On the Communication Requirements of Secure—and Dominant Strategy Implementation

Ville Korpela *†
Public Choice Research Centre,
University of Turku

December 3, 2009
Last Revision: May 20, 2011

Abstract

The literature on communication requirements of goal functions (or social choice rules) mostly assume that agents act sincerely. In the case that incentive compatibility must be met, these results give only a lower bound for the number of messages needed. In this paper we show that the lower bound of sincere behavior is also an upper bound for a wide class of goal functions when the appropriate incentive compatibility requirement is secure- or dominant strategy implementation.

JEL Classification: D71; D78; D82; D83
Keywords: Communication requirements; Decentralized mechanism; Direct revelation mechanism; Implementation; Informational efficiency

1. INTRODUCTION

When the designer of a social choice mechanism has no reason to assume that agents know anything about the environment but merely their own preferences, dominant strategy equilibrium is the appropriate solution con-

---

*E-mail: ville.korpela@utu.fi.
†Many thanks to Hannu Vartiainen for useful discussions. I would also like to thank Klaus Kultti for comments on an earlier draft.
cept to be used in an implementation problem.\footnote{Dominant strategy implementation can be interpreted as a sort of \textit{robust implementation}, see e.g. Bergemann and Morris (2008).} On the other hand, direct revelation mechanism is able to implement truthfully any goal function that is implementable in dominant strategies (Dasgupta et al. 1979), so that implementation problems look almost trivial under this informational assumption. Furthermore, even if truthful implementation is not considered as satisfactory, as there may be other dominant strategy equilibria besides the truth-telling one, an additional property called weak non-bossiness is enough to guarantee that direct revelation mechanism has no bad equilibria (Saijo et al. 2007, Mizukami and Wakayama, 2007).

Unfortunately, this clean view does not address one important practical question. That is, what if the direct revelation mechanism is informationally very inefficient? When mechanism design problem has $m$ possible (social) outcomes, the number of conceivable linear preferences alone is $m!$. Therefore, the number of messages needed in a direct revelation mechanism can, at least potentially, be exponentially larger than the number of messages needed in a minimal indirect mechanism. Even though the Gibbard-Satterthwite-theorem (Gibbard, 1973, Satterthwaite, 1975) \footnote{If the preferences domain is unrestricted (i.e. universal) and the goal function is sovereign (i.e. onto), then strategy-proofness implies that the goal function must be dictatorial.} tells us that the preference domain cannot be this large for every agent, if the goal function is to be implementable at all, it can certainly be many times larger than the number of outcomes. This has been made evident by many interesting dominant strategy implementable goal functions recently presented in the literature: Generalized median voter rules in single-peaked environments (Moulin, 1980), serial cost sharing rules (Moulin and Shenker, 1992) and many others (Saijo et al. 2007, Barberà, 2001).

The main purpose of this paper is to find out how many messages are needed in a minimal indirect mechanism when the relevant incentive constraint is that of secure- or dominant strategy implementation. Quite surprisingly,
it turns out that the minimal number of messages (or strategies) needed in an implementing game form is often exactly the same as the minimal number of messages needed in a mechanism that realizes the goal function in a decentralized way. The literature on communication requirements of goal functions has mostly concentrated on resource allocation processes (e.g. Hurwicz 1972, Osana 1987)\(^3\) or completely neglected the incentive side (e.g. Mount and Reiter 1974, Segal 2007). There are few notable exceptions (e.g. Williams, 1984, Reichelstein and Reiter, 1988), but contrary to this paper, the relevant incentive constraint has been that of Nash equilibrium. Moreover, these papers usually assume some structure on the set of outcomes (manifold or a topological space), whereas we assume no abstract structure at all.

The most common objection raised against indirect mechanisms is that agents will have to learn more complicated rules, instead of simply announcing their own preferences, which they do not necessarily even understand. Consequently, it is not obvious whether anything can be accomplished using indirect mechanisms. Despite this, there are at least two things that suggest the question might be important. First, and foremost, the direct revelation mechanism is mostly just a representational tool. In the complicated real world institutional environment, strategies are not usually preferences themselves (even though they can be). It may then be that the role of complexity and informational efficiency are central in explaining the evolution of these institutions. These are, in fact, some of the questions that we do not yet understand well.\(^4\) Second, sometimes it may be preferable to use indirect mechanisms because then the agents do not need to know their preferences accurately. It may be demanding for an agent to know her preferences in a fine tuned manner and indirect mechanisms can have one strategy that is dominant for an entire class of preferences. Think about the median voter

\(^3\)Mainly the competitive price system.

\(^4\)There does not exist a consensus about the definition of an institution. Are institutions part of the equilibrium concept, or, are they rather rules of the game. See e.g. Hurwicz (1994) and Ostrom (1986).
rule for example.\footnote{See Moulin (1980).} If the number of voters is odd and the domain consists of all possible single-peaked preferences, then this rule is dominant strategy implementable. But the outcome only depends on some features of the preferences, namely the "peak". So the rule would be dominant strategy implementable even if every agent is asked to announce only the "peak". That is, to vote for the most favoured candidate.

