the approximate error E
0.0108	0.0064	0.0172

Example 5.3. We still consider the bilateral negotiation problem in Example 5.2. Table 2 shows the discretization approximate error (defined as $\sup_{x \in \mathcal{X}_E} \inf_{v \in \Xi_\epsilon} |x - v| =: E_d$ with $\Xi_\epsilon = \{\arg\min_X \sum_{i=1}^n \omega_i f_i, \omega \in \Omega_\epsilon\}$ denoting the exact POSs corresponding to the weight vectors in Ω_ϵ) for different discretization error ϵ. Clearly, the discretization approximate error decreases as the discretization error ϵ decreases.

Table 3 shows the numerical approximate error (defined as $\sup_{\omega \in \Omega_\epsilon} |\bar{x}^\omega(T) - \arg\min_X \sum_{i=1}^n \omega_i f_i| =: E_f$) for different discretization error ϵ, where the DAR Θ is generated by ARGA with the number of iterations $T = 200$, step-size $\alpha = 0.1$ and initial condition $x_1(0) = x_2(0) = (5, -5)'$. Clearly, the approximate error $\sup_{x \in \mathcal{X}_E} \inf_{z \in \Theta} |x - z| =: E$ is bounded by $E_f + E_d$, i.e., $E \le E_f + E_d$.

Table 4 shows 11 weight vectors selected from $\Omega_{1/500}$, the generated approximate POSs by ARGA, the exact POSs corresponding to the 11 weight vectors and the Euclidean metric between each pair points. Here $\epsilon = 1/500$, $T = 200$, $\alpha = 0.1$, $x_1(0) = x_2(0) = (5, -5)'$.

6. Conclusion

In this paper we proposed a decentralized method for finding an approximate representation of the Pareto frontier in multiparty negotiations with privacy preserving concern. In our setup, all negotiators are unwilling to communicate with each other directly and only exchange their noisy estimates with the mediator. All parties are semi-honest in the sense that they follow the designed protocol correctly, but they may record and analyze the received data in the algorithm execution in order to infer other parties' private information.

Our decentralized algorithm is based on the weight sum method and subgradient optimization algorithm. The proposed weighted average and local optimization scheme can generate a POS for some particular weight vector and a discrete approximate representation by systematically varying the weights. The approximate error between the generated approximate representation and the Pareto frontier can be controlled by the algorithm parameters to achieve any pre-specified accuracy level. It also reveals that the developed method is privacy preserving.

POS computation problem for resource allocation negotiations and Cournot games have been widely discussed in the literature. The developed method in this paper is applicable in these practical situations by finding a proper third-party to serve as a neutral mediator, for example, the resource supplier in resource allocation negotiations and some product purchaser in Cournot games. In such a negotiator-mediator scenario, an approximate POS or an approximation representation of the Pareto frontier can be obtained provided that all parties obey the designed estimate update rule. Developing other more efficient decentralized methods to deal with other types of value functions, for example, general convex functions awaits further investigation.

Appendix A. Proof of Lemma 2.2

We first show (i). Let $\{\omega^r\}$, $\omega^r \in \Delta_n$ be a convergent sequence with $\lim_{r\to\infty}\omega^r = \bar\omega$. Since Δ_n is a closed set, $\bar\omega \in \Delta_n$. Let $x^r = \arg\min_X \sum_{i=1}^n \omega_i^r f_i$, i.e., $\sum_{i=1}^n \omega_i^r f_i(x^r) \le \sum_{i=1}^n \omega_i^r f_i(x), \forall x \in X$. Since X is bounded, the sequence $\{x^r\}$ has a limit point. Let $\bar x$ be a limit point of $\{x^r\}$ with $\lim_{s\to\infty} x^{r_s} = \bar x$. Taking the limit for the previous inequality with the identity $r = r_s$ yields $\sum_{i=1}^n \bar\omega_i f_i(\bar x) \le \sum_{i=1}^n \bar\omega_i f_i(x), \forall x \in X$. Noting that $\bar\omega$ has at least one positive component and $f_i, i = 1, \dots, n$ are strictly convex, $\bar x$ is the unique optimal solution of $\min_X \sum_{i=1}^n \bar\omega_i f_i$, i.e., $\bar x = \arg\min_X \sum_{i=1}^n \bar\omega_i f_i$. Then the continuity of $\hat x(\cdot)$ follows from that $\bar x$ is taken from the limit point set freely.

