Nash Implementation with Little Communication

Ilya Segal

September 14, 2007

Abstract

The paper considers the communication complexity (measured in bits or real numbers) of Nash implementation of social choice rules. A key distinction is whether we restrict to the traditional one-stage mechanisms or allow multi-stage mechanisms. For one-stage mechanisms, the paper shows that for a large and important subclass of monotonic choice rules – called "intersection monotonic" – the total message space size needed for one-stage Nash implementation is essentially the same as that needed for "verification" (with honest agents who are privately informed about their preferences). According to Segal (2007), the latter is the size of the space of minimally informative budget equilibria verifying the choice rule. However, multi-stage mechanisms allow a drastic reduction in communication complexity. Namely, for an important subclass of intersection-monotonic choice rules (which includes rules based on coalitional blocking such as exact or approximate Pareto efficiency, stability, and envy-free allocations) we propose a two-stage Nash implementation mechanism in which each agent announces no more than two alternatives plus one bit per agent in any play. Such two-stage mechanisms bring about an exponential reduction in the communication complexity of Nash implementation for discrete communication measured in bits, or a reduction from infinite- to low-dimensional continuous communication.

1 Introduction

This paper considers the problem of Nash implementation of social choice rules – i.e., designing a mechanism whose set of Nash equilibria equals to (or is a nonempty subset of) the set of socially desirable alternatives. As shown by Maskin [10], any Nash implementable choice rule must satisfy the property of "monotonicity," which, together with the "No Veto Power" (NVP) property, also proves sufficient for Nash implementation with \( N \geq 3 \) agents. The sufficiency part is shown by constructing a "canonical" mechanism to implement the choice rule. The canonical mechanism has been criticized on several grounds, one of which being its enormous communication burden. Indeed, the mechanism
requires each agent to describe the preferences of all the agents (along with an integer), which is impractical in most settings.\footnote{In addition to its communication complexity, the canonical mechanism has also been criticized for other reasons (e.g., see [8]) which are not considered in this paper.} A number of papers have demonstrated that Nash implementation can be achieved with simpler mechanisms, even much simpler in some special settings [6, 9, 11, 16, 13, 2, 19, 21, 20, 3, 17]. However, these papers have not examined the minimal communication cost of Nash implementation, and how it could be achieved or approximated, except in several very special settings.

The present paper offers two contributions to this literature: (1) constructing mechanisms for one-stage Nash implementation at a close to minimal possible communication cost, and (2) constructing multi-stage mechanisms for Nash implementation that have drastically lower communication costs. Our construction is not for all implementable choice rules, but for a large class of them (which includes all specific monotonic choice rules examined previously). Our approach follows the program suggested by Williams [22], which is to relate the message space needed for Nash implementation to that needed for verifying the desirability of an alternative when agents know their preferences privately but can be trusted to report honestly. At first glance, the two problems appear quite different: Nash implementation assumes symmetric information and selfish behavior by agents, while verification assumes private information and honest behavior by agents. Yet, as observed in [12] and [22], Nash implementation is a special case of verification, since each agent’s acceptance of (unwillingness to deviate from) a candidate Nash equilibrium depends only on his own preferences. Thus, the total size of strategy spaces required for Nash implementation is at least as high as that required for verification.\footnote{However, [22] does not attempt a reverse comparison of the communication costs of implementation and verification. Indeed, while the paper shows how to “embed” a verification protocol into an implementation mechanism under some conditions, it admits that “the strategy space in our construction is rather large, relative to the size of the message space [used for verification]. Clearly, if the goal is to devise games with small strategy spaces, then the embedding itself is a key step [...] Within the context of economic theory, this issue has not yet been studied.”}

This paper further exploits the relation between implementation and verification, using concepts and results developed in Segal [18]. The latter paper focuses on a large and important subclass of monotonic choice rules, called “Intersection Monotonic” (IM), and shows that such rules are verified with minimal communication by announcing a “minimally informative verifying budget equilibrium.” Such an equilibrium describes a proposed alternative and offers each agent a budget set - an appropriately restricted subset of alternatives. The fact that the proposed equilibrium is indeed an equilibrium in certain state – i.e., each agent cannot improve over the proposed alternative within his budget set – must verify that the proposed alternative is socially desirable in this state. The budget sets must be chosen carefully: on the one hand, they must be large enough for the equilibrium to achieve verification; on the other hand, they must not be too large so that the equilibrium does not reveal more than necessary about the agents’ preferences. [18] gives an algorithm for construct-
ing such “minimally informative verifying budget equilibria” for any given IM choice rule.

To apply these ideas to Nash implementation, observe that a Nash equilibrium of a mechanism induces for each agent a “budget set” defined as the set of alternatives he could achieve by unilateral deviations, and that the induced budget equilibrium must verify that the outcome is socially desirable. Intuitively, to reduce the strategy spaces in the mechanism, we ensure that its induced budget equilibria are minimally informative verifying equilibria. Formally, we construct a mechanism in which each agent describes a minimally informative verifying budget equilibrium, an alternative, and an integer between 1 and $N$. The outcome function prescribes that if one agent deviates from a unanimous agreement, he can attain any alternative in his budget set as it is described by the other agents. Thus, unanimous agreement is a Nash equilibrium in a given state if and only if the agreement is on a budget equilibrium in this state, and since the agents only announce budget equilibria verifying the choice rule, unanimous-agreement Nash equilibria yield desirable outcomes. To ensure that non-unanimous Nash equilibria do not yield undesirable outcomes, we use the integers announced by the agents to induce a “modulo game”, and make use of the NVP property, just as in the canonical mechanism. The size of each agent’s strategy space in the mechanism is thus the minimal size of the message space needed for verification (which consists of minimally informative verifying budget equilibria), plus the size of the alternative space, plus $\log_2 N$ bits, which is close to that required for verification.3,4,5,6

**Mechanism 1:** The mechanism implements any choice rule that is IC and NVP with $N \geq 3$ agents. Each agent’s strategy space in the mechanism is the minimal message space needed for verification (which consists of minimally informative verifying budget equilibria), plus the space of alternatives, plus $\log_2 N$ bits.