The rest of the paper is organized as follows. In section 2 some properties that are needed in characterizing implementable goal functions are given. After this we introduce a method, presented in Hurwicz and Reiter (2008), which can be used to construct a decentralized mechanism with minimal number of messages. Since every game form that implements in Nash- or dominant strategy equilibrium is a decentralized mechanism, it is conceivable that this minimal decentralized mechanism can be expanded to obtain a minimal implementing game form.\footnote{See Williams (1984) for a rigorous definition of embedding problem in the case of Nash equilibrium.} In section 3 we prove that this can indeed be done. More than this, it turns out that the minimal decentralized mechanism of Hurwicz and Reiter (2008) is quite generally also incentive compatible. Finally, section 4 concludes. It is not possible to go through all set theoretic concepts that are needed, so a fair amount of familiarity is assumed.

2. DEFINITIONS, PRELIMINARIES AND NOTATIONAL CONVENTIONS

We denote the set of outcomes by $Z$ and the set of agents by $N = \{1, \ldots, n\}$. A typical element of $N$ is denoted by $i$ or $j$ and a typical element of $Z$ is denoted by $x$, $y$ or $z$, and so forth. We assume that there are at least two agents $n \geq 2$. Every agent $i$ is endowed with a complete and transitive preference ordering $\theta_i$ over the outcomes $Z$ and the set of all admissible preferences orderings for agent $i$ is denoted by $\Theta_i$. The strict part of $\theta_i$ is denoted by $P(\theta_i)$ and the indifference part by $I(\theta_i)$. Then, using the notation $\theta = (\theta_1, \ldots, \theta_n) \in \Theta \equiv \times_{i\in N} \Theta_i$, a goal function is any function...
\( f : \Theta \rightarrow Z \) that associates a unique alternative \( f(\theta) \in Z \) with every profile of preference orderings \( \theta \in \Theta \). A few properties of goal functions will be needed.

**Definition 1 (Strategy-Proofness).** A goal function \( f \) satisfies strategy-proofness if, for all \( \theta \in \Theta \) and all \( i \in N \), there is no \( \theta'_i \in \Theta_i \) such that

\[
f(\theta'_i, \theta_{-i}) = f(\theta_i, \theta_{-i}) \Rightarrow f(\theta'_i) \neq f(\theta_i),
\]

Strategy-proofness is an incentive compatibility condition which says that no agent can gain by lying, assuming that everyone else is speaking the truth.\(^7\)

**Definition 2 (Rectangular Property).** A goal function \( f \) satisfies rectangular property if, for all \( \theta, \theta' \in \Theta \), we have

\[
f(\theta'_i) = f(\theta_i, \theta'_{-i}) \quad \text{for all } i \in N \Rightarrow f(\theta'_i) = f(\theta_i).
\]

Rectangular property is a technical rule that emerges as a necessary condition for secure implementation (Saijo et al. 2007) defined later on.

**Definition 3 (Weak Non-Bossiness).**\(^8\) A goal function \( f \) satisfies weak non-bossiness if, for all \( \theta \in \Theta \), all \( i \in N \), and all \( \theta'_i \in \Theta_i \), we have

\[
f(\theta_i, \theta_{-i}) \neq f(\theta'_i, \theta'_{-i}) \Rightarrow \exists \theta^*_{-i} \in \Theta_{-i} : \neg f(\theta_i, \theta^*_{-i}) = f(\theta'_i, \theta^*_{-i}).
\]

Weak non-bossiness requires, roughly, that whenever an agent can unilaterally change the outcome, this must affect her own utility at least in some cases.

A mechanism, as defined by Hurwicz and Reiter (2008), is a triplet \( \pi = (\mu, M, h) \), where \( M \) is the (common) message space, \( \mu : \Theta \rightarrow M \) is the (group) equilibrium message correspondence and \( h : M \rightarrow Z \) is the outcome function. We say that mechanism \( \pi \) realizes \( f \) if

\[
h \circ \mu(\theta) = f(\theta) \quad \text{for all } \theta \in \Theta,
\]

and call \( \pi \) informationally decentralized, or simply decentralized, if for every

\(^7\)See e.g. Barberà (2001) for more on strategy-proofness.

\(^8\)This condition is called Quasi-Strong-Non-Bossiness in Mizukami and Wakayama (2007). A similar condition has been presented in Satterthwaite and Sonnenschein (1981).
agent \( i \) there exists a correspondence \( \mu_i : \Theta_i \rightarrow M \), such that

\[
\mu(\theta) = \bigcap_{i \in N} \mu_i(\theta_i) \text{ for all } \theta \in \Theta. \tag{2}
\]

This condition states that equilibrium can be obtained in a privacy-preserving way. That is, the message sent by an agent depends on her own preferences only. One should notice that any 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 \( h(\theta) = f(\theta) \). Therefore, the question is not whether a given goal function \( f \) can be realized, but rather, how can it be realized with the minimal number of messages \( |M| \)? This has been solved in Hurwicz and Reiter (2008) and we explain next the constructive method in its essentials.

By a covering of \( \Theta \) we mean a class \( C = \{ K \mid K \subseteq \Theta \} \subseteq 2^\Theta \), such that \( \bigcup_{K \in C} K = \Theta \). Covering \( C \) 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,\(^{10}\) has a system of distinct representatives (SDR).\(^{11}\) That is, a function \( \Lambda : C \rightarrow \Theta \) which satisfies two properties: (1) \( \Lambda(K) \in K \) for all \( K \in C \) and (2) \( K' \neq K'' \) implies \( \Lambda(K') \neq \Lambda(K'') \).