We next show (ii). Clearly, $|\sum_{i=1}^n \omega_i^1 f_i(x) - \sum_{i=1}^n \omega_i^2 f_i(x)| \le B\sum_{i=1}^n |\omega_i^1 - \omega_i^2|$, $\forall x \in X$, where $B = \sup_{i, x\in X} f_i(x)$ is a finite number due to the boundedness of X and the continuity of convex functions $f_i, i = 1, \dots, n$.

Let $\hat x(\omega^1) = \arg\min_X \sum_{i=1}^n \omega_i^1 f_i =: x^1$, $\hat x(\omega^2) = \arg\min_X \sum_{i=1}^n \omega_i^2 f_i =: x^2$. We now show by contradiction that $|x^1 - x^2| \le 2\sqrt{\frac{B\sum_{i=1}^n |\omega_i^1 - \omega_i^2|}{\sigma_{min}}}$. Hence suppose $|x^1 - x^2| > 2\sqrt{\frac{B\sum_{i=1}^n |\omega_i^1 - \omega_i^2|}{\sigma_{min}}}$. First it follows from the strong convexity of $f_i, i = 1, \dots, n$ that $\sum_{i=1}^n \omega_i^\ell f_i$ is also strongly convex with parameter $\sigma_{min} > 0$, $\ell = 1, 2$. Then based on inequality (3),

$$\sum_{i=1}^n \omega_i^\ell f_i(x) \ge \sum_{i=1}^n \omega_i^\ell f_i(x^\ell) + \frac{1}{2}\sigma_{min}|x - x^\ell|^2, \ell = 1, 2.$$

Therefore,

$$\sum_{i=1}^n \omega_i^2 f_i(x^2) + B\sum_{i=1}^n |\omega_i^1 - \omega_i^2|$$
$$\ge \sum_{i=1}^n \omega_i^1 f_i(x^2)$$
$$\ge \sum_{i=1}^n \omega_i^1 f_i(x^1) + \frac{1}{2}\sigma_{min}|x^2 - x^1|^2$$
$$\ge \sum_{i=1}^n \omega_i^2 f_i(x^1) - B\sum_{i=1}^n |\omega_i^1 - \omega_i^2| + \frac{1}{2}\sigma_{min}|x^2 - x^1|^2,$$

which leads to

$$\sum_{i=1}^n \omega_i^2 f_i(x^2) \ge \sum_{i=1}^n \omega_i^2 f_i(x^1) - 2B\sum_{i=1}^n |\omega_i^1 - \omega_i^2| + \frac{1}{2}\sigma_{min}|x^2 - x^1|^2$$
$$> \sum_{i=1}^n \omega_i^2 f_i(x^1).$$

This contradicts that x^2 is the minimizer of $\min_X \sum_{i=1}^n \omega_i^2 f_i$. Thus, $|x^1 - x^2| \le 2\sqrt{\frac{B\sum_{i=1}^n |\omega_i^1 - \omega_i^2|}{\sigma_{min}}}$, which completes the proof. □

Appendix B. Proof of Theorem 3.1

In this proof, when there is no potential confusion, we omit ω in $\hat x(\omega)$, x_i^ω, $\bar x^\omega$, y_i^ω and write them simply $\hat x$, x_i, $\bar x$, y_i.

