A GAME FORM WITH MINIMAL MESSAGE SPACE FOR SECURE– AND DOMINANT STRATEGY IMPLEMENTATION

Ville Korpela [*] [†]

August 21, 2009

Abstract

A method for constructing a minimal implementing game form under the assumption that each agent is only aware of her own preferences is presented. For this method to work the direct revelation mechanism must implement the goal in dominant strategies, so an additional property of weak non-bossiness is required besides strategy-proofness. This method also works in the case of securely implementable goal function without any modifications.

JEL Classification: D71, D78

Keywords: Decentralized Mechanism, Direct Revelation Mechanism, Dominant Strategy Implementation, Rectangular Property, Revelation Principle, Secure Implementation, Strategy-Proofness, Weak Non-Bossiness.

1 Introduction

Dominant strategy equilibrium is the appropriate solution consept to be used in implementation problems when agent's are assumed to know only their

[*]University of Turku, Public Choice Research Centre and Department of Economics, FIN-20014. E-mail: ville.korpela@utu.fi.

[†]Many thanks to Hannu Vartiainen for useful discussions.

own preferences. Since direct revelation mechanism implements truthfully any goal function that is dominant strategy implementable by Dasgupta, Hammond and Maskin (1979), the implementation problem seems almost trivial under this informational assumption. And even if truthfull implementation is not considered as satisfactory, since there may be other dominant strategy equilibria besides truth telling, an additional property called weak non-bossiness is enough to make the direct revelation mechanism do the trick by Saijo, Sjöström and Yamato (2007).

Unfortunately, this clean view omits an important problem. In many realistic situations direct revelation mechanism can be informationally very inefficient. If there are k different outcomes to choose from, the number of possible preferences is 2^k. Even though Gibbard-Satterthwite -theorem[1] tells us that the preference domain can not be this large for every agent, it can certainly be for some of them. The number of strategies in the direct revelation mechanism can then be exponentially larger that the number of equilibrium strategies needed a priori, which makes it important to study how many messages are in fact inevitable by finding the minimal indirect mechanism. This is our aim in the following chapters.

The common objection raised against indirect mechanisms is that the computational task will just shift to agent's in the form of learning more complicated rules that they do not necessarily even understand. Considering this, it is a bit unclear whether anything can be really achieved by using indirect mechanisms. Still, as the previous computerized environment example shows, this kind of distributed computing (in a sense) may sometimes be inevitable for implementation to be possible at all. Also, in some cases it may be preferable to use indirect mechanism on the ground that agent's don't have to introspect as accurately. It may be demanding for an agent to know her preferences in a fine tuned manner and indirect mechanisms can

[1]If the domain of preferences is unrestricted and the goal function is surjective, then strategy-proofness implies that the goal function is dictatorial. It will later be explained why these properties must hold. For more details see for example Danilov and Sotskov (2002).

have one strategy that is dominant for an entire class of preferences.

We proceed as follows. In chapter 2 some concepts that are needed in characterizing securely- and dominant strategy implementable goal functions are introduced. After this we give a method, presented in Hurwicz and Reiter (2008), for constructing a decentralized mechanism with minimal number of equilibrium messages. Since dominant strategy equilibrium and Nash equilibrium are decetralizable equilibrium conceps, every game form that implements a goal function securely- or in dominant strategies can be used to obtain a decentralized mechanism that realize the same goal function *i.e* there is always a realizing decentralized mechanism embedded in the implementing game form. This makes it conceivable that the decentralized mechanism with minimal message space could be expanded to obtain a minimal implementing game form. In chaper 3 we shall prove that this can indeed be done. Chapter 4 concludes.

2 Definitions, Preliminaries and Some Notational Conventions

Let Z be an abstract outcome space, without any special structure, and let $I = \{1, \ldots, n\}$ be the set of agents. A generic element of this set is denoted by i and we assume that $n \geq 2$. Every agent i has a complete and transitive preference ordering over Z denoted by θ_i, the strict part of which is denoted by $S\theta_i$ and the indifference part by $\sim_{\theta_i}$.[2] Furthermore, for every agent i, let Θ_i be the set of all possible preference orderings. Then, using the notation $\theta = (\theta_1, \ldots, \theta_n) \in \Theta \equiv \times_{i \in I} \Theta_i$,[3] a *goal function* is a function $f : \Theta \to Z$ that connects a unique alternative $f(\theta)$ in Z with every $\theta \in \Theta$. A goal function

[2] θ_i is not necessarily a preference relation, it can also be a label for utility function as in $u(\cdot, \theta_i)$. For the sake of simplicity, all formulas are expressed as if θ_i would be a preference relation.