For any covering \( C \) of \( \Theta \), define a correspondence \( \Omega : \Theta \rightarrow C \), \( \Omega(\theta) = \{ K \in C \mid \theta \in K \} \) and let \( v : \Lambda(C) \rightarrow M \) be a bijective (onto) mapping.\(^{12}\)

---

\(^9\)Let us assume that every agent \( i \) acts according to some message verification protocol \( m_{i+1} = g_i(m_t, \theta_i) \), where \( m_t \) is the vector of messages sent at time \( t \) and \( m_{t+1} \) is the reply of agent \( i \) at time \( t + 1 \). With this interpretation, \( \mu \) can be thought of as representing a static equilibrium of a message verification scenario i.e.

\[
\mu(\theta) = \{ m \in M \mid m_i = g_i(m, \theta_i) \text{ for all } i \in N \} = \bigcap_{i \in N} \{ m \in M \mid m_i = g_i(m, \theta_i) \} = \bigcap_{i \in N} \mu_i(\theta_i).
\]

For more details see ex. Hurwicz (1994).

\(^{10}\)Formally, we do not have \( K \subseteq \bigcup_{K' \in C \setminus K} K' \) for any \( K \in C \).

\(^{11}\)A basic theorem on systems of distinct representatives is proven in Hall (1948).

\(^{12}\)We could simply choose a subset of \( \Theta \) as our message space. The main purpose of coding function \( v \) is to make it explicit that agents do not have to transmit a complete characterization of their preferences, only an abstract message.
Theorem 1 (Hurwicz and Reiter, 2008). Let \( C \) be an f-cc and rectangular covering of \( \Theta \) that does not contain redundancy. The mechanism \( \pi_C = (\mu, M, h) \) defined by the following two conditions:

(i) \( \mu = v \circ \Lambda \circ \Omega \), and

(ii) \( h = f \circ v^{-1} \),

will realize \( f \). ■

To complete the description, we need to address two more questions. Namely, can \( \mu \) be decentralized and what are the properties of \( C \) that guarantee the minimality of \( M \)? To this end, define for every agent \( i \in N \), a correspondence \( \Omega_i : \Theta_i \rightarrow C \), \( \Omega_i(\theta_i) = \{ K \in C \mid \theta_i \in \text{proj}_i K \} \).

Theorem 2 (Hurwicz and Reiter, 2008). Condition (2) can be satisfied by choosing \( \mu_i = v \circ \Lambda \circ \Omega_i \) for all \( i \in N \). Hence, mechanism \( \pi_C \) can indeed be decentralized. ■

To answer the second question, we must emphasize that any decentralized mechanism \( \pi \) can be produced with the previous method using some rectangular and f-cc covering of \( \Theta \). That is, for any decentralized mechanism \( \pi \), there exists a rectangular and f-cc covering \( C \) of \( \Theta \), such that \( \pi = \pi_C \). Consequently, it should be obvious that the minimal size of the message space \( M \) is somehow connected with \( C \) being a maximally coarse covering.\(^{14}\) Unfortunately, the relation ”coarsening” is not complete. There can exist, and usually does exist, many maximally coarse coverings with different or equal number of sets.

Luckily, we do not need to dwell on the question of constructing a maximally coarse covering with the minimal number of sets. It turns out that when the

\(^{13}\)The set \( \text{proj}_i K \) is formally defined as \( \{ \theta_i \in \Theta_i \mid (\theta_i, \theta_{-i}) \in K \text{ for some } \theta_{-i} \in \Theta_{-i} \} \).

\(^{14}\)Covering \( C' \) is a coarsening of \( C \) if for every \( K \in C \), there is \( K' \in C' \), such that \( K \subseteq K' \). It is a proper coarsening, if it is a coarsening and \( K \subset K' \) for some \( K \in C \) and \( K' \in C' \). A maximally coarse covering can then be defined as a covering that does not have any proper coarsenings. Notice that a maximally coarse, f-cc and rectangular covering cannot contain redundancy (see Theorems 1 and 2).
goal function $f$ is sufficiently "well-behaved" (e.g. implementable), then the construction of Hurwicz and Reiter (2008), reproduced in Theorems 1 and 2, can be used to build an incentive compatible mechanism with a minimal message space starting from any maximally coarse covering of $\Theta$.  

Before presenting the main results, we need a few definitions to make a clear-cut distinction between realization and an incentive compatible realization. A Game form is a tuple $G = (S, g)$, where $S = S_1 \times \cdots \times S_n$ is the strategy space, the set $S_i$ being a strategy space of agent $i$, and $g : S \rightarrow Z$ is the outcome function. For a fixed preference profile $\theta \in \Theta$, this game form defines a game $\Gamma(\theta) = (G, \theta)$ in normal form. Strategy profile $s^*$ is a Nash equilibrium of the game $\Gamma(\theta)$ if $g(s^*_{-i}, s_i) \theta_i g(s)$ for all $i \in N$ and all $s_i \in S_i$. The set of all Nash equilibria in the game $\Gamma(\theta)$ is denoted by $NE[\Gamma(\theta)]$. We say that game form $G$ implements $f$ in Nash equilibrium if

$$g\left(NE[\Gamma(\theta)]\right) = f(\theta) \text{ for all } \theta \in \Theta.$$  

In a similar way, strategy profile $s^*$ is a dominant strategy equilibrium of the game $\Gamma(\theta)$ if $g(s^*_{-i}, s_i) \theta_i g(s)$ for all $i \in N$ and all $s \in S$. The set of all dominant strategy equilibria in the game $\Gamma(\theta)$ is denoted by $DOM[\Gamma(\theta)]$, and, a game form $G$ implements $f$ in dominant strategies if equation (3) holds when $NE = DOM$. If game form $G$ implements $f$ in Nash- and dominant strategy equilibrium, then following Saijo et al. (2007), we call it securely implementable.  

