Mount, Kenneth; Reiter, Stanley

Working Paper

The Informational Size of Message Spaces

Discussion Paper, No. 3

Provided in Cooperation with:
Kellogg School of Management - Center for Mathematical Studies in Economics and Management Science, Northwestern University

Suggested Citation: Mount, Kenneth; Reiter, Stanley (1973) : The Informational Size of Message Spaces, Discussion Paper, No. 3, Northwestern University, Kellogg School of Management, Center for Mathematical Studies in Economics and Management Science, Evanston, IL

This Version is available at:
https://hdl.handle.net/10419/220363

Northwestern University
2001 Sheridan Road 580 Leverone Hall Evanston, IL 60208-2014 USA

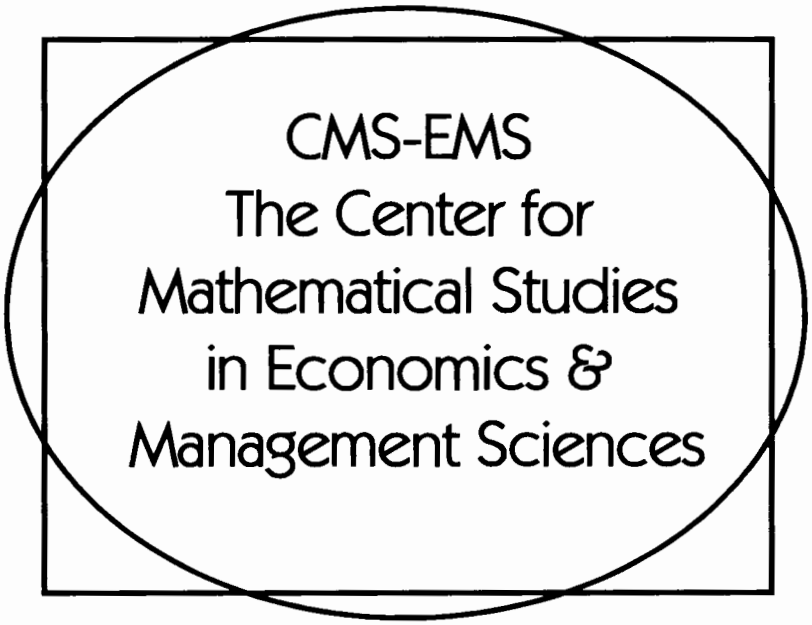
Discussion Paper #3
September, 1973

"The Informational Size of Message Spaces"

Stanley Reiter
Northwestern University

Kenneth Mount
Northwestern University

www.kellogg.nwu.edu/research/math



Discussion Paper No. 3

THE INFORMATIONAL SIZE OF MESSAGE SPACES

by

Kenneth Mount and Stanley Reiter

Revised September 1973

THE INFORMATIONAL SIZE OF MESSAGE SPACES

ABSTRACT

We study the space of equilibrium messages of a resource allocation process. A process is characterized by a "message correspondence" and a "choice function." The dependence of messages on the structure of direct knowledge of the environment on the part of each agent is expressed by requiring the message correspondence to be a coordinate correspondence (i.e., privacy preserving). A concept of the informational size of a topological space is given and used to study the informational size of the message space of a process. Classical pure exchange economies are studied, and it is shown that for such environments the message space of the competitive process is of minimal informational size among all Pareto-satisfactory processes whose message correspondence preserves privacy and is upper semi-continuous. Several corollaries specialize this result to message spaces having dimension.

to the information processing required by a system. [3/] Experience suggests that lack of attention to this aspect of institutional design, perhaps as a consequence of lack of applicable theory, results in designs whose performance is often quite different from what was intended or anticipated. [4/] Questions relating to informational

---

3/ Other important classes of properties are, among others, (1) those relating to the incentives experienced by economic agents, and (2) those relating to authority relations among them. Both incentives and authority relations are closely related to and in a sense dependent upon informational properties. Analytical convenience is served by separating these problems.