The proposed mechanism is particularly useful in conjunction with Segal’s [18] algorithm for constructing minimally informative verifying budget equilibria. Combined with Theorem 1, this gives us an “almost-minimal” Nash

---

3This result could be interpreted as saying that the “communication cost of selfishness” for Nash implementation of a class of choice rules is rather low. [5] examines the communication cost of selfishness for Bayesian-Nash implementation and ex post implementation.

4The strategy spaces could be reduced further by noting that each agent’s budget set need not be described by every other agent, as long as it is somehow determined from their reports. This can allow substantial reduction when the number $N$ of agents is large (see, e.g., [11] and [13]). We do not consider this further reduction as it is sensitive to the structure of minimally informative verifying budget sets, which in turn depends on the social choice rule at hand.

5The closest approach to ours for strategy space reduction in Nash implementation was suggested by McKelvey [7, Section 5], but he did not relate his strategy spaces to the minimal ones required for implementation, which we are able to do using the characterization of verification for IM choice rules in [18].

6This mechanism can be used for the “weak” versions of the implementation and verification problems, in which it suffices to sustain/verify a nonempty subset of desirable outcomes in any given state, as well as to the “full” version, in which all desirable outcomes must be sustained/verified.
implementation mechanism. In some settings, such a mechanism proves to have a much smaller strategy space than what full description of agents’ preferences or even their lower contour sets at a given point would require.

The second observation of the paper is that while the total size of strategy spaces describes the communication complexity of a one-stage mechanism, it may severely overstate the communication complexity of a multistage mechanism. This is because describing an agent’s (complete contingent) strategy in a multi-stage game may take a lot longer than simply playing the game. In fact, we show that multi-stage mechanisms allow a huge reduction in the communication complexity of Nash implementation. We do this for a subclass of intersection monotonic choice rules, called “CU rules”, which still includes all the monotonic choice rules that have been considered in economics (such as the Pareto rule, approximate Pareto, the core, stable matching, envy-free rules). For such rules, construct

**Mechanism 2**: This 2-stage mechanism implements any choice rule that is CU and NVP with $N \geq 3$ agents. In this mechanism, each agent announces no more than two alternatives plus $N$ bits in any play.

To see the potential communication reduction allowed by multistage mechanisms, recall from [18] that in some social choice problems, the minimally informative verifying budget equilibria must use all possible subsets of alternatives as budget sets. For example, for verifying Pareto efficiency on the universal preference domain, any partition of the set $X$ alternatives among the $N$ agents must be used as a verifying budget equilibrium. Describing such a partition requires sending $\log_2 N$ bits per alternative (to say whose budget set it belongs to), or $|X| \log_2 N$ bits in total, when $X$ is a finite set of alternatives.\(^7\) Any 1-stage Nash implementation mechanism has to have at least as much communication. However, consider a two-stage mechanism in which in the 1st stage each agent announces an alternative, and in equilibrium they announce the same alternative. If one of the agents deviates to a different alternative in the 1st stage, then in the 2nd stage every other agent is asked to say whose budget set the deviation belongs to. Thus, while agents’ complete contingent strategies in the mechanism describe all their budget sets, any play of the mechanism does not do that: instead, each agent describes just one alternative plus (off-equilibrium) $\log_2 N$ bits.\(^8\) Note that it takes only $\log_2 |X|$ bits to describe an alternative, and $\log_2 N$ bits to say whose budget set it belongs to. Thus, when the set of alternatives is large, we have an exponential reduction in communication complexity from the 1-stage mechanism.

In a model with continuous communication, multi-stage mechanisms allow even more drastic reduction from in communication. E.g., consider the prob-

\(^7\)For other problems, the minimally informative budget equilibria may be described more succinctly. E.g., for Pareto efficiency in smooth convex exchange economies, the budget sets are Walrasian and so can be described with linear prices [18].

\(^8\)This is not a complete description of the mechanism - we need to make sure that the agents’ reports about budget sets are consistent with verifying the choice rule, for which purpose announcement of a second alternative off-equilibrium is used.
lem of allocating a divisible good among the agents, compensating them with unlimited transfers of the numeraire. Agents have utilities that are quasilinear in the numeraire and nondecreasing in their consumption of the good. The goal is to find a Pareto efficient (i.e., surplus-maximizing) allocation. As shown by Calsamiglia [1], verifying this goal requires infinite-dimensional communication. In [15], this result is derived from the observation that verifying efficiency requires describing a nonlinear personalized pricing function \([0, 1] \rightarrow \mathbb{R}\) (for divisible good consumption in terms of numeraire) for all agents but one, which is infinite-dimensional (even if arbitrary smoothness is assumed). One-stage Nash implementation is at least as hard. However, we can achieve Nash implementation with a 2-stage mechanism in which in the 1st stage each agent announces an allocation, and if one agent disagrees with the others by announcing a different allocation, the other agents only need to announce supporting personalized prices for this particular allocation, which takes only \(N\) real numbers per agent. So the two-stage mechanism allows a reduction from infinitely-dimensional to low-dimensional communication.