---

15Hurwicz and Reiter (2008) advance two methods of constructing a maximally coarse covering. The simpler one, called reflexive rectangular method (rRM), works heuristically as follows: Take an arbitrary preference profile $\theta \in \Theta$ and form a largest possible rectangle contained in the same contour set (outcome is not unique). Choose a new preference profile that is outside the class already formed and continue until a covering of $\Theta$ is obtained. The end result will always be a maximally coarse covering in the set of all rectangular and f-cc coverings (but not generally the minimal).

16Double implementation, a term that was coined by Maskin (1979), is called secure implementation if the two solution concepts are Nash- and dominant strategy equilibrium. To better appreciate this implementation form, see Repullo (1985) and Saijo et al. (2007).
3. MAIN RESULTS

Even though the problem of finding an informationally efficient decentralized mechanism and the problem of finding a minimal implementing game form are fundamentally very different, we can still use the former as a starting point when seeking an answer to the latter. If we want to implement goal function \( f \) using a solution concept that is decentralizable,\(^{17}\) then every game form \( G = (S, g) \) that implements \( f \) can be used to form a decentralized mechanism with a (common) message space of cardinality \(|S|\). It is then conceivable, but by no means a priori certain, that the minimal decentralized mechanism can be used to obtain a minimal implementing game form. The main purpose of this section is to show that this can be done, and more than that, fairly easily.

Next we need to complete the construction given in Theorems 1 and 2 to show how the individual message space \( M_i \) can be recovered. Let \( f \) be a goal function and \( C \) a f-cc and rectangular covering of \( \Theta \) that does not contain redundancy. Moreover, for all agents \( i \in N \), let \( C[i] \) be the maximally coarse covering of \( \Theta_i \) that satisfies the following condition: for all \( A \in C[i] \) and all \( K \in C \),

\[
\text{either } A \subseteq \text{proj}_i K \text{ or } A \cap \text{proj}_i K = \emptyset.
\]

(4)

Now let \( v_i : C[i] \to M_i \) be a bijective (coding) function for all \( i \in N \), and, define a decentralized mechanism \( \hat{\pi}_C = (\mu, M, h) \) by the following three rules:\(^{18}\)

\[
(i) \quad M = M_1 \times \cdots \times M_n, \quad \quad (5)
\]

\[
(ii) \quad \mu(\theta) = \bigcap_{i \in N} \mu_i(\theta_i) \text{ and } \mu_i(\theta_i) = \{ m \in M \mid \theta_i \in v_i^{-1}(m_i) \}, \quad \quad (6)
\]

\[
(iii) \quad h(m) = f \left( \times_{i \in N} v_i^{-1}(m_i) \right). \quad \quad (7)
\]

\(^{17}\)The Nash equilibrium correspondence \( f : \Theta \to NE[G(\theta)] \) of game form \( G = (S, g) \) can be decentralized through the mechanism \( \pi = (\mu, S, g) \), where \( \mu_i(\theta_i) = \{ s \in S \mid g(s)\theta_i g(s', s_{-i}) \text{ for all } s' \in S_i \} \). All equilibrium concepts are not decentralizable in this fashion, ex. strong equilibrium.

\(^{18}\)For any \( K \subseteq \Theta \), we denote \( f(K) = \{ f(\theta) \mid \theta \in K \} \) as usual.
The general idea behind this construction is sketched in figure 1 below. Here \( C = \{ K_i \mid i = 1, 2, 3, 4, 5 \text{ or } 6 \} \) and \( M_i = \{ m_{i1}, m_{i2}, m_{i3}, m_{i4} \} \) for agent \( i \in \{ 1, 2 \} \).

\[
\begin{array}{cccc}
\theta_1 & m_{i1}^2 & m_{i2}^2 & m_{i3}^2 & m_{i4}^2 \\
\theta_2 & m_{i1} & m_{i2} & m_{i3} & m_{i4} \\
\end{array}
\]

\( \Theta_1 \)

\( \Theta_2 \)

FIGURE 1. Constructing the message space of mechanism \( \hat{\pi}_C \)

The following important Lemma makes the construction in equations (4)-(7) more transparent.