4/ For example, the federal government can recover "excess profits" on defense contracts under the so-called Renegotiation Act. That Act provides that several factors be considered in determining a "proper" level of profit, factors including such things as an unusual degree of technical expertise, or of efficiency, and value to the national defense, among others. In order to evaluate these factors, the administering authority (the Renegotiation Board) would have to investigate the technical details of production and costs to determine whether or not the firm was operating on a technical frontier, and where that frontier was in relation to the technical possibilities of other firms. The Board would also need to study the characteristics of the product in relation to its uses, and compare them with alternatives actually or potentially available. Leaving aside questions of incentives to conceal or misrepresent data and the investigative burdens imposed by such activities, it is in itself a substantial burden to receive the information implied by factors mentioned in the Act and to analyse it so as to determine an allowable profit. Some administratively feasible procedure must perforce be used; if the budget of the Board is not large enough to provide for a staff adequate to the assigned task, then a feasible task will likely be substituted. The result is probably that the policy under which profits are actually recovered is different from that visualized by the Congress when it wrote the legislation. In an extreme case, informational burdens of administration could make the policy as administered random with respect to the factors provided in the Act! Many other examples to the same point could be given.

THE INFORMATIONAL SIZE OF MESSAGE SPACES

by

Kenneth R. Mount [1/] and Stanley Reiter [2/]

I. 1 Problems of economic policy may be grouped in two broad classes which may be loosely described as those involving choice of the value of a "parameter" within a given system of economic institutions, and those involving choice among institutions. Familiar examples of problems of the first type include choice of tax rates, rates of government expenditures, size of the money supply. Examples of the second type include design of "new" economic systems such as embodied in the Yugoslavian economic reform of 1968, or the choice of economic institutions confronting a developing country, as well as more limited problems, such as design of regulatory mechanisms, or structuring of the system of financial institutions, such as is embodied in the Federal Reserve Act of 1933.

In order to analyze and compare alternative economic systems so as to permit more enlightened choice among them, we seek to identify those properties of such systems on which choice should turn and to study their counterparts in a formal model. Among such properties are those relating

---

1/ This research was partly supported by The National Science Foundation Grant (GP 28915).

2/ This research was partly supported by The National Science Foundation Grant (GS 31346 X) and by a grant from the General Electric Company.

preferences of consumers), and in order to arrive at (optimally) coordinated actions. this information must somehow be communicated among agents. Hayek saw the economic system (in part) as a mechanism for communicating and processing information. Some methods for achieving that optimal coordination were regarded by him as infeasible; e.g. transfer of all relevant data to a central planning board, which then solves the resulting optimization problem and transmits instructions to each agent about the actions he is to take. While several types of information processing may be seen to be involved, the task of communicating all the necessary information was regarded by Hayek to be sufficient by itself to render central planning infeasible. Hayek also stressed the advantages of the competitive pricing mechanism as an "efficient" way of performing the tasks of communication and information processing necessary to achieve optimal coordination (at least for a certain class of economic environments). [5, p. 211; 7, p. 524] While his detailed discussion dealt almost exclusively with the competitive model as against one of a centrally planned economy, Hayek recognized the possibility of rational design of the institutional framework, and the possibility of new economic institutions ("new" in the broader sense of "hitherto not conceived" as well as "other than those historically observed".) [5, p.22]

More recently, Hurwicz undertook a more formal study of this range of questions [8] [9]. He saw that progress in the study of this kind of question would be aided by a more general formulation of information processing and communication, one which allows explicitly for new

properties of economic systems have a long history in economic thought, although it is only recently that formal study of them has been undertaken. While there is an elaborate body of theory applicable to the first type of policy problem, at least within the framework of the competitive model, the growing body of theory applicable to the second type of problem is relatively new and substantially less elaborated than is the theory of the competitive model.[5/]

Without attempting a full historical summary, it may be noted that Hayek [5, p. 209-212] gave great weight to informational considerations in the context of the debate over the feasibility of central planning. [See also 14, p. 15] Hayek [5, p. 209-212] distinguished between the problem of characterizing optimal resource allocations and the problem of processing the relevant information by means of some economic mechanism so as to find (at least a reasonable approximation to) an optimal resource allocation. As Hayek saw the problem, economic information is naturally initially dispersed among economic agents (e.g. the manager of a firm knows his own production set, but not that of any other firm nor does he know the