[3] We assume that Θ is at most numerably infinite. This makes it possible to avoid comparing infinite cardinals.

f is called *strategy-proof* if

$$f(\theta)\theta_i f(\theta_i', \theta_{-i}) \text{ for all } \theta_i' \in \Theta_i,\ \theta \in \Theta \text{ and } i \in I. \tag{1}$$

It satisfies the *rectangular property*, if for all $\theta, \theta' \in \Theta$

$$f(\theta') \sim_{\theta_i} f(\theta_i, \theta_{-i}')\ \ \forall\, i \in I \ \ \Rightarrow \ \ f(\theta') = f(\theta), \tag{2}$$

and *weak non-bossiness*,[4] if for all $\theta, \theta' \in \Theta$ and all $i \in I$

$$f(\theta_i, \theta_{-i}) \neq f(\theta_i', \theta_{-i}) \ \ \Rightarrow \ \ \exists\, \theta_{-i}^* :\ f(\theta_i, \theta_{-i}^*) \nsim_{\theta_i} f(\theta_i', \theta_{-i}^*). \tag{3}$$

A *mechanism* is a triplet $\pi = (\mu, M, h)$, where M is the *(common) message space*, $\mu : \Theta \to M$ is the *(group) equilibrium message correspondence* and $h : M \to Z$ is the *outcome function*. We say that the mechanism π *realize* f if

$$h \circ \mu(\theta) = f(\theta) \ \text{ for all } \ \theta \in \Theta, \tag{4}$$

and call it *informationally decentralized*, or simply *decentralized*, if there exists a correspondence $\mu_i : \Theta_i \to M$ for every agent i, such that

$$\mu(\theta) = \bigcap \mu_i(\theta_i) \ \text{ for all } \ \theta \in \Theta.^5 \tag{5}$$

This means that message verification depends only on agent's own preferences, it is *privacy-preserving*. One should notice that every goal function f can be realized with the *decentralized direct revelation mechanism*, defined by $M = \Theta$, $\mu_i(\theta_i) = \{\theta' \in \Theta \mid \theta_i' = \theta_i\}$ and $h(\theta) = f(\theta)$. So the question is not whether something can be realized, but rather, how can it be realized

[4]Rectangular property is stronger than weak non-bossiness, the former implies the latter (just choose $\theta_{-i}^* = \theta_{-i}'$).

[5]Let's assume that every agent i acts according to some message verification protocol $\boldsymbol{m}_i^{t+1} = g_i(\boldsymbol{m}^t, \theta_i)$, where $\boldsymbol{m}^t$ is the vector of messages sent at time t and $\boldsymbol{m}_i^{t+1}$ is the reply of agent i at time $t+1$. With this interpretation, μ can be thought of as representing a static equilibrium of a message verification scenario *i.e.*

$$\mu(\theta) = \{\boldsymbol{m} \in M \ \mid \boldsymbol{m}_i = g_i\left(\boldsymbol{m}, \theta_i\right) \text{ for all } i \in I\} = \bigcap \{\boldsymbol{m} \in M \mid \boldsymbol{m}_i = g_i(\boldsymbol{m}, \theta_i)\} = \bigcap \mu_i(\theta_i).$$

For more details see ex. Hurwicz (1994).

with the smallest possible message space M?[6] This has been solved in Hurwicz and Reiter (2008) and we shall next explain their constructive method in it's essentials.

A coverin C of Θ is called f *contour contained* (shortly f-cc) if for all $K \in C$, there exists $z \in Z$ such that $K \subseteq f^{-1}(z)$, and *rectangular*, if all sets $K \in C$ have the structure of a cartesian product. Any f-cc and rectangular covering C, that does not contain redundancy,[7] has a *system of distinct representatives* (SDR)[8] *i.e* a function $\Lambda : C \to \Theta$ which satisfies two properties: (i) for every $K \in C$, $\Lambda(K) \in K$ and (ii) $K' \neq K''$ implies $\Lambda(K') \neq \Lambda(K'')$. Now define two correspondences, $\Omega : \Theta \to C$, $\Omega(\theta) = \{K \in C \mid \theta \in K\}$ and a bijection $v : \Lambda(C) \to M$, and assume that C is f-cc, rectangular and does not contain redundancy. Then, a mechanism $\pi_C = (\mu, M, h)$ defined by the two conditions

$$\mu = v \circ \Lambda \circ \Omega \quad \text{and} \quad h = f \circ v^{-1} \tag{6}$$

will realize f. To complete the description, two more questions need to be addressed. Namely, can μ be decentralized *i.e* expressed as an intersection of coordinate correspondences, and, what are the properties of C that guarantee the minimality of M? [9]

To this end, define a correspondence $\Omega_i : \Theta_i \to C$, $\Omega_i(\theta_i) = \{K \in C \mid \theta_i \in proj_i K\}$ for every agent i.[10] Condition (5) can then be satisfied by choosing $\mu_j = v \circ \Lambda \circ \Omega_j$ for all $j \in I$, so π_C can in fact be decentralized. To answer the second question, we must first emphasize that every decentralized mechanism π can be produced with the previous method using some rectangular and f-cc covering C. Furthermore, it is clear that the minimal size of the

[6] Keep in mind that the minimal size of M is a well defined concept, while the minimal size of M_i is not. When $i \neq j$, the mechanism that minimize the size of M_i may not be the same that minimize the size of M_j.