We conclude with a philosophical discussion. While it has long been believed that economic mechanisms must use prices to provide incentives, we showed in [18] that prices must be used to attain many important social goals even if agents are honest but their preference information is private. An intuition for this, based on Hayek (1945), is that to achieve social goals that are “sufficiently congruent” with private goals, communication is minimized by asking individuals to maximize their own preferences within certain “budget sets,” which must be carefully outlined to coordinate their choices and attain the social goals.

The analysis of 1-stage Nash implementation suggests another possible justification for prices: they must be used to create incentives even when information is symmetric. This justification is not valid, however, once multistage mechanisms are allowed. Multistage Nash mechanisms with symmetric information need not reveal supporting prices in any play, and so can have very low communication complexity. In contrast, multistage mechanisms with private information, even when agents are honest, cannot do any better than verification mechanisms, and therefore must still reveal prices, which determines their communication complexity. In brief, price revelation is necessary when information is private (even if agents are honest) but not necessary when information is symmetric (even if agents are selfish). Thus, we conclude that price revelation must arise due to the need to aggregate distributed information, rather than to the need to create incentives for selfish agents.

2 Setup

2.1 The Social Choice Problem

Let \(N\) be a finite set of agents, and \(X\) be a set of social alternatives. (With a slight abuse of notation, the same letter will denote a set and its cardinality when this causes no confusion.) Let \(\mathcal{P}\) denote the set of all preference relations over
set $X$. For any preference relation $R \in \mathcal{P}$ and any alternative $x \in X$, it is convenient to define the relation’s lower contour set at $x$, $L(x, R) = \{ y \in X : xRy \}$. The set of agent $i$’s possible preference relations is denoted by $\mathcal{R}_i \subset \mathcal{P}$. A state is a preference profile $R = (R_1, \ldots, R_N) \in \mathcal{R}_1 \times \cdots \times \mathcal{R}_N \equiv \mathcal{R}$, where $\mathcal{R}$ is the state space, also called preference domain. The goal is to realize a choice rule, which is a correspondence $F : \mathcal{R} \rightarrow X$. For every state $R \in \mathcal{R}$, the rule specifies the set $F(R)$ of “desirable” alternatives in this state.

The following two properties of choice rules, introduced in [10], play a prominent role in Nash implementation:

**Definition 1** Choice rule $F$ is monotonic if $\forall R \in \mathcal{R}$, $\forall x \in F(R)$, and $\forall R' \in \mathcal{R}$ such that $L(x, R_i) \subset L(x, R'_i) \forall i \in N$, we have $x \in F(R')$.

**Definition 2** Choice rule $F$ has No Veto Power if $\forall i \in N, R \in \mathcal{R}, x \in X$ such that $L(x, R_j) = X \forall j \in N \setminus \{i\}$, we have $x \in F(R)$.

The next two properties are introduced in [18]:

**Definition 3** Choice rule $F$ is Intersection-Monotonic (IM) if $\forall R = (R_1, \ldots, R_N) \in \mathcal{R}$, $\forall x \in \bigcap_{R \in \mathcal{R}} F(R)$, and $\forall R' \in \mathcal{R}$ such that $\bigcap_{R_i \in \mathcal{R}_i} L(x, R_i) \subset L(x, R'_i) \forall i \in N$ we have $x \in F(R')$.

**Definition 4** Choice rule $F$ is a Coalitionally Unblocked (CU) choice rule if there exists a blocking correspondence $\beta : X \times 2^N \rightarrow X$ for which

$$F(R) = \{ x \in X : \beta(x, S) \subset \bigcup_{i \in S} L(x, R_i) \forall S \subset N \} \forall R \in \mathcal{R}.$$  

[18] shows that every CU rule is IM, every IM rule is monotonic, and both inclusions are strict. The class of CU rules is still large enough to include all specific monotonic rules that have been considered, such as exact or approximate Pareto efficiency, the core, stable matchings, or envy-free rules.

### 2.2 Nash Implementation

In the Nash implementation problem, all agents observe the state of the world, and they play a Nash equilibrium of the mechanism offered to them.\(^9\)

---

\(^9\)A preference relation $R$ over set $X$ is a binary relation over $X$, with $xRy$ interpreted as “$x$ is weakly preferred to $y$.” It is common to restrict attention to preference relations that are rational, i.e., complete and transitive. Rationality will play no role in the general analysis, but it will be assumed in all the applications.

\(^10\)We want to point out a fundamental difference between the “Nash implementation” and a similar-sounding concept of “ex post Nash” implementation that has been studied recently (e.g., [5]). The former assumes full information, and so it allows both agents’ equilibrium strategies and their deviations to depend on the whole state of the world. The latter assumes private information, and so it requires an agent’s equilibrium strategy to depend only on his own type, while allowing his deviations to depend on the whole state of the world (so that the equilibrium is “robust” to the possibility of his observing other agents’ private information). Thus, the latter concept is much more restrictive than the former (however, papers using the latter concept usually do not rule out bad equilibria, with the exception of [14]).
A mechanism ("game form") $G = (M_1, ..., M_N, h)$ describes a strategy space $M_i$ for each agent and an outcome function $h : \prod_i M_i \to X$. The Nash equilibrium correspondence of the mechanism is given by

$$\nu_G(R) = \{ m \in M : g(m) R_i g(m', m_{-i}) \ \forall i \in N \ \forall m'_i \in M_i \}.$$ 

$\Gamma$ (weakly) implements choice rule $F$ if $\emptyset \neq h(\nu_F(R)) \subset F(R) \ \forall R \in \mathcal{R}$. $\Gamma$ fully implements $F$ if $h(\nu_G(R)) = F(R) \ \forall R \in \mathcal{R}$. 