---

5/ It is also considerably more abstract. This feature of the theory is a consequence of its aims and problems. To analyse, compare or choose among alternative economic systems it is necessary to have a framework in which those alternative systems can be represented in the language of theory. This stands in relation to the first type of theory as a calculus of variations problem does to a calculus problem. In the case of a problem of calculus, e.g. a minimization problem, the problem is to find a value of a real variable which minimizes a given function on some set, while a calculus of variations problem can be one in which the problem is to find a function which minimizes a given functional on some class of functions. In each case it is necessary to include formally the range of alternatives to be considered. In one case that range is the real continuum, but in the other it is a more abstract class of functions. The necessity to encompass several alternative economic institutions, rather than just different "parameter values" within one given system of institutions, similarly requires a step up in the level of generality and hence abstraction of the theory.

simplified view, as consisting of a communication process in which agents exchange formal messages in an iterative fashion, followed by a decision process, and finally a translation of decisions into real actions. Hurwicz formalized the communication process by means of "language" and "response functions", specifying how each agent arrives at the messages to be emitted at each stage of the iterative exchange of messages. After the process of communication terminates, decisions are determined on the basis of the state of information at the final stage of communication. Such a formalized economic system he called an adjustment process. Hurwicz distinguished two classes of processes, one a sub-class of the other, the so-called abstract adjustment processes, in which the language used for messages could be arbitrarily specified, and the concrete processes, which are restricted to using messages consisting of sets of proposed production and exchange activities, (with decisions determined by consensus). With reference to the concrete adjustment processes, Hurwicz gave a formal definition of informational decentralization, a definition which formalized essential elements of the earlier discussion. That definition has two parts. The first, referring to the initial dispersion of information, (formalized as a property of response functions) is called "privacy", the second part, also a property of response functions, refers to the messages used by agents. The effect of the second part of his definition is to restrict the messages of an informationally decentralized concrete adjustment process to sets of commodity space vectors. Thus, after due provision for the initial dispersion of information, the concept of informational decentralization turns on a property of the space of messages, a property

economic systems, and which consequently does not formally restrict the possible alternatives so as to permit identification of efficiency with the competitive market mechanism and infeasibility with central planning. He approached the problem by giving an explicit, though abstract, formalization for an economic system, a formalization which permits inclusion of both the competitive mechanism and central planning as particular elements in a class of systems which includes others as well.

Hurwicz's formulation, though originally published in 1960, may be sufficiently unfamiliar as to call for a brief summary. Hurwicz used the term "environment" to refer to those elements of the economic situation which are given to the economy, namely, the commodity space, the set of agents, their admissible consumption sets, preferences, production sets and initial endowments. A resource allocation mechanism or adjustment process "computes" resource allocations, taking environments as its inputs. The resource allocations arrived at by a mechanism can be evaluated using the usual notions of efficiency or Pareto-optimality. Hence, one may consider the set of environments for which a given mechanism is sure to calculate all optimal allocations and only those. Hurwicz called this the class of environments for which the mechanism is Pareto-satisfactory. The initial distribution of knowledge about the environment is characterized by the assumption that individual agents know those characteristics of the environment naturally associated with them (in the absence of externalities); i.e., each individual is assumed to know his own consumption and production set, preferences and initial endowment. Knowledge so dispersed is not in general capable of yielding optimally coordinated action. Hence, communication in some form is necessary. The economic system is seen, in an admittedly

proposed mechanisms for finding optimal resource allocations in the presence of externalities. While no formal concept of information was given, such notions are implicit in the discussion. One element of the discussion involved the necessity of transmitting to one of the agents information about the production function of another, a matter covered by the concept of privacy; another turned on counting the number of variables whose values must be transmitted, a matter of "size" of messages.