[7] No set is contained in the union of the others.

[8] A basic theorem on systems of distinct representatives is proven in Hall (1948).

[9] We could simply choose a subset of C as our message space. The purpose of the coding function v is to make it explicit that agents don't have to transmit a complete characterization of their preferences, only an abstract message.

[10] $proj_i K$ is formally defined as the set $\{\theta_i \in \Theta_i \mid (\theta_i, \theta_{-i}) \in K \text{ for some } \theta_{-i} \in \Theta_{-i}\}$.

message space M is connected with the maximal coarseness of the covering C.[11] Unfortunately, the relation "*coarsening*" is not complete. There can exist, and usually does exist, many maximally coarse coverings with different number of sets. This means that in decentralized mechanisms *observational efficiency*, the precision in which agents have to observe their preferences, is not completely aligned with *informational efficiency* , the minimal number of messages needed in communication. More precisely, the latter implies the former, but not vice versa.[12]

A few more definitions are needed before we can continue. *Game form* is a tuple $G = (S, g)$, where $S = \times_{i \in I} S_i$ is the *strategy space* and $g : S \to Z$ is the *outcome function*. When preference profile $\theta \in \Theta$ is given, this game form defines a game $\Gamma(\theta) = (G, \theta)$ in normal form. A strategy $\boldsymbol{s}^*$ is *Nash equilibrium* of the game $\Gamma(\theta)$, if $g(\boldsymbol{s}^*)\theta_i h(s_i, \boldsymbol{s}^*_{-i})$ for all $i \in I$ and for all $s_i \in S_i$. The set of all Nash equilibria in $\Gamma(\theta)$ is denoted by $N(\Gamma(\theta))$. We say that the game form G *implements* f *in Nash equilibrium* if $g(N(\Gamma(\theta))) = f(\theta)$ for all $\theta \in \Theta$. In a similar manner, strategy $\boldsymbol{s}^*$ is a *dominant strategy equilibrium* of the game $\Gamma(\theta)$, if $g(\boldsymbol{s}^*_i, \boldsymbol{s}_{-i})\theta_i g(\boldsymbol{s})$ for all $i \in I$ and for all $\boldsymbol{s} \in S$. The set of all dominant strategy equilibria in $\Gamma(\theta)$ is denoted by $D(\Gamma(\theta))$, and, a game form G *implements* f *in dominant strategies* if $g(D(\Gamma(\theta))) = f(\theta)$ for all $\theta \in \Theta$. If the game form G implements f in Nash$-$ and in dominant startegy equilibrium, then, following Saijo et. al. (2007), we call it *securely*

[11] A covering C' is a coarsening of the covering C , if for every $K \in C$ there is $K' \in C'$ such that $K \subseteq K'$. It is a proper coarsening, if $K \subset K'$ for some $K \in C$ and $K' \in C'$. A maximally coarse covering can then be defined as one that does not have any proper coarsenings.

[12] In Hurwicz and Reiter (2008) two methods for constructing maximally coarse coverings are presented. The *reflexive rectangular method* (rRM), which does not necessarily produce a minimal covering, and the *orinary reflexive rectangular method* (OrRM), which produce a minimal rRM covering, although it does not always work when Z is infinite and it is more cumbersome. Heuristically rRM works as follows. Take an arbitrary preference profile θ and form a largest possible rectangle contained in the same contour set (outcome is not unique, it may depend on which direction the expansion is made first). Choose then a new preference profile that is outside the class already formed and continue until a covering of Θ is obtained. The end result will always be a maximally coarse covering in the set of all f-cc and rectangular coverings.

implementable.[13]

3 A Game Form With Minimal Message Space

Even though the problem of finding an informationally efficient decentralized mechanism and the problem of finding a minimal game form that can be used in implementation are fundamentally very different, we can still use the former as a strating point when seeking an answer for the latter. If we want to implement in a soultion concept that is decentralizable,[14] then every implementing game form can be used to form a decentralized mechanism that has the same number of equilibrium messages. It is then possible, but not a priori certain, that the minimal decentralized mechanism could be expanded to obtain a minimal implementing game form. This is exactly why we have restricted our analysis only to Nash$-$ and dominant strategy implementation.

3.1 The Case of Secure Implementation

A necessary and sufficient condition for secure implementation is given in Saijo et.al. (2007). Goal function must satisfy strategy-proofness (1) and rectangular property (2). The proof is simple and elegant. If these properties hold, the game form (Θ, f) will implement f.[15] But the message space $M = \Theta$ of the direct revelation mechanism can be informationally very inefficient. It is then important to find out how large messages space is needed in a minimal indirect mechanism.