Note that we can also allow multistage mechanisms, whose normal form can be described as above. Since Nash equilibrium is defined on the normal form, allowing multistage mechanisms does not affect the implementability of choice rules. However, we will see that multistage mechanisms will prove useful in reducing the communication cost of implementation.

### 2.3 Verification

Now we consider the communication problem, in which each agent $i$ observes only his own "type" - in our case, preference relation $R_i$. but can be prescribed to follow an arbitrary strategy, rather than being selfish. Furthermore, we focus on a special kind of communication, called the "verification problem" (or "non-deterministic communication" in computer science). In the verification problem, an omniscient oracle knows the true state $R$ and consequently the desirable alternatives. However, he needs to prove to an ignorant outsider that alternative $x \in F(R)$ is indeed desirable. He does this by publicly announcing a message $m \in M$. Each agent $i$ either accepts or rejects the message, doing this on the basis of his own type $R_i$. The acceptance of message $m$ by all agents must prove to the outsider that alternative $x$ is desirable.

Formally, verification can be defined as follows:

**Definition 5** A verification protocol is a triple $\Gamma = (M, \mu, h)$, where

- $M$ is the message space,
- $\mu : \mathcal{R} \to M$ is the message correspondence satisfying Privacy Preservation:
  $$\mu(R) = \cap_{i \in N} \mu_i(R_i) \ \forall R \in \mathcal{R}, \text{ where } \mu_i : \mathcal{R}_i \to M \ \forall i \in N,$$
- $h : M \to$ is the outcome function.

$\Gamma$ weakly verifies choice rule $F$ if $\emptyset \neq h(\mu(R)) \subset F(R) \ \forall R \in \mathcal{R}$.

$\Gamma$ (fully) verifies $F$ if $h(\mu(R)) = F(R) \ \forall R \in \mathcal{R}$.

While the verification problem is patently unrealistic, it is useful to consider. The key reason to consider it that any multi-stage communication protocol can be represented as a weak verification protocol by letting all the messages be sent
by the oracle instead of the agents, and having each agent accept the message sequence if and only if all the messages sent in his stead are consistent with his strategy given his type. The oracle’s message space \( M \) is thus identified with the set of the protocol’s possible message sequences (terminal nodes). Therefore, the communication cost of weak verification bounds below the communication cost of computing an outcome in the choice rule [7, Chapter 2]. The lower bound is tight in some cases but weak in some other cases, where communication requires a lot more than verification.

In addition, verification gives a lower bound on the one-stage Nash implementation problem, since any Nash implementation protocol \( G = (M_1, ..., M_N, h) \) can be viewed as a verification protocol \( \Gamma = (M_1 \times, ..., M_N, h, \nu_G) \). Indeed, note that the Nash equilibrium correspondence \( \nu_G \) by construction satisfies Privacy Preservation: \( \nu_G(R) = \bigcap \nu_G^i(R_i) \), where \( \nu_G^i(R_i) = \{m \in M : g(m) R_i g(m', m_{-i}) \forall m' \in M_i\} \) describes the best-response correspondence of agent \( i \) and so depends only on this agent’s preferences \( R_i \).

We will show in this paper that the relation between verification and Nash implementation is quite tight (unlike the relation between verification and communication). Intuitively, this is because in the implementation problem each agent has full information and so can send the oracle’s message by himself, as long as he is incentivized to do so.

### 2.4 Measures of Communication Cost

#### 2.4.1 Verification Protocols

In the case of discrete communication, the communication cost is defined as “communication complexity,” which is the number of bits needed to encode the messages [7]. In the case of verification, the oracle needs \( \log_2 |M| \) bits to encode his message from \( M \). The minimal communication complexity of a verification protocol offers a lower bound on the “communication complexity” without an oracle [7].

For continuous communication, the communication cost can be naturally defined as the “total dimension” of the messages sent. However, for a meaningful concept of dimension, we need to rule out “smuggling” a multidimensional message in a single dimension with a 1-to-1 function such as the inverse Peano function. For this purpose, the dimension of the message space must be defined in relation to the “meaning” of the messages, given by the message correspondence \( \mu \). We assume that the state space \( R \) is a metric space with a metric \( \rho \), and propose the following way to measure the dimension of a verification protocol:

**Definition 6** Consider verification protocol \( \Gamma \). Let \( N_\varepsilon(\mu) \) be minimal cardinality of a subset of \( \{\mu^{-1}(m)\}_{m \in M} \) that is an \( \varepsilon \)-cover of \( R \). \( (A \subset 2^R \text{ is an } \varepsilon \text{-cover of } R \text{ if for all } R \in R \text{ there exist } a \in A \text{ and } R' \in A \text{ s.t. } \rho(R, R') \leq \varepsilon.) \) Define \( \dim \mu = \limsup_{\varepsilon \to 0} \log_2 N_\varepsilon(\mu) / \log_2 (1/\varepsilon) \).
This concept is similar to ball-covering dimension [4]. Interpretation: this measure describes the difficulty of discrete approximation: \( \log_2 |M_\varepsilon(\Gamma)| \) is how many bits are needed to approximate state of the world within \( \varepsilon \) using a subset of the messages in \( \Gamma \).\(^{12}\)