Let $\hat x = \arg\min_X \sum_{i=1}^n \omega_i f_i$. By the estimate update equation (4) in Algorithm 1, $X \subseteq X_i$ and the convex projection inequality $|P_{X_i}(y) - z| \le |y - z|$ for any $y \in \mathbb{R}^m$ and $z \in X_i$, we have

$$\begin{aligned}|x_i(k+1) - \hat x|^2 &\le \left|\bar x(k) - \alpha g_i(k) - \hat x\right|^2 \\ &= |\bar x(k) - \hat x|^2 + \alpha^2|g_i(k)|^2 - 2\alpha\langle \bar x(k) - \hat x, g_i(k)\rangle \\ &\le |\bar x(k) - \hat x|^2 + \alpha^2 L^2 - 2\alpha\Big(f_i(\bar x(k)) - f_i(\hat x) \\ &\quad + \frac{1}{2}\sigma_i|\bar x(k) - \hat x|^2\Big),\end{aligned} \tag{9}$$

where the second inequality follows from the relation (2). Here $L = \sup_{z\in\cup_{i,x\in X_i}\partial f_i(x)} |z|$ is a finite number. By the convexity of function $|\cdot|^2$, we have

$$\begin{aligned}|\bar x(k+1) - \hat x|^2 &\le \sum_{i=1}^n \omega_i |x_i(k+1) - \hat x|^2 \\ &\le \Big(1 - \alpha\sum_{i=1}^n \omega_i\sigma_i\Big)|\bar x(k) - \hat x|^2 \\ &\quad - 2\alpha\Big(\sum_{i=1}^n \omega_i f_i(\bar x(k)) - \sum_{i=1}^n \omega_i f_i(\hat x)\Big) + \alpha^2 L^2 \\ &\le \Big(1 - \alpha\sum_{i=1}^n \omega_i\sigma_i\Big)|\bar x(k) - \hat x|^2 + \alpha^2 L^2,\end{aligned} \tag{10}$$

where the second inequality follows from taking the sum for both sides of (9) over $i = 1, \dots, n$.

By recursive computation for inequality (10), we have

$$\begin{aligned}|\bar x(k+1) - \hat x|^2 &\le \Big(1 - \alpha\sum_{i=1}^n \omega_i\sigma_i\Big)^{k+1}|\bar x(0) - \hat x|^2 \\ &\quad + \alpha^2 L^2 \sum_{r=0}^k \Big(1 - \alpha\sum_{i=1}^n \omega_i\sigma_i\Big)^r \\ &\le \Big(1 - \alpha\sum_{i=1}^n \omega_i\sigma_i\Big)^{k+1}|\bar x(0) - \hat x|^2 + \frac{\alpha L^2}{\sum_{i=1}^n \omega_i\sigma_i},\end{aligned}$$

where the second inequality follows from that $0 < \alpha\sum_{i=1}^n \omega_i\sigma_i < 1$ under the hypothesis $\alpha < 1/\sum_{i=1}^n \omega_i\sigma_i$. We complete the proof. □

Appendix C. Proof of Lemma 4.1

In fact, $|\Omega_\epsilon|$ is equal to the number of the solutions to the following integer programming problem:

$$\kappa_1 + \kappa_2 + \cdots + \kappa_n = \frac{1}{\epsilon^*}, \ \kappa_i \text{ is a nonnegative integer}, i = 1, \ldots, n.$$

Then it is not hard to see

$$|\Omega_\epsilon| = \binom{\frac{1}{\epsilon^*} + n - 1}{n-1} = \frac{(\frac{1}{\epsilon^*} + n - 1)!}{(n-1)!\frac{1}{\epsilon^*}!} = \frac{\prod_{j=1}^{n-1}(\frac{1}{\epsilon^*} + j)}{(n-1)!}$$
$$= \prod_{j=1}^{n-1}\left(1 + \frac{\frac{1}{\epsilon^*}}{j}\right) \le \prod_{j=1}^{n-1} e^{\frac{\frac{1}{\epsilon^*}}{j}} = e^{\frac{1}{\epsilon^*}\sum_{j=1}^{n-1}\frac{1}{j}}$$
$$\le e^{\frac{1}{\epsilon^*}\ln n} = n^{\frac{1}{\epsilon^*}} = n^{\left\lceil \frac{\sqrt{n}}{\epsilon} \right\rceil}.$$