We are interested in analysing the communication processes of a wide class of mechanisms. Once we admit administrative mechanisms, messages can become quite abstract, (as observation of the nature and variety of bureaucratic forms and memoranda suggests) and not directly related to the commodity space. Hence, it is desirable to have a concept of informational size and a formulation of privacy applicable to message spaces which are capable of representing the kinds of messages actually used. Something considerably more abstract than Euclidean space is clearly necessary. We have chosen to consider general topological spaces. It is also desirable to have a concept of informational size of messages and of privacy which provides a basis for classifying processes into more than the two classes "informationally decentralized" or "not informationally decentralized" and hence could serve as the basis for a notion of the degree of informational decentralization. This is also a property of the concepts introduced here.

Hayek's insight into the informational virtues of the competitive process

we may loosely call the "size" of the messages. In the case of a Euclidean commodity space, informational decentralization restricts messages to sets of vectors whose dimension is that of the commodity space. Because information is initially assumed to be dispersed, and hence all additional information acquired by an agent must be communicated to him via the formal message process, restriction of the "size", or information-carrying capacity of messages, can serve as an indirect way of restricting the kind as well as the amount of information exchanged. Thus, for example, a production set not describable by a small number of real parameters cannot in general be communicated using a commodity space vector as the message.[6/] The concept of informational decentralization, which classifies (concrete) adjustment processes into two classes, consisting of the informationally decentralized ones and all the others, permits posing the problem of trade-off between desirable informational properties of adjustment processes and other performance characteristics, such as the inclusiveness of the class of environments for which optimal coordination by the process can be guaranteed. This trade-off is of the same sort as was encountered in the renegotiation of contracts mentioned above, namely, a trade-off between desired performance and informational feasibility. The same kind of comparison has been considered, although more implicitly, by others. A debate between Wellicz [16] and Davis-Whinston [4] turned on the comparison of communication requirements imposed by various alternative

---

6/ Certain additional restrictions are needed to avoid anomolies arising from the fact that arbitrary amounts of information can be encoded in a single real number. This matter is dealt with below. See Example following Lemma 10.

I.2 In addition to the informal considerations just discussed, examples arising in the formal study of resource allocation processes (formalized economic organizations) suggest the existence of a "trade-off" between environmental coverage (the class of environments for which a given process achieves a desired performance standard) and the informational requirements of the process. One such example is afforded by the comparison between the greed process and the quasi-competitive process given by Hurwicz [8] which reveals that the extension of Pareto-satisfactory performance for all convex environments, achieved by the quasi-competitive process, to the same performance for the class of all decomposable environments, achieved by the greed process, comes at the "cost" of requiring more complex messages. The greed process uses preference sets as messages, while the quasi-competitive process uses convex cones with vertex at the origin. A second example, also due to Hurwicz [10], shows that in order to achieve Pareto-satisfactory performance for a case involving an externality, either messages of higher Euclidean dimension must be used, or an inadmissable coding process involving a Peano-type curve, must be used.

In these examples the informational requirements of a process are discussed in terms of the messages used, as we have already remarked. In the one case, the dimension of the message space is considered and in the other a more subtle notion of "size", related to a comparison of the collection of all possible preference sets with the collection of all convex cones with vertex at the origin, seems to be involved. Further, Hurwicz [10] has restated the concept of informational decentralization originally given in [8] so that it is given explicitly in terms of the dimension of the space of messages used

is perhaps a natural one for economists to have. It is of interest to establish whether the competitive process is in some sense an "informationally best" process. Hurwicz has posed a problem of this kind and has shown that there is no other process which preserves privacy and achieves optimal coordination for the same class of environments as the competitive process and which uses a Euclidean message space of lower dimension than the competitive process. We also study a form of this question, asking whether there is a process using a message space of smaller informational size (without the restriction to Euclidean spaces) which achieves optimal coordination for the same class of environments as does the competitive process. The answer is roughly, "No."