TO BE COMPLETED

2.4.2 Implementation Mechanisms

An important issue in defining the communication cost of a mechanism is whether we want to count only the message profiles sent in equilibrium or all possible message profiles. If we only want to count the equilibrium message profile, then we can simply think of Nash implementation as a special case of verification, in which off-equilibrium messages could simply be eliminated. However, for Nash implementation, we cannot just eliminate off-equilibrium messages, since this would create undesirable Nash equilibria. If we believe that the mechanism should be able to also process off-equilibrium messages, all possible message profiles should be counted.

In a discrete one-stage mechanism, each agent \( i \) needs \( \log_2 |M_i| \) bits to encode his strategy from \( M_i \), and so the total communication complexity of the game can be defined as \( \sum_i \log_2 |M_i| = \log_2 \prod_i M_i \). For a continuous one-stage mechanism \( \Gamma \), we can define the dimension of agent \( i \)'s message space as \( \dim \mu_i \), and the total dimension of the mechanism as \( \sum_i \dim \mu_i \).

For a multi-stage mechanism whose normal form is \( \Gamma \), the communication cost could be drastically lower. For example, consider the discrete case, in which the agents’ moves in the extensive-form game are announcing bits. Suppose that the maximum number of bits sent in the game is \( d \). This game can have up to \( 2^d - 1 \) decision nodes, and describing agents’ contingent strategies in it requires 1 bit per decision node, and so up to \( 2^d - 1 \) bits total. Thus, the communication complexity of describing strategies in a multistage game can be exponentially higher than that of playing the game. In a continuous mechanism, the increase can be even more drastic: even a very simple extensive-form mechanism can have an infinite-dimensional strategy space. E.g., consider the two-stage mechanism in which first agent 1 announces \( x_1 \in [0,1] \) and then agent 2 announces \( x_2 \in [0,1] \). Agent 2’s strategy in this mechanism is an arbitrary function \([0,1] \to [0,1]\), and so it is is infinite-dimensional. In contrast, only two numbers are communicated in any play of the mechanism. While these examples are abstract, we will construct examples of similar reduction in the communication complexity of Nash implementation.

\(^{12}\)This dimension concept is similar to the concept of protocol dimension defined in [18]. By definition, the former cannot exceed the latter, but the “fooling set” argument in [18] applies to this concept as well, and so all the lower bounds in [18] apply to this concept as well. The key property of this concept for our purposes is that it is not increased when we replace one message with another that is less informative, i.e., \( \mu^{-1}(m) \subset \mu^{-1}(m') \).
2.5 Role of Budget Equilibria

A famous economic example of verification is Walrasian equilibrium. The role of the oracle is played by the “Walrasian auctioneer,” who announces the equilibrium prices and allocations. Each agent accepts the announcement if and only if his announced allocation constitutes his optimal choice from the budget set given by the announced prices. This concept can be generalized to that of a “budget equilibrium,” in which the oracle’s message consists of a proposed alternative $x \in X$ and a budget set $B_i \subset X$ for each agent $i$. Each agent $i \in N$ accepts message $(B_1, \ldots, B_N, x)$ if and only if there is no alternative in his budget set $B_i$ that he strictly prefers to the proposed alternative $x$. $(B_1, \ldots, B_N, x)$ is a budget equilibrium in state $R \in \mathcal{R}$ if it is accepted by all agents in this state.\(^{13}\) Formally, the budget equilibrium correspondence $E : \mathcal{R} \rightarrow 2^{XN} \times X$ is described as

$$E(R) = \{(B, x) \in 2^{XN} \times X : B_i \subset L(x, R_i) \ \forall i \in N\}.$$ 

$E$ satisfies Privacy Preservation because each agent’s acceptance depends only on his own preferences.

The oracle’s message space $M$ in a budget protocol is a collection of budget equilibria that he is allowed to announce, and the outcome function simply implements the proposed alternative:

**Definition 7** Protocol $(M, \mu, h)$ is a budget protocol if $M \subset 2^{XN} \times X$, $\mu(R) = E(R) \cap M \ \forall R \in \mathcal{R}$, and $h(B, x) = x \ \forall (B, x) \in M$.

Clearly, the space of budget equilibria used is important for whether the protocol verifies $F$. In particular, if it does, it can only use budget equilibria of the following kind:

**Definition 8** $(B, x) \in 2^{XN} \times X$ is a budget equilibrium verifying $F$ if $\mu^{-1}(B_1, \ldots, B_N, x) \subset F^{-1}(x)$.