**Lemma.** Mechanism \( \hat{\pi}_C \) is well-defined and it realizes \( f \).

**Proof.** Notice that a maximally coarse covering \( C[i] \) of \( \Theta_i \) must exist due to the fact that \( \Theta_i \) itself satisfies the defining condition (4). We shall first show that \( C[i] \) is unique. Suppose there are two different maximally coarse coverings of \( \Theta_i \), \( C[i] \) and \( C'[i] \), which both satisfy (4). Then, for some \( A \in C[i] \) and \( A', A'' \in C'[i] \), such that \( A' \neq A'' \), we have

\[
A \cap A' \neq \emptyset \text{ and } A \cap A'' \neq \emptyset.
\]

But then also the class \( (C'[i] \setminus \{ A', A'' \}) \cup (A' \cup A'') \) satisfies condition (4),\(^{19}\) which is a contradiction with the fact that \( C'[i] \) is maximally coarse. For

\(^{19}\)Since \( A \cup A' \) and \( A \cup A'' \) must satisfy condition (4), as \( \theta \in A \cap A' \) and \( \psi \in A \cap A'' \) for some \( \theta, \psi \in \Theta \), also \( A' \cup A'' \) must satisfy it.
$\hat{\pi}_C$ to be well-defined, we still have to show that $\times_{i \in N} v_i^{-1}(m_i)$ is included in the same contour set for all $m \in M$. Choose any $m \in M$ and $\theta \in \times_{i \in N} v_i^{-1}(m_i)$. Let $K \in C$ be such that $\theta \in K$, so that by definition, we have $v_i^{-1}(m_i) \subseteq \text{proj}_i K$ for all $i \in N$. Since $C$ is rectangular, this implies $\times_{i \in N} v_i^{-1}(m_i) \subseteq K$, and since $C$ is f-cc, the set $\times_{i \in N} v_i^{-1}(m_i)$ must be included in the same contour set and hence the outcome function $h$ is well-defined. The fact that $\hat{\pi}_C$ realizes $f$ can be verified by a direct computation:

$$h(\mu(\theta)) = h\left(\bigcap_{i \in N} \mu_i(\theta_i)\right) = h\left(\{m \in M \mid \theta \in \times_{i \in N} v_i^{-1}(m_i)\}\right) = f(\theta),$$

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

The construction given in equations (4)-(7) is important. Hurwicz and Reiter (2008) has shown that the mechanism $\hat{\pi}_C$ has a minimal number of messages $|M_i|$, in the set of all decentralized mechanisms that realize $f$, when $C$ is chosen as a maximally coarse covering with a minimal number of sets. In fact, as we shall see shortly, this construction even preserves incentive compatibility. The following example illustrates the theoretical construction in equations (4)-(7) and gives a premiere on the theorems to come.

**Example 1.** Let $N = \{1, 2\}$, $Z = \{x, y, z\}$ and $\Theta = \{\theta_1, \theta_2, \theta_3\} \times \{\psi_1, \psi_2, \psi_3\}$. The preferences are given in the table below and goal function $f$ is defined in figure 2 below.

<table>
<thead>
<tr>
<th>$\theta_1$</th>
<th>$\theta_2$</th>
<th>$\theta_3$</th>
<th>$\psi_1$</th>
<th>$\psi_2$</th>
<th>$\psi_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$</td>
<td>$x$</td>
<td>$z$</td>
<td>$x$</td>
<td>$z$</td>
<td>$x$</td>
</tr>
<tr>
<td>$y$</td>
<td>$y, z$</td>
<td>$x, y$</td>
<td>$y$</td>
<td>$y$</td>
<td>$y, z$</td>
</tr>
<tr>
<td>$z$</td>
<td></td>
<td>$x$</td>
<td></td>
<td></td>
<td>$x$</td>
</tr>
</tbody>
</table>

TABLE.

It is straightforward to show that the direct revelation mechanism $G = (\Theta, f)$ implements $f$ in dominant strategies. It satisfies strategy-proofness and weak non-bossiness (see Theorem 6). The unique maximally coarse,
rectangular and f-cc covering of $\Theta$ is $C = \{K_1, K_2, K_3, K_4\}$, where

$$K_1 = \{\theta_1, \theta_2\} \times \{\psi_1, \psi_3\}, \quad K_2 = \{\theta_1, \theta_2\} \times \{\psi_2\},$$
$$K_3 = \{\theta_3\} \times \{\psi_1, \psi_3\}, \quad K_4 = \{\theta_3\} \times \{\psi_2\}.$$

Hence, the maximally coarse covering $C[1]$ of $\Theta_1$ is $\{\{\theta_1, \theta_2\}, \{\theta_3\}\}$ and the maximally coarse covering $C[2]$ of $\Theta_2$ is $\{\{\psi_1, \psi_3\}, \{\psi_2\}\}$. Using the construction in equations (4)-(7) gives us the mechanism in figure 3 below.

![Figure 2](image)

FIGURE 2. A diagram of goal function $f$

Again, it is straightforward to show that the game form defined by this mechanism implements $f$ in dominant strategies.\textsuperscript{20} This must be the game

\textsuperscript{20}A game form $G_\pi$ defined by the mechanism $\pi = (\mu, M, h)$ is $G_\pi = (M, h)$. That is,
form with minimal number of strategies, since $f$ cannot be even realized in a decentralized way with less than $|M_1| = |M_2| = 2$ messages. □

In the remainder of this paper we show that the phenomenon in Example 1 is quite general.

3.1 The Case of Secure Implementation

The following theorem presents a necessary and sufficient condition for a goal function $f$ to be securely implementable.