[13] Double implementation is called secure implementation when the solution concepts are Nash- and dominant strategy equilibrium. To better uderstand the origins of this form of implementation, see Repullo (1985).

[14] For ex. the Nash equilibria of the game form (S, g) can be decentralized by the mechanism $\pi = (\mu, S, g)$ with $\mu_j(\theta_j) = \{\boldsymbol{s} \in S \mid g(\boldsymbol{s})\theta_j g(s', \boldsymbol{s}_{-j})$ for all $s'_i \in S_i\}$. All equilibrium concepts are not decentralizable in this fashion, for ex. the cooperative ones like the strong equilibrium.

[15] This is the harder part of implementation proof, since a mechanism has to be invented.

Let f be a goal function, not necessarily securely implementable, and C a rectangular and f-cc covering of Θ with no redundancy. Furthermore, for all $i \in I$, let $C[i]$ be a minimal covering of Θ_i that satisfy the following condition

$$\forall K[i] \in C[i],\ \forall K \in C: \ K[i] \subseteq proj_i K \text{ or } K[i] \cap proj_i K = \emptyset. \tag{7}$$

Assume that $v_i : C[i] \rightarrow M_i$ is a bijective coding function of agent i, and, define a decentralized mechanism $\widehat{\pi}_C = (\mu, M, h)$ as follows

$$\mu_i(\theta_i) = \{\boldsymbol{m} \in M \mid \theta_i \in v_i^{-1}(\boldsymbol{m}_i)\} \ \text{ and } \ h(\boldsymbol{m}) = f(\times_{i \in I}\, v_i^{-1}(\boldsymbol{m}_i)).^{16} \tag{8}$$

The general idea behind this construction is sketched in figure 1 below.

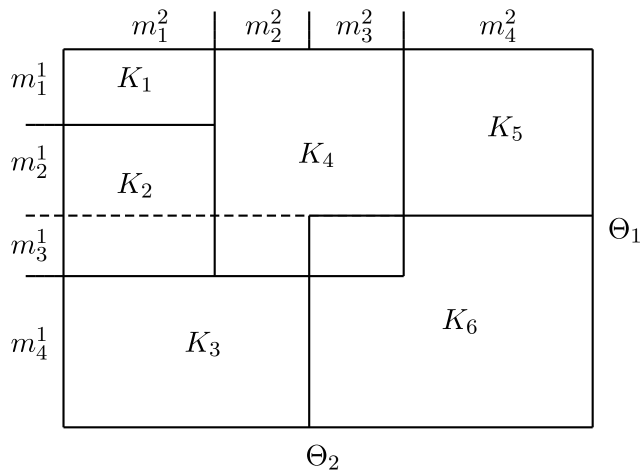

FIGURE 1. Constructing the message space for mechanism (8).

LEMMA 1. Mechanism $\widehat{\pi}_C$ is well-defined and realize f.

PROOF. Notice first that a minimal covering $C[i]$ must exist, since at least Θ_i satisfy the defining condition (7). Assume that $C[i]$ and $C'[i]$ are two different minimal coverings, obtained from the same covering C of Θ.[17] Then

[16]For any $K \subseteq \Theta$, we denote $f(K) = \{f(\theta) \mid \theta \in K\}$.

[17]It is important to realize that we can assume $C[i]$ and $C'[i]$ to be finite without loss of generality. If there are no finite coverings, then every covering is numerably infinite and we can just choose $C[i] = \Theta_i$.

for some $K[i] \in C[i]$ and $K'[i], K''[i] \in C'[i]$ such that $K'[i] \neq K''[i]$, we have $K[i] \cap K'[i] \neq \emptyset$ and $K[i] \cap K''[i] \neq \emptyset$. This implies that also $C'[i] \setminus \{K'[i], K''[i]\} \cup (K'[i] \cup K''[i])$ satisfy condition (7) [18] - a contradiction with the minimality of $C'[i]$. For $\widehat{\pi}_C$ to be well-defined, we still have to show that $\times_{i \in I}\ v_i^{-1}(\boldsymbol{m}_i)$ is included in the same contour set. Choose any $\theta \in \times_{i \in I}\ v_i^{-1}(\boldsymbol{m}_i)$. Let $K \in C$ be such that $\theta \in K$, so that by definition we have $v_i^{-1}(\boldsymbol{m}_i) \subseteq proj_i K$ for all $i \in I$. Since K is rectangular, this implies $\times_{i \in I}\ v_i^{-1}(\boldsymbol{m}_i) \subseteq K$. But C is f-cc by assumption, so $\widehat{\pi}_C$ is indeed well-defined.