Then the conclusion follows. □

Appendix D. Proof of Theorem 4.1

Take $x^* \in \mathcal{X}_E$ arbitrarily. By Lemma 2.1, there exists $\omega^* \in \Delta_n$ such that $x^* = \arg\min_X \sum_{i=1}^n \omega_i^* f_i$. Based on the definition of Ω_ϵ, there exists $\omega \in \Omega_\epsilon$ such that $\sum_{i=1}^n |\omega_i - \omega_i^*| \le \frac{n}{2}\epsilon$. Let $\hat{x}(\omega) = \arg\min_X \sum_{i=1}^n \omega_i f_i$. By Lemma 2.2,

$$|\hat{x}(\omega) - x^*| \le 2\sqrt{\frac{B\sum_{i=1}^n |\omega_i - \omega_i^*|}{\sigma_{min}}} \le \sqrt{\frac{2Bn\epsilon}{\sigma_{min}}}. \tag{11}$$

Moreover, there is $\bar{x}^\omega(T) \in \Theta$ obtained by Algorithm 2 with weight vector ω. Therefore, from Theorem 3.1 we have

$$|\bar{x}^\omega(T) - \hat{x}(\omega)| \le \sqrt{\left(1 - \frac{\alpha\sum_{i=1}^n \omega_i\sigma_i}{n}\right)^T |\bar{x}^\omega(0) - \hat{x}(\omega)|^2 + \frac{\alpha L^2}{\sum_{i=1}^n \omega_i\sigma_i}}. \tag{12}$$

Combining (11) with (12) together yields

$$|\bar{x}^\omega(T) - x^*|$$
$$\le |\bar{x}^\omega(T) - \hat{x}(\omega)| + |\hat{x}(\omega) - x^*|$$
$$\le \sqrt{\frac{2Bn\epsilon}{\sigma_{min}}} + \sqrt{\left(1 - \frac{\alpha\sum_{i=1}^n \omega_i\sigma_i}{n}\right)^T |\bar{x}^\omega(0) - \hat{x}(\omega)|^2 + \frac{\alpha L^2}{\sum_{i=1}^n \omega_i\sigma_i}}$$
$$\le \sqrt{\frac{2Bn\epsilon}{\sigma_{min}}} + \sqrt{C\left(1 - \frac{\alpha\sigma_{min}}{n}\right)^T + \frac{\alpha L^2}{\sigma_{min}}}, \tag{13}$$

where $C = \max_{1\le j\le \nu} |\bar{x}^{\omega^j}(0) - \hat{x}(\omega^j)|^2$, which is a finite number due to the boundedness of $X_i, i = 1, \ldots, n$. Then by inequality (13) and the fact that x^* is taken from $\mathcal{X}_E$ arbitrarily, we conclude that the approximate error $\sup_{y\in\mathcal{X}_E}\inf_{z\in\Theta}|y - z|$ is not greater than the number given in (13). The proof is completed. □

References

Ehrgott, M. (2000). *Multicriteria optimization*. Springer Verlag.

Ehtamo, H., Hamalainen, R., Heiskanen, P., Teich, J., Verkama, M., & Zionts, S. (1999a). Generating Pareto solutions in a two-party setting: Constraint proposal methods. *Management Science, 45*, 1697–1709.

Ehtamo, H., Kettunen, E., & Hamalainen, R. (2001). Searching for joint gains in multiparty negotiations. *European Journal of Operational Research, 130*, 54–69.

Ehtamo, H., Verkama, M., & Hamalainen, R. (1996). On distributed computation of Pareto solutions for two decision makers. *IEEE Transactions on Systems, Man, and Cybernetics Part A, 26*, 498–503.

Ehtamo, H., Verkama, M., & Hamalainen, R. (1999b). How to select fair improving directions in a negotiation model over continuous issues. *IEEE Tracsactions on Systems, Man and Cybernetics Part C, 29*, 26–31.

Fulga, C. (2007). Decentralized cooperative optimization for multi-criteria decision making. *Advances in cooperative control and optimization* (pp. 65–80). Berlin: Springer.

Geoffrion, A. (1968). Proper efficiency and the theory of vector maximization. *Journal of Mathematical Analysis and Applications, 22*, 618–630.

Goldreich, O. (1998). Secure multi-party computation, (working draft), available at: URL: http://www.wisdom.weizmann.ac.il/~oded/pp.html.