Furthermore, to reduce the size of the message space, for IM choice rules we can restrict attention to the following budget equilibria:

**Definition 9** For an IM choice rule $F$ that is defined on all $R$, $(B, x) \in 2^{XN} \times X$ is a minimally informative budget equilibrium verifying $F$ if for some $R \in \mathcal{P}^N$,

$$B_i = L(x, R_i) = \bigcap_{R'_i \in R_i : \exists x \in F(R'_i, R_{-i})} L(x, R'_i) \ \forall i \in N.$$

\(^{13}\)A number of related concepts have been suggested, including “social equilibrium” [?], “social situations” [?], “effectivity functions” [?], “effectivity forms” [?], “opportunity equilibrium” [?], “attainable sets” [3], and “interactive choice sets” [?]. However, all these papers have motivated the concept by incentive compatibility, rather than deriving it from communication among sincere agents (see Section ?? below for a more detailed comparison).
In [18], this concept is not defined but derived by constructing messages that verify $F$ while revealing minimal information about the state of the world. When $F$ is IM, these messages can be characterized as budget equilibrium messages of the form $1$.\footnote{McKelvey [11] offers a similar concept of “$F$-minimal states”, but without restricting $F$ to be IM, they don’t have the simple characterization of 1, and need not correspond to minimally informative messages verifying $F$.} Furthermore, [18] offers a simple mechanism for deriving these messages.

Letting $E_F$ be the space of all minimally informative budget equilibria verifying $F$, the following proposition follows from [18]:

**Proposition 10** For an IM choice rule $F$, there exists a budget equilibrium protocol whose message space is a subset of $E_F$ that minimizes the communication cost among all protocols verifying $F$. The same is true for weakly verifying $F$.

### 3 One-Stage Mechanisms

Recall that Nash implementation protocol can be viewed as a verification protocol. (Furthermore, it can be viewed as a budget protocol, with message space $M = \{B_1(m), \ldots, B_N(m), g(m)\}_{m \in M^i}$, where $B_i(m) = \{g(m'_i, m_{-i}) : m'_i \in M^i\}$.) Thus, we have the following

**Lemma 11** The minimal total size of strategy spaces required for (full/weak) Nash implementation is at least as high as the minimal size of the message space required for (full/weak) verification.

Here we also find an upper bound for Nash implementation of IM choice rules, that is not too much higher when the number of agents and the size of the alternative space are small relative to the space of the budget equilibria that have to be used. The upper bound is reached by the following mechanism: let $E \subset 2^N \times X$ be a space of budget equilibrium messages.

**Mechanism 1:**

Each agent $i$’s strategy space is $M_i = \{(E_i, y_i, l_i) : E_i \in E, y_i \in X, l_i \in \{1, \ldots, N\}\}$.

The outcome function $h$ is described as follows:

1. If $E_1 = \ldots = E_N = (B_1, \ldots, B_N, x)$, and $y_1 = \ldots = y_N = x$, implement $x$.
2. If $E_j = (B_1, \ldots, B_N, x)$ and $y_j = x$ for all $j \neq i$, and $y_i \notin B_i$ implement $x$.
3. If $E_j = (B_1, \ldots, B_N, x)$ and $y_j = x$ for all $j \neq i$, and $y_i \in B_i$, implement $y_i$.
4. Otherwise implement $y_i$ for $i = \sum_j l_j \text{ mod } N + 1$
Proposition 12. Suppose choice rule $F$ is IM and NVP, and $N \geq 3$. Then, letting $E$ be a minimal space of minimally informative budget equilibria needed for weakly/fully verifying $F$, Mechanism 1 weakly/fully implements $F$.

Proof. For definiteness, we focus on full implementation and verification; the proof for the weak case is similar. The result follows from three simple claims:

Claim 1: If $x \in F(R)$, then all agents announcing the same budget equilibrium $(B_1, \ldots, B_N, x) \in E$ that is an equilibrium in state $R$ and $y_1 = \ldots = y_N = x$ is a NE in state $R$. Indeed, agent $i$ can only deviate and change the outcome if he announces $y \in B_i$ and gets to case 2, but he would not want to do since $(B_1, \ldots, B_N, x)$ is a budget equilibrium in state $R$.

Claim 2: Any Case-1 NE in state $R$ implements $x \in F(R)$. Indeed, if all agents announce $(B_1, \ldots, B_N, x) \in E$, then this must be a budget equilibrium in state $R$, for otherwise an agent $i$ would prefer to deviate to case 2 and get her preferred outcome in $B_i$. Since by assumption any budget equilibrium in $E$ verifies $F$, we must have $x \in F(R)$.

Claim 3: Any NE of the form other than Case 1 implements $x \in F(R)$. Indeed, from all message profile that do not fall in Case 1, all agents except (possibly) one could deviate to Case 4 to get their best outcome in $X$. By NVP, this implies if we have a NE, $x \in F(R)$.

Recall from Proposition 10 that the verification cost of an IM choice rule $F$ is exactly the minimal size of a space of minimally informative budget equilibria needed for weakly/fully verifying $F$. Thus, combining Proposition 12, and examining the size of strategy spaces in Mechanism 1 yields

Corollary 13. Suppose choice rule $F$ is IM and NVP, and $N \geq 3$. Then for discrete communication, we can (fully/weakly) Nash implement $F$ with a one-stage mechanism in which the number of bits sets by each agent is the minimal number of bits needed for (fully/weakly) verifying $F$ plus $\log_2 |X| + \log_2 |N|$ bits. For continuous communication, we can (fully/weakly) Nash implement $F$ with a one-stage mechanism in which the dimension of each agent’s strategy space is the minimal message space dimension needed for (fully/weakly) verifying $F$ plus the dimension of $X$.

4 Multistage Mechanisms

Considering multistage games allows substantial savings in communication. The insight is that while the agents’ strategies in the mechanism must still describe supporting budget sets (as is the case in any verification mechanism), these budget sets need not be described in any single play of the multistage mechanism. Instead, it suffices that if a single agent deviates, the others state whether the deviation belongs to his budget set. The agents’ complete contingent strategies
(contingent on all possible deviations) would still describe all the budget sets, but these strategies would not be revealed in any given play.