**Theorem 3** *(Saijo et al. 2007, Mizukami and Wakayama, 2007)*. A goal function $f$ is securely implementable if and only if both strategy-proofness and rectangular property hold. ■

The proof of this theorem is simple and elegant. If the two properties hold, then the direct revelation mechanism $G = (\Theta, f)$ implements $f$.²¹ Still, the strategy space $S = \Theta$ of this game form can be informationally very inefficient, which makes it important to find out how many strategies are needed in a minimal indirect game form implementing $f$. The following theorem will answer this question.

**Theorem 4.** Let $f$ be securely implementable and $\hat{\pi}_C = (\mu, M, h)$ the mechanism defined by equations (4)-(7) using a maximally coarse, rectangular and $f$-cc covering $C$. The game form $G = (S, g) = (M, h)$ 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 strategy profile $m \in \text{DOM}[\Gamma(\theta)]$ such that $h(m) = f(\theta)$, and, for every strategy profile $m \in \text{NE}[\Gamma(\theta)]$ we have $h(m) = f(\theta)$. First, choose any $\theta \in \Theta$ and let $m^d \in M$ be such that $\theta \in \times_{i \in N} v_i^{-1}(m^d_i)$. We show that $m^d \in \text{DOM}[\Gamma(\theta)]$. Assume the contrary. That is, there exists a message profile $m' \in M$, such that $h(m')P(\theta_j)h(m^d_j, m'_{-j})$ for some $j \in N$. Since $\hat{\pi}_C$ realizes $f$ in

²¹This is the hard direction in all implementation proofs since some kind of *canonical mechanism* has to be found.
a decentralized way, we have \( h(m') = f(\theta') \) and \( h(m'_j, m'_{-j}) = f(\theta_j, \theta'_{-j}) \) for all \( \theta' \in \times_{i \in N} v^{-1}(m'_i) \), so that \( f(\theta')P(\theta_j)f(\theta_j, \theta'_{-j}) \) must hold for some \( \theta'_{-j} \in \Theta_{-j}^{22} \). This is a contradiction with the fact that \( f \) is strategy-proof and hence \( m^d \in \text{DOM}[\Gamma(\theta)] \).

To verify the second part, let us assume that \( m \in NE[\Gamma(\theta)] \). Since the strategy \( m^d_i \) defined in the previous paragraph is a dominant strategy for every agent \( i \in N \), we must have \( h(m^d_i, m_{-i})\theta_i h(m) \) for all \( i \in N \). As \( m \) is Nash equilibrium under \( \theta \), this implies that \( h(m^d_i, m_{-i})I(\theta_i)h(m) \) for all \( i \in N \). Thus, since \( \pi_C \) realizes \( f \) in a decentralized way, there must exist \( \theta' \in \times_{i \in N} v^{-1}(m_i) \) such that \( f(\theta_i, \theta'_{-i})I(\theta_i)f(\theta'_i, \theta'_{-i}) \) for all \( i \in N \). Now the fact that \( f \) satisfies rectangular property implies \( f(\theta') = f(\theta) \), and since \( \theta' \in \times_{i \in N} v^{-1}(m_i) \), we finally get \( h(m) = f(\theta') = f(\theta) \) as required. ■

This theorem implies the following strong result as a direct corollary.

**Corollary 1.** The minimal number of messages needed for a decentralized realization of a securely implementable goal function is exactly the same as the minimal number of strategies needed to implement it.

**Proof.** The number of strategies needed in implementation is at least as great as the number of messages needed to realize in a decentralized way. Hence, the result follows from Theorem 4. ■

Next we prove this result directly to generate a deeper insight into the equations (4)-(7).

**Theorem 5.** Let \( f \) be securely implementable and \( \pi_C = (\mu, M, h) \) the mechanism defined in theorem 4. Then, \( f \) cannot be securely implemented with less than \(|M|\) strategies.

**Proof.** We prove this claim by showing that every agent \( i \in N \) needs at least \(|M_i|\) strategies. For the sake of contradiction, suppose that agent \( i \) could have fewer strategies in a securely implementing game form \( G = (S, g) \). Then, by the definition of message space \( M \), there must exist \( K, K' \in C \),

\[22\text{Notice that } (\theta_i, \theta'_{-i}) \in v^{-1}(m'_i) \times \left( \times_{j \in N \setminus \{i\}} v^{-1}(m'_j) \right).\]
$K \neq K'$, such that the same strategy $s^d \in S_i$ is dominant for some $\theta_i \in \text{proj}_i K \setminus \text{proj}_i K'$ and $\theta'_i \in \text{proj}_i K'$. Choose $\theta'_{-i} \in \Theta_{-i}$ in such way that $(\theta'_i, \theta'_{-i}) \in K'$ and let $s^d_{-i}$ be a vector of dominant strategies for $\theta'_{-i}$. Since dominant strategies only depend on agents own preferences, it must be that $(s^d_i, s^d_{-i}) \in \text{DOM}[\Gamma(\theta_i, \theta'_{-i})]$ and $(s^d_i, s^d_{-i}) \in \text{DOM}[\Gamma(\theta'_i, \theta'_{-i})]$, which implies $f(\theta_i, \theta'_{-i}) = f(\theta'_i, \theta'_{-i})$. As this must hold for any $\theta'_{-i} \in \times_{j \in N \setminus \{i\}} \text{proj}_j K'$, the covering

$$(C \setminus K') \cup \left(\{\theta_i \cup \text{proj}_i K'\} \times_{j \in N \setminus \{i\}} \text{proj}_j K'\right)$$

is f-cc and rectangular - a contradiction with the assumption that $C$ is maximally coarse. ■

Theorems 4 and 5 do not seem to depend on the covering, as long as it is maximally coarse. We could easily show that this is due to the fact that maximally coarse covering is a unique partition when $f$ is securely implementable.