Heiskanen, P. (1999). Decentralized method for computing Pareto solutions in multiparty negotiations. *European Journal of Operational Research, 117*, 579–590.

Heiskanen, P. (2001). Generating Pareto-optimal boundary points in multiparty negotiations using constraint proposal method. *Naval Research Logistics, 48*, 210–225.

Heiskanen, P., Ehtamo, H., & Hamalainen, R. (2001). Constraint proposal method for computing Pareto solutions in multi-party negotiations. *European Journal of Operational Research, 133*, 44–61.

Hwang, C. L., & Masud, A. S. M. (1979). *Multiple objective decision making methods and applications: A state-of-the-art survey*. Berlin: Springer-Verlag.

Karasakal, E., & Köksalan, M. (2009). Generating a representative subset of the nondominated frontier in multiple criteria decision making. *Operations Research, 59*, 187–199.

Kearns, M., Tan, J., & Wortman, J. (2007). Privacy-preserving belief propagation and sampling. *Advances in Neural Information Processing Systems, 20*.

Kitti, M., & Ehtamo, H. (2007). Analysis of the constraint proposal method for two-party negotiations. *European Journal of Operational Research, 181*, 817–827.

Klamroth, K., & Miettinen, K. (2008). Integrating approximation and interactive decision making in multicriteria optimization. *Operations Research, 56*, 222–234.

Lou, Y., Hong, Y., Xie, L., Shi, G., & Johansson, K. H. (2016). Nash equilibrium computation in subnetwork zero-sum games with switching communications. *IEEE Transactions on Automatic Control, 61*. (In press), A version is available at URL: http://arxiv.org/abs/1312.7050

Lou, Y., Shi, G., Johansson, K. H., & Hong, Y. (2014). Approximate projected consensus for convex intersection computation: Convergence analysis and critical error angle. *IEEE Transactions on Automatic Control, 59*, 1722–1736.

Masin, M., & Bukchin, Y. (2008). Diversity maximization approach for multiobjective optimization. *Operations Research, 56*, 411–424.

Nedić, A., & Ozdaglar, A. (2009). Distributed subgradient methods for multi-agent optimization. *IEEE Transactions on Automatic Control, 54*, 48–61.

Nedić, A., Ozdaglar, A., & Parrilo, P. A. (2010). Constrained consensus and optimization in multi-agent networks. *IEEE Transactions on Automatic Control, 55*, 922–938.

Pathak, M. A., & Raj, B. (2011). Efficient protocols for principal eigenvector computation over private data. *Transactions on Data Privacy, 4*, 129–146.

Raiffa, H. (1982). *The art and science of negotiation*. Cambridge, MA: Harvard University Press.

Sayin, S. (2003). A procedure to find discrete representations of the efficient set with specified coverage errors. *Operations Research, 51*, 427–436.

Sebenius, J. K. (1992). Negotiation analysis: A characterization and review. *Management Science, 38*, 18–38.

Sehgal, S. K., & Pal, A. K. (2005). Privacy preserving decentralized method for computing a Pareto-optimal solution, *Lecture Notes in Computer Science: 3741* (pp. 578–583). Berlin Heidelberg: Springer-Verlag.

Steuer, R. E. (1986). *Multiple criteria optimization: Theory, computation, and application*. New York: John Wiley.

Teich, J., Wallenius, H., Wallenius, J., & Zionts, S. (1995). A decision support approach for negotiation with an application to agricultural income policy negotiations. *European Journal of Operational Research, 81*, 76–87.

Teich, J., Wallenius, H., Wallenius, J., & Zionts, S. (1996). Identifying Pareto-optimal settlements for two-party resource allocation negotiations. *European Journal of Operational Research, 93*, 536–549.

Verkama, M., Ehtamo, H., & Hamalainen, R. (1996). Distributed computation of Pareto solutions in n-player games. *Mathematical Programming, 74*, 29–45.

Yan, F., Sundaram, S., Vishwanathan, S. V. N., & Qi, Y. (2013). Distributed autonomous online learning: Regrets and intrinsic privacy-preserving properties. *IEEE Transactions on Knowledge and Data Engineering, 25*, 2483–2493.