The trickiest part of the argument is making sure that agents can only use strategies that correspond to budget equilibria verifying the choice rule. (Recall that if the budget sets are too small, the equilibrium would not verify the choice rule, and we would not have realization.) We are able to accomplish this for the class of CU choice rules defined in Section 2. For this purpose, we use the observation that the CU choice rule given by a blocking rule is fully verified with the budget protocol using budget equilibria $(B_1, ..., B_N, x)$ satisfying

$$\bigcup_{i \in T} B_i \subset \beta(x, T) \quad \text{for all } T \subset N.$$ \hfill (*)

Indeed, if $(B_1, ..., B_N, x)$ is a budget equilibrium in state $R$ and satisfies condition (*), we must have $\bigcup_{i \in T} L(x, R_i) \subset \beta(x, T)$ for all $T \subset N$, and therefore $x \in F(R)$. Furthermore, in any state $R$ for any $x \in F(R)$, the equilibrium $(L(x, R_1), ..., L(x, R_N), x)$ satisfies condition (*).\textsuperscript{15}

We can ensure that an agent’s strategy corresponds to a budget equilibrium of the form (*) by requiring that for any possible deviation $x'$, the agent must place $x'$ into the budget sets of a sufficiently large group $S \subset N$ of agents so that $S$ that intersects any $T \subset N$ such that $x' \in \beta(x, T)$. Furthermore, we can ensure that all agents’ strategies correspond to the same budget sets by rewarding each agent for proving that other agents disagree on the placement of alternative $x'$ in budget sets, by announcing $x'$.

Formally, consider the following 2-stage mechanism, which has imperfect information: the only information the agents observe in the 2nd stage about each other’s 1st stage reports are the public “revelations” by the mechanism.

**Mechanism 2.**

**Stage 1.** Each agent $i$ announces $x_i \in X$

- If $x_1 = ... = x_N = x$, implement $x$.
- If, for some $i \in N$, $x_j = x$ for all $j \not= i$, and $x_i = x' \not= x$, then the mechanism publicly reveals “a,” reveals $x'$ (does not reveal $i$), goes to Stage 2 case (a).
- If neither of the above, the mechanism reveals “b,” goes to Stage 2 case (b).

**Stage 2**

**Case (a).** Agent $i$ announces $y \in X$; each agent $j \not= i$ announces $S_j \in \Sigma(x, x')$, where

$$\Sigma(x, x') = \{ S \subset N : \forall T \subset N, x' \in \beta(x, T) \Rightarrow S \cap T \not= \emptyset \}.$$  

\textsuperscript{15}Budget equilibria of the form (*) are minimally informative equilibria verifying $F$ on the universal preference domain, but not necessarily on a restricted domain. We are not looking for minimally informative verifying equilibria in this section, because we are able to have a low communication cost in a multistage mechanism anyway.
Proposition 14

If $S_j = S$ for all $j \neq i$ and $i \in S$, implement $x'$.

(2a-ii) If $S_j = S$ for all $j \neq i$ and $i \notin S$, implement $x$.

(2a-iii) If neither of the above, implement $y$.

Case (b). Each agent announces $l_i \in \{1, \ldots, N\}$, implement $x_i$ for

$$i = \left(\sum_j l_j\right) \mod N + 1.$$

Proposition 14 If $F$ is a CU choice rule described by the blocking rule $\beta$, $F$ satisfies NVP, and $N \geq 3$, then Mechanism 2 fully Nash implements $F$.

Proof. Agent $i$'s strategy in the mechanism can be described as $(x_i, \sigma_i, y_i, l_i)$, where $x_i \in X$ is the agent's 1st-stage announcement, $\sigma_i : X \setminus \{x_i\} \rightarrow 2^N$ describes his announcement $\sigma_i(x') \in \Sigma(x_i, x')$ in Stage 2 case (a) if he announced $i$ and someone else deviated to $x'$ in Stage 1, $y \in X$ is his announcement in Stage 2 case (a) if he himself was the deviator in stage 1, and $l_i \in \{1, \ldots, N\}$ is his announcement in Stage 2 case (b).

We can interpret $\sigma_i(x')$ as the set of agents whose deviations to $x'$ are "approved" by agent $i$. The function $\sigma_i$ can be equivalently described by defining for each agent $j$ the budget set $B_j = \{x' : x' \in X : \sigma_i(x') \cup \{x'\}\}$ - the set of agent $j$'s deviations that are "approved" by agent $i$. The restriction $\sigma_i(x') \subset \Sigma(x_i, x')$ for all $x' \in X$ is equivalent to requiring that $(B_1, \ldots, B_N, x')$ satisfy condition (*). Thus, we will describe agent $i$'s strategy as $(x_i, B_1, \ldots, B_N, x', l_i)$ satisfying condition (*) (from which we can deduce for each $x'$, $\sigma_i(x') = \{j \in N : x' \in B_j\} \subset \Sigma(x_i, x')$).

Now, the result is proved with the following three claims:

Claim 1: If $x \in F(R)$, then $(x_i, B_1, \ldots, B_N, l_i) = (x_i, L(x, R_1), \ldots, L(x, R_N), l_i)$ is a NE in state $R$.

Proof: Agent $i$ can deviate to change the outcome only by going to case (2a-i), where he can only get outcomes in $L(x, R_i)$.