The fact that $\widehat{\pi}_C$ realize f can be verified by a direct computation

$$h(\mu(\theta)) = h\left(\bigcap \mu_i(\theta_i)\right) = h(\{\boldsymbol{m} \in M \mid \theta \in \times_{i \in I}\ v_i^{-1}(\boldsymbol{m}_i)\}) = f(\theta),$$

where the last equality must hold since f is well-defined. ■

THEOREM 1. Let f be securely implementable and $\widehat{\pi}_C = (\mu, M, h)$ the mechanism defined by (7) and (8) using a maximally coarse, rectangular and f-cc covering C. The game form $G = (M, h)$ implements f securely.

PROOF. Denote $\Gamma(\theta) = (G, \theta)$. To prove this theorem, we have to verify two things: for every preference profile $\theta \in \Theta$, there exists a message $\boldsymbol{m} \in D(\Gamma(\theta))$ such that $h(\boldsymbol{m}) = f(\theta)$, and, for every message $\boldsymbol{m} \in N(\Gamma(\theta))$ we have $h(\boldsymbol{m}) = f(\theta)$. First, choose $\theta \in \Theta$ and let $\boldsymbol{m}^d \in M$ be such that $\theta \in \times_{i \in I}\ v_i^{-1}(\boldsymbol{m}_i^d)$. We shall prove $\boldsymbol{m}^d \in D(\Gamma(\theta))$. Let's assume the contrary - there exists a message $\boldsymbol{m'} \in M$, such that $h(\boldsymbol{m'}) S\theta_i h(\boldsymbol{m}_i^d, \boldsymbol{m'}_{-i})$ for some $i \in I$. But then, by the definition, we have $h(\boldsymbol{m'}) = f(\theta')$ and $h(\boldsymbol{m}_i^d, \boldsymbol{m'}_{-i}) = f(\theta_i, \theta'_{-i})$ for all $\theta' \in \times_{j \in I}\ v_j^{-1}(\boldsymbol{m'}_j)$, so that $f(\theta') S\theta_i f(\theta_i, \theta'_{-i})$ must hold for some $\theta'_{-i} \in \Theta_{-i}$ [19] - a contradiction with the fact that f is strategy-proof.

To verify the second part, let's assume $\boldsymbol{m} \in N(\Gamma(\theta))$. Since $\boldsymbol{m}_i^d$ is a dominant strategy for every agent $i \in I$, we must have $h(\boldsymbol{m}_i^d, \boldsymbol{m}_{-i}) \theta_i h(\boldsymbol{m})$ for all $i \in I$.

[18] Since $K[i] \cup K'[i]$ and $K[i] \cup K''[i]$ must satisfy condition (7), also $K'[i] \cup K''[i]$ must satisfy it.

[19] Notice that $(\theta_i, \theta'_{-i}) \in v_i^{-1}(\boldsymbol{m}_i^d) \times \left(\times_{j \in I \setminus \{i\}}\ v_j^{-1}(\boldsymbol{m'}_j)\right)$.

As $\boldsymbol{m}$ is Nash equilibrium under θ, this implies $h(\boldsymbol{m}_i^d, \boldsymbol{m}_{-i}) \sim_{\theta_i} h(\boldsymbol{m})$ for all $i \in I$. Thus by the definition , there must exist $\theta' \in \times_{i\in I}\ v_i^{-1}(\boldsymbol{m}_i)$ such that $f(\theta_i, \theta'_{-i}) \sim_{\theta_i} f(\theta'_i, \theta'_{-i})$ for all $i \in I$. Rectangular property then implies $f(\theta') = f(\theta)$, and since $\theta \in \times_{i\in I}\ v_i^{-1}(\boldsymbol{m}_i^d)$, $\theta' \in \times_{i\in I}\ v_i^{-1}(\boldsymbol{m}_i)$, we finally get $h(\boldsymbol{m}) = h(\boldsymbol{m}^d) = f(\theta)$ as required. ■

THEOREM 2. Let f be securely implementable and $\widehat{\pi}_C = (\mu, M, h)$ the mechanism defined by (7) and (8) using a maximally coarse, rectangular and f-cc covering C. Goal function f can not be securely implemented with less than $|M|$ strategies.