Notice that any securely implementable goal function can be implemented with the direct revelation mechanism, which means that only outcomes in the range are needed in an implementing game form. That is, 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\(^{23}\) and dominant strategy implementation (Example 2 below). This is the reason that allows us to use the method of Hurwicz and Reiter (2008) as a starting point in the first place.

**Example 2.** Assume that $Z = \{x, y, z\}$ and $\Theta = \{\theta_1, \theta'_1\} \times \{\theta_2\}$. Define goal function $f$ by the rule $f(\theta_1, \theta_2) = x$ and $f(\theta'_1, \theta_2) = y$, so that $z \notin f(\Theta)$. Moreover, define the preferences $\theta_1, \theta'_1$ and $\theta_2$ by setting

$$xI(\theta_1)y, xI(\theta'_1)y \text{ and } xI(\theta_2)y.$$ 

It is obvious that $f$ cannot be implemented in dominant strategies using alternatives only from $f(\Theta) = \{x, y\}$, since both agents would be indifferent between playing any strategy. Still, it can be implemented using

\(^{23}\)See e.g. Williams (1984).
$Z = \{x, y, z\}$, at least if the following preference reversals hold:

$$z P(\theta_1) x, \quad x P(\theta'_1) z \quad \text{and} \quad x P(\theta_2) z.$$ 

Assuming that this is indeed the case, the game form in figure 4 below will implement $f$.

![Figure 4. A game form implementing $f$ in dominant strategies](image)

As a consequence of Theorem 3, $f$ cannot be securely implemented even when using the whole set $Z$. For example, the game form in figure 4 has a bad Nash equilibrium $(s^2_2, s^1_2)$ for the preference profiles $(\theta'_1, \theta_2)$. □

There is nothing trivial in this example. The fact that all outcomes are indifferent for the agents involved, does not mean that they are indifferent from the social point of view (or from the principal point of view). Nonetheless, it is not completely harmless to use game forms that do not give outcomes from the range of a goal function if out of equilibrium strategies are played. As explained in Maskin and Moore (1999), this will inevitably raise some questions of credibility. If the designer cannot fully commit to implement anything that might arise as an outcome of the game, then agents 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 completely change the 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 more elaborate schemes could be used. Leaving this problem behind,
Example 2 makes it very clear that Theorem 4 cannot hold for dominant strategy equilibrium as such.

### 3.2 The Case of Dominant Strategy Implementation

When the solution concept is dominant strategy equilibrium, we do not necessarily get a minimal implementing game form by applying (4)-(7) with maximally coarse covering. Some new strategies may have to be added. To proceed, then, we need to know when our goal function can be implemented in dominant strategies by the direct revelation mechanism.

**Theorem 6** (Saijo et al. 2007). The direct revelation mechanism $G = (\Theta, f)$ implements $f$ in dominant strategies if and only if both strategy-proofness and weak non-bossiness holds. ■

It turns out that Theorems 4 and 5 hold for dominant strategies in the case described by Theorem 6.

**Theorem 7.** Let $f$ satisfy strategy-proofness and weak non-bossiness and let $\hat{\pi}_C = (\mu, M, h)$ be the mechanism defined in theorem 4. The game form $G = (S, g) = (M, h)$ implements $f$ in dominant strategies, and furthermore, $f$ cannot be implemented with less than $|M|$ strategies.

**Proof.** We already know that for any $\theta \in \Theta$, the messages profile $m^d \in M$ that was defined in theorem 4 is a dominant strategy equilibrium and $h(m^d) = f(\theta)$. Only strategy-proofness was used to prove this. Now assume that $m$ is any other dominant strategy equilibrium for $\theta$ and let $\theta' \in i \in N \times v_i^{-1}(m_i)$. Notice that, again by theorem 4, $m$ is a dominant strategy equilibrium also for $\theta'$. By the definition of dominant strategy equilibrium we must then have $h(m_i, m'_{-i})I(\theta_i)h(m^d_i, m'_{-i})$ for all $i \in N$ and all $m'_{-i} \in M_{-i}$, so that by the definition of $\hat{\pi}_C$ we must also have $f(\theta'_i, \theta''_i)I(\theta_i)f(\theta'_i, \theta''_i)$ for all $i \in N$ and all $\theta''_i \in \Theta_{-i}$. Consequently, weak non-bossiness implies $f(\theta_i, \theta_{-i}) = f(\theta'_i, \theta_{-i})$, and, by the definition of $\hat{\pi}_C$ we then have $h(m^d) = h(m_i, m'_{-i})$. But also $(m_1, m'_{-1})$ must be a dominant strategy equilibrium for $\theta$ (since $m_1$ is a dominant strategy for $\theta_1$). We can then replace $m^d$ with $(m_1, m'_{-1})$ in the previous argument and continue.
inductively in the number of agents to finally obtain \( h(m) = h(m^d) = f(\theta) \) as required.

The proof that \( f \) cannot be implemented with less than \(|M|\) strategies is analogous to theorem 5.