Claim 2: Each NE that stops in Stage 1 yields $x \in F(R)$.

Proof: Suppose $(x, B_1, \ldots, B_N, y_i, l_i)_{i \in N}$ is a NE. (1) If there exist $x' \neq x$, $j, k, i$ such that $x' \in B_i \setminus B_k$, then each agent except possibly one (namely, either agent $j$ or agent $k$ if all the others agree on the budget sets) could get to case 2a-iii by announcing $x'$, and then get any preferred outcome $y \in X$. Hence, by NVP, $x \in F(R)$. (2) If, on the contrary, for each $i$,  

---

16Strictly speaking, agent $i$ can also use strategies that condition $y_i$ and $l_i$ on his own 1st-stage report, but such strategies are strategically equivalent in the normal-form game to ones that do not have such conditioning, and so we do not consider them for notational simplicity.
Claim 3: Each NE that goes to stage 2 is in $F(R)$.

Proof: each agent except one (in case a) or each agent (in case b) can deviate to induce case b and get any outcome in $X$, hence by NVP $x \in F(R)$.

4.1 Examples of communication reduction

Since in any play of Mechanism 2, at most $N + 1$ alternatives plus $N^2$ bits are announced by the agents, this offers a potentially huge reduction in communication relative to 1-stage implementation mechanisms, in which, as we know, budget sets - subsets of alternatives - have to be described. Here we offer two examples of such reduction - one with discrete and the other with continuous communication.

4.1.1 Discrete communication: exponential reduction

It is known in the communication complexity literature [7] that going from 1-stage to multistage games we could have an exponential reduction in the communication complexity measured in bits. Using Mechanism 2, we can see that such exponential reduction can be achieved for the Nash implementation problem.

For example, take the Pareto efficient choice rule:

$$F(R) = \{x \in X : X = \cup_{i \in N} L(x, R_i)\} \forall R \in \mathcal{R}.$$  

and consider the universal preference domain. For this domain, the minimally informative verifying budget equilibria are partitional equilibria supporting $x$, i.e., a budget equilibrium $(B, x)$ in which $x \in \cap_{i \in N} B_i$, and $(B_1, \ldots, B_N)$ forms a partition of $X \setminus \{x\}$. Furthermore, any partitional equilibrium must be used for full verification of $F$. Indeed, for every partitional equilibrium $(B, x)$ we can find a state $R \in \mathcal{P}^N$ in which $L(x, R_i) = B_i$ for all $i$, and thus $x \in F(R)$. Then $(B, x)$ is a unique partitional equilibrium verifying $x$ in state $R$.

There are $X N^{X-1}$ partitional equilibria (choose $x \in X$, and allocate each of the alternatives in $X \setminus \{x\}$ to a budget set). Taking the binary logarithm, we obtain that full verification requires exactly $\log_2 X + (X - 1) \log_2 N$ bits. When $X$ is large, this cost is asymptotically proportional to $X$, which is exponentially larger than that of simply naming an alternative (which takes $\log_2 X$ bits). In fact, the cost is comparable to that of full revelation of an agent’s preferences, which is asymptotically equivalent to $\log_2 X! \sim X \log_2 X$ bits as $X \to \infty$.

Compare this with the 2-stage Mechanism 2, whose communication complexity is $(N + 1) \log_2 X + N^2$ bits - exponentially smaller. Intuitively, the exponential savings arises because instead of describing budget sets, we simply allocate a given alternative to a budget set in any play of the mechanism.
Note that we can’t have more than exponential reduction in communication complexity, because every extensive-form game can be converted into a 1-stage normal form with at most exponential increase in communication, and we already know that 1-stage Nash implementation cannot be easier than realization.

4.1.2 Continuous communication: from infinite- to low-dimensional

Consider the problem of Pareto efficiency with quasilinear preferences.

Suppose that we want to allocate a unit of a divisible good among \( N \) agents, using also numeraire transfers. Thus, \( X = \{(k, t) : k \in K, t \in \mathbb{R}^N : \Sigma_i t_i = 0\} \) where \( K = \{k \in \mathbb{R}^N_+ : \Sigma_i k_i = 1\} \) is the set of possible allocations of the divisible good, and \( t \in \mathbb{R}^N \) denotes balanced-budget numeraire payments to the agents. Thus, the alternative space is \( 2(N-1) \)-dimensional.

Agents’ preferences are described by quasilinear utility functions of the form \( u_i(k_i) + t_i \), where \( u_i \) can be arbitrary nondecreasing functions. Calsamiglia [1] showed that the verification problem in this model requires infinite-dimensional communication, even with two agents, and even if their utility functions are known to be smooth. Segal [18] rederived the result using the fact that any verification protocol even with two agents must to reveal an infinite-dimensional nonlinear price function \([0, 1] \rightarrow \mathbb{R}\) for consumption of the good for one agent in terms of the numeraire. This implies that the one-stage Nash implementation problem also requires infinite-dimensional communication.

However, for multistage Nash implementation, we can use Mechanism 2, in which only \( N + 1 \) alternatives are described, which means a total of \( (N + 1) \cdot 2(N-1) \) real numbers (sending bits is “free” relative to the real numbers). Intuitively, instead of describing numeraire prices for all possible allocations of the divisible good, in any play of Mechanism 2 the agents only need to describe for one deviation who can afford this deviation under the prices. Thus, we only learn about the prices for one allocation instead of all possible allocations from \( K \), which makes the communication low-dimensional instead of infinitely-dimensional.

References