PROOF. We shall prove this claim by showing that every agent $j \in I$ needs at least $|M_j|$ strategies. Assume that some agent i could have less strategies in a securely implementing game form $G = (S, g)$. Then by the definition of M, there must exist $K, K' \in C$, $K \neq K'$, such that the same strategy $s^d \in S_i$ is dominant for some $\theta_i \in proj_i K \setminus proj_i K'$ and $\theta'_i \in proj_i K'$. Choose $\theta'_{-i} \in \Theta_{-i}$ in such way that $(\theta'_i, \theta'_{-i}) \in K'$ and let $\boldsymbol{s}^d_{-i}$ be a vector of dominant startegies for θ'_{-i}. Since dominant strategies depend on agent's own preferences only, it must be that $(s_i^d, \boldsymbol{s}^d_{-i}) \in D(\Gamma(\theta_i, \theta'_{-i}))$ and $(s_i^d, \boldsymbol{s}^d_{-i}) \in D(\Gamma(\theta'_i, \theta'_{-i}))$, which implies $f(\theta_i, \theta'_{-i}) = f(\theta'_i, \theta'_{-i})$. Since this holds for any $\theta'_{-i} \in \times_{j\in I\setminus\{i\}} proj_j K'$, the covering $(C \setminus K') \cup (\{\theta_i \cup proj_i K'\} \times_{j\in I\setminus\{i\}} proj_j K')$ is f-cc and rectangular - a contradiction with the assumption that C is maximally coarse. ■

Taken together, theorems 1 and 2 imply we can obtain a minimal implementing game form for a securely implementable goal function by first finding a maximally coarse covering C of Θ and then applying constructions (7) and (8). This result does not seem to depend on the covering used, as long as it is maximally coarse. This is no wonder, since we could easily show that the maximally coarse covering is a unique partition in this case.

As any securely implementable goal function can be implemented by the direct revelation mechanism, only outcomes in the range are needed in the implementing game form *i.e.* outcomes in $Z \setminus f(\Theta)$ are never needed. We can interprete this by saying that secure implementation is context independent, which is in stark contrast with Nash implementation[20] and dominant strategy implementation (example 1 below). In fact, this is the main reason we can use the method of Hurwicz and Reiter (2008) as a starting point in the first place.

EXAMPLE 1. Assume $Z = \{z_1, z_2, z_3\}$ and $\Theta = \{\theta_1, \theta_1'\} \times \{\theta_2\}$. Define the goal function f by $f(\theta_1, \theta_2) = z_1$ and $f(\theta_1', \theta_2) = z_2$, so that $z_3 \notin f(\Theta)$. Define the preferences θ_1, θ_1' and θ_2 by setting

$$z_1 \sim_{\theta_1} z_2,\; z_1 \sim_{\theta_1'} z_2,\; z_1 \sim_{\theta_2} z_2.$$

It is clear that f can not be implemented in dominant strategies using only $f(\Theta) = \{z_1, z_2\}$, since both agent's would be indifferent about playing any strategy. It can still be implemented using $\{z_1, z_2, z_3\}$, at least if

$$z_3 S\theta_1 z_1,\; z_1 S\theta_1' z_3 \text{ and } z_1 S\theta_2 z_3.$$

Assuming that this is indeed the case, the game form in figure 2 below will do the trick.

		Agent 2	
		s_2^1	s_2^2
Agent 1	s_1^1	z_1	z_3
	s_1^2	z_2	z_1

FIGURE 2. A game form implementing f in dominant strategies.

As we noticed earlier, f can not be securely implemented even when using the whole set Z. For example, the game form in figure 2 has a bad Nash equilibrium (s_1^2, s_2^1) for the preference profiles (θ_1', θ_2). ■

Notice that there is absolutely nothing trivial in this example. The fact that all outcomes are indifferent for the agent's involved, does not mean that they

[20] Alternatives in $Z \backslash f(\Theta)$ are very crucial for Nash implementation. See Williams (1984) for more details.

are indifferent from a social point of view. Imagine a situation in which the actions of certain agent's inflict an externality to others. It may well be that these actions are indifferent for the agent's themselves, but the externality caused for the rest of the society is different.

Still, it is not an unproblematic thing to use an implementing game form that does not always give outcomes from the range if equilibrium strategies are not played. As explained in Maskin and Moore (1999), this will raise a question of credibility. If the planner can not fully commit in implementing anything that might rise as an outcome of the game, then agent's can use this to initiate a renegotiation process by playing non-equilibrium strategies. It is then natural to assume that the outcome played before the renegotiation serves as an outside option. This will change the whole nature of the game and a new implementation concept is needed. It would be a lot harder to find a minimal implementing game form in this kind of setting, since a lot more elaborate schemes could be used. We shall therefore simply assume from now on that the goal function is surjective.[21]

3.2 The Case of Dominant Strategy Implementation

As demonstreted in example 1, if the solution concept is dominant strategy equilibrium, we do not necessarily get a minimal implementing game form when applying (7) and (8) with maximally coarse covering. Some strategies may have to be added, since it is clear that the decentralized mechanism produced by this method can always be embedded into a minimal implementing game form.[22] To proceed then, we need to know when goal function is dominant startegy implemented by the direct revelation mechanism. Again, the aswer can be found from Saijo et.al. (2007) - a necessary and sufficient condition is strategy-proofness (1) together with weak non-bossiness (3).

THEOREM 3. Let f satisfy strategy-proofness (1) and weak non-bossiness

[21] A property also known as *citizen sovereignty*.