Also Corollary 1 generalizes in an obvious manner.

**Corollary 2.** Assume that \( f \) satisfies strategy-proofness and weak non-bossiness. The minimal number of messages needed for a decentralized realization of \( f \) is exactly the same as the minimal number of strategies needed to implement it in dominant strategies.

To conclude the paper, let us take a look at one well-known example from the literature.

**Example 3** *(The Generalized Median Voter Rule in a Single-Peaked Environment).*\(^{24}\) For all \( i \in N \), let \( \Theta_i = U_i \) be the set of all single-peaked preferences on some interval \([a, b] \subseteq \mathbb{R}_+\). The "peak" of the preference \( u_i \in U_i \) is denoted by \( P(u_i) \). It is well-known, that in this environment, the generalized median voter rule

\[
    f(u_1, \ldots, u_n) = \text{median of } \{ P(u_1), \ldots, P(u_n), \alpha_1, \ldots, \alpha_k \},
\]

where \( n \) is odd, \( k < n \) and the numbers \( \alpha_j \in [a, b] \) are "votes" of the society,

is implementable in dominant strategies by the direct revelation mechanism. It is obvious that the strategy space of the minimal implementing game form, in this unrestricted preference domain, should consist of announcing only the "peak". This is exactly what our construction suggests. Even though the maximally coarse coverings \( C \) of \( \Theta \) is a bit complicated to obtain, the only maximally coarse covering \( C[i] \) that satisfies condition (4) must be

\[
    C[i] = \{ A \subseteq U_i \mid u_i, u_j \in A \text{ if and only if } P(u_i) = P(u_j) \}.
\]

\(^{24}\)We do not define all these, by now, well-known concepts here. See e.g. Moulin (1980,1983) or Saijo et al. (2007) for a rigorous definitions. Moulin (1980) attributes the idea of single-peaked -environments dating at least as far as Dummett and Farquharson (1961).

\(^{25}\)Numbers \( \alpha_1, \ldots, \alpha_k \) are sometimes called "phantom" votes.
Note that this need not hold if the preference domain is restricted, but it is rather hard to say anything about this more general case without arbitrarily fixing the domain. □

4. CONCLUDING REMARKS

We have shown that the systematic procedure of Hurwicz and Reiter (2008) for constructing a minimal decentralized mechanism quite often preserves incentive compatibility. This is always so for a securely implementable goal function, but for a goal function implementable in dominant strategies, an additional property called weak non-bossiness in Saijo et al. (2007) is needed. A Simple example from Mizukami and Wakayama (2007) verifies that the assumption of weak non-bossiness is essential. Let $N = \{1, 2\}$, $Z = \{x, y, z\}$ and $\Theta = \{\theta_1, \theta'_1\} \times \{\theta_2, \theta'_2\}$. The preferences are defined in the following way:

$$zP(\theta_1)xP(\theta_1)y, \ xP(\theta'_1)zP(\theta'_1)y, \ zI(\theta_2)xP(\theta_2)y \text{ and } yP(\theta'_2)zI(\theta'_2)x,$$

and goal function $f$ in the following way:

$$f(\theta_1, \theta_2) = z \text{ and } f(\theta_1, \theta'_2) = f(\theta'_1, \theta_2) = f(\theta'_1, \theta'_2) = x.$$

This goal function is implementable in dominant strategies. The indirect game form in figure 5 below verifies this. The only dominant strategy for $\theta_1$ is $s^1_1$, the only dominant strategy for $\theta'_1$ is $s^2_1$, the only dominant strategy for $\theta_2$ is $s^1_2$ and the only dominant strategy for $\theta'_2$ is $s^2_2$. It is easy to verify that the outcome in these equilibria coincide with $f$. Since the direct revelation mechanism $G = (\Theta, f)$ does not implement $f$, and on the other hand the direct revelation mechanism must be inside any game form that implements $f$, the game form in figure 5 must have a minimal number of strategies. Still, it has more strategies than direct revelation mechanism, which is the largest number of messages that is ever needed for realization.

The main idea behind the procedure of Hurwicz and Reiter (2008) is, roughly, to group similar preferences behind the same equilibrium strategy. We have

\[\text{Since } f(\Theta) = \{z, x\}, \text{ agent 2 would be completely indifferent between any two strategies in the direct revelation mechanism.}\]
seen, in Example 3, that the usefulness of this result depends very heavily on the context. That is, on the exact form of the preference domain. Unfortunately, the construction does not give us any means to calculate numerical bounds for the number of strategies needed in a minimal implementing game form, and hence, there is no way to say how much it differs from the order of magnitude of the preference domain. However, the results that we have obtained stand in a stark contrast with the results obtained for other equilibrium concepts, such as Nash equilibrium. Williams (1984) and Reichelstein and Reiter (1988) have shown that the increase in communication requirements can be quite substantial in this case.

<table>
<thead>
<tr>
<th></th>
<th>Agent 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$s^1_2$</td>
</tr>
<tr>
<td>$s^1_1$</td>
<td>$z$</td>
</tr>
<tr>
<td>$s^2_1$</td>
<td>$x$</td>
</tr>
<tr>
<td>$s^3_1$</td>
<td>$x$</td>
</tr>
</tbody>
</table>

FIGURE 5. A game form implementing $f$
References