[22] For a rigorus definition of embedding problem in the case of Nash equilibrium, see Williams (1984).

(3) and let $\widehat{\pi}_C = (\mu, M, h)$ be the mechanism defined by (7) and (8) using a maximally coarse, rectangular and f-cc covering C. Goal function f can not be dominant strategy implemented with less than $|M|$ strategies.

PROOF. We know that for any $\theta \in \Theta$, the vector of messages $\boldsymbol{m}^d \in M$ defined in theorem 1, is a dominant strategy equilibrium and $h(\boldsymbol{m}^d) = f(\theta)$ - only strategy-proofness was used in the proof. Assume then, that $\boldsymbol{m}$ is another dominant strategy equilibrium for θ and let $\theta' \in \times_{i \in I} v_i^{-1}(\boldsymbol{m}_i)$. Notice that $\boldsymbol{m}$ is a dominant strategy equilibrium also for θ'. By the definition of dominant strategy equilibrium we must now have $h(\boldsymbol{m}_i, \boldsymbol{m}'_{-i}) \sim_{\theta_i} h(\boldsymbol{m}_i^d, \boldsymbol{m}'_{-i})$ for all $i \in I$ and all $\boldsymbol{m}'_{-i} \in M_{-i}$, so that by the definition of $\widehat{\pi}_C$ we must also have $f(\theta'_i, \theta''_i) \sim_{\theta_i} f(\theta_i, \theta''_i)$ for all $i \in I$ and all $\theta''_i \in \Theta_{-i}$. Then, weak non-bossiness implies $f(\theta_i, \theta_{-i}) = f(\theta'_i, \theta_{-i})$, and, by the defintion of $\widehat{\pi}_C$ we have $h(\boldsymbol{m}^d) = h(\boldsymbol{m}_i, \boldsymbol{m}^d_{-i})$. But also $(\boldsymbol{m}_1, \boldsymbol{m}^d_{-1})$ must be a dominant strategy equilibrium for θ. We can then replace $\boldsymbol{m}^d$ with $(\boldsymbol{m}_1, \boldsymbol{m}^d_{-1})$ in the previous argument and continue inductively in the number of agents to finally obtain $h(\boldsymbol{m}) = h(\boldsymbol{m}^d)$ as required.

The proof that f can not be implemented with less than $|M|$ strategies is analogous with theorem 2. ■

We shall not try to solve this problem more generally, the task would be by no means trivial. To finish the paper, we'll investigate the set of VCG -mechanisms[23]. It has to be assume that the goal function satisfies weak non-bossiness, if theorem 3 is to be applied. This amounts to a simple restriction on the domain of preferences, which we plainly assume to hold in the next example.

EXAMPLE 2. Let D be a finite set of alternative public decisions. Each agent $i \in I$ posess a utility function $u_i(m, d)$ over money $m \in \mathbb{R}$ and public decision $d \in D$. We assume that this utility function is quasi-linear in money,

[23]Named so after the contributions of Vickrey (1961), Clark (1971) and Groves (1973). This class of mechanisms is essentially unique when the domain of preferences is comprehensive enough. See Groves and Loeb (1975) and Holmström (1979).

so that it can be expressed as

$$u_i(m,d) = m + v_i(d).$$

Here $v_i(d)$ is called agent i's valuation function, and the set of possible utility functions U_i for agent i can be identified by giving the set of possible valuation functions V_i. The cost of producing alternative d is $c(d)$.

The objective is to choose a socially efficient alternative from D *i.e.* an alternative $d^*(\mathbf{v})$ which satisfy

$$d^*(\mathbf{v}) \in \text{argmax}_{d\in D} \sum_{i\in I} v_i(d) - c(d),$$

where $\mathbf{v} = (v_1, \ldots, v_n) \in \times_{i=1}^{n} V_i = V$ is the vector of true valuation functions for the agents. It is assumed that V and D are such that this maximization problem is well-defined. A *VCG -mechanism* is then any function of the form

$$\phi : V \to \mathbb{R}^{n+1}, \;\; \phi(\mathbf{v}) = (d^*(\mathbf{v}), t_1(\mathbf{v}), \ldots, t_n(\mathbf{v})),$$

where the *monetary transfer* $t_i(\mathbf{v}) : V \to \mathbb{R}$ of agent i is determined by the formula

$$t_i(\mathbf{v}) = K_i(\mathbf{v}_{-i}) + \sum_{j\neq i} \mathbf{v}_j(d^*(\mathbf{v})) - c(d^*(\mathbf{v})).$$[24]

It can be easily verified that every member of this family implement the socially efficient public decision in dominant strategies.[25]

Consider the *Pivotal mechanism*, defined by setting $K_i(\mathbf{v}_{-i}) \equiv 0$ for all $i \in I$. For the sake of simplicity, assume that the domain of preferences is dense *i.e* for all $v \in V_i$ and all $\epsilon \in \mathbb{R}_+$, there exists $v' \in V_i$, such that $\mid v'(d) - v(d) \mid < \epsilon$ for all $d \in D$. Notice that VCG -mechanisms implement a cardinal goal function. It is then rather realistic to assume that the planner does not know much about the utility levels.

Fix any $\mathbf{v} \in V$ and denote $\phi(\mathbf{v})_1 = \widehat{d}$. By definition the set

$$V_1^{\epsilon} = \{v' \in V_1 \mid \; |v'(d) - \mathbf{v}_1(d)| < \epsilon \;\; \forall\, d \in D\}$$

[24] Here $K_i(\mathbf{v}_{-i})$ is any function that does not depend on the preferences of agent i.

[25] Only truthfully if weak non-bossiness does not hold.

has infinitely many elements for any $\epsilon \in \mathbb{R}_+$. Furthermore, also the set

$$\text{val}(V_1^\epsilon) = \{v'(d) \ | \ v' \in V_1^\epsilon\}$$

is infinite for all $\epsilon \in \mathbb{R}_+$. Now it is obvious that there has to exist a number δ, such that $\phi(\mathbf{v}_{-1}, V_1^\delta) = \widehat{d}$. This implies that the range of transfer functions $t_2, \ldots, t_n$ must be infinite, since for all $v' \in V_1^\delta$ the change $\mathbf{v} \rightarrow (\mathbf{v}_{-1}, v')$ does not affect the optimal choice, only agent 1's valuation of it.

It is clear from this analysis, even without any of the theorems, that there can not exist any indirect mechanism that is informationally more efficient - infinitely many equilibrium strategies are needed. ■

This example demonstrates what is quite generally the case with cardinal goal functions in economic environments. To obtain a mechanism that implement the given goal in dominant strategies, a transfer scheme that expand the outcome space beyond what would be informationally feasible has to be used. In the previous example an optimal public decision is chosen from a finite set D, but the mechanism ϕ use an infinite outcome space $\{(d^*(\mathbf{v}), t_1(\mathbf{v}), \ldots, t_n(\mathbf{v}) \ | \ \mathbf{v} \in V\}$.

4 Conclusion

We have presented a systematic procedure for constructing a minimal implementing game form in the case of secure- and dominant strategy implementation, the latter when an additional property of weak non-bossiness holds. In more general situations the mechanism found by this method would have to be augmented with additional rows and\or columns. The usfulness of the results depends on the context. Think of an institutional design problem. The direct revelation mechanism can be just a representational tool, since the strategies in the game form must have some kind of a real world counterpart. It may then be costly to introduce new strategies, so it is important to know with how many one can cope. Unfortunately, with many interesting economic mechanisms in cardinal utility environment no reduction in the number of strategies is possible.

References

CLARK, E., H. (1971): "Multipart Pricing of Public Goods". *Public Choice*: **11**: 17-33.

DANILOV, V., SOTSKOV, A. (2002): *Social Choice Mechanisms.* Springer, USA.

DASGUPTA, P., HAMMOND, P., MASKIN, E. (1979): "The Implementation of Social Choice Rules - Some General Results on Incentive Compatibility". *The Review of Economic Studies*, **46**: 185-216.

GROVES, T., LOEB, M. (1975): "Incentives and Public Inputs". *Journal of Public Economics*, **4**: 311-326.

GROVES, T. (1973): "Incentives in Teams". *Econometrica*, **41**: 617-631.

HALL, M. (1948): "Distinct Representatives of Subsets". *Bulletin American Mathematics Society*, **54**: 922-926.

HOLMSTRÖM, B. (1979): "'Groves' Scheme on Restricted Domains". *Econometrica*, **47**: 1137-1144.

HURWICZ, L., REITER, S. (2008): *Designing Economic Mechanisms.* Cambridge University Press, New York, USA.

HURWICZ, L. (1994): "Economic Design, Adjustment Processes, Mechanisms, and Institutions". *Economic Design*, **1**: 1-14.

MASKIN, E., MOORE, J. (1999): "Implementation and Renegotiation". *The Review of Economic Studies* **66**: 39-56.

REPULLO, R. (1985): "Implementation in Dominant Strategies under Complete and Incomplete Information". *The Review of Economic Studies*, **52**: 223-229.

SAIJO, T., SJÖSTRÖM, T., YAMATO, T. (2007): "Secure Implementation". *Theoretical Economics*, **2**: 204-229.

VICKREY, W. (1961): "Counterspeculation, Auctions, and Competitive Seald Tenders". *Journal of Finance*, **16**: 8-37.

WILLIAMS, S. (1984): "Realization and Nash Implementation -Two Aspects of Mechanism Design". *Econometrica*, **54**: 139-51.