there that any resource allocation process capable of achieving Pareto-satisfactory performance for a class of environments with Cobb-Douglas utility functions and whose message correspondence is upper semi-continuous, must use a message space whose informational size is at least that of the message space used by the competitive process [Theorem 31, III]. We show further that this result also holds for any class of environments which includes the Cobb-Douglas utility function [Corollary 34,III]. This means that the Cobb-Douglas case is merely a device of analysis and is not a restriction of the results.If the requirement of upper semi-continuity of the message correspondence is dropped and only privacy is required, then as the Example following Corollary 34 shows, the message space of the competitive process is not of minimal informational size. It remains true, even without upper semi-continuity, that any Pareto-satisfactory process which preserves privacy and uses a Hausdorff message space has a message space which is locally at least as large informationally as that of the competitive process [Theorem 35, III]. Since the message space of the competitive process is Euclidean, it has a dimension. Two results relate the dimension of the message space of a process to that of the competitive process. First, in the presence of the upper semi-continuity condition, if a process is Pareto-satisfactory for the class of Cobb-Douglas environments and uses a separable metric message space then its dimension is at least that of the competitive message space [Corollary 32, III]. Second, without upper semi-continuity, if a process is Pareto satisfactory for the class of Cobb-Douglas environments, and

(together with a "privacy" requirement). Motivated by such interest in the "size" of the space of messages used by a resource allocation process, we introduce a concept of the informational size of a topological space (Definition 9, II). With this concept, and with the formal representation of a resource allocation process given below (Definitions 1 and 3,II), we can approach the study of the trade-off between environmental coverage and informational size of the message space. We do this somewhat indirectly by looking for the message space of minimal informational size sufficient for a process to achieve a specified performance. Put somewhat figuratively, to find a message space of minimal informational size sufficient for a specified performance is to find a point on the efficiency frontier in a space in which the axes are "performance" and "informational size." This efficiency frontier is, of course, the set characterizing the possible trade-offs. Our results in this direction are only partial. For the case in which the space of environments, the space of actions and the message space are topological spaces, we find the message space of minimal informational size for processes which we do not necessarily preserve privacy [Lemma 10, II]. But for privacy preserving processes, at this level of generality we find only rather obvious bounds on the informational size of the message space.

However, specializing somewhat, we study one portion of the efficiency frontier alluded to above in some detail in III, where we [illegible] pure exchange economies with a finite number of agents and commodities. We show

PROCESSES, PRIVACY AND INFORMATIONAL SIZE

II.1 Processes and Privacy: We suppose that the set of agents is $\{1,\ldots,n\}$ and let X^i denote the space of possible characteristics of agent i, (e.g. his admissible consumption set, preferences, technology, etc.). The space $X = X^1 x \ldots x X^n = \prod_{i=1}^{n} X^i$ is the space of the possible economic environments. In writing X as a product of the X^i's we are considering the class of decomposable environments [7] [8]. We further suppose that there is a space Z, whose elements are interpreted as joint actions, and a function $f:X \to Z$. We interpret f as designating the action f(x) in Z which is to be taken when the environment is $x \in X$. We shall refer to f as a performance standard or choice function. To clarify further the interpretation of f, consider the set of all actions $z \in Z$ which are Pareto-optimal for an environment $x \in X$. Because this is in general a set consisting of actions not Pareto-comparable, it does not in itself define a unique (up to a Pareto-indifferent set) action to be chosen. Yet a resource allocation process should be required to determine an essentially unique action. (A weaker form of such a requirement, called essential single valuedness, is imposed by Hurwicz in [8].) Any process which determines a unique action for each environment thereby defines a choice function. Thus, a choice function is a specification of the performance of an allocation process. In III we consider Pareto-satisfactory choice functions on the class of convex, decomposable environments. In this section we shall require only that the X^i

---

[7] It is possible to interpret X^i as the space in which agent i's direct information about the environment is contained, where the environment is an element of a different space. Under certain assumptions about the relationship of the distribution of information among agents to the true environment, the analysis given below applies without alteration.

is privacy preserving and its message space is Euclidean, then its dimension is at least that of the competitive message space (Corollary 36, III]. This result has been obtained independently and in a different way by Hurwicz [11].

Finally, we note that the concept of informational size of a space applies to finite sets with the discrete topology. In that case, informational size corresponds to the number of elements in the space. (See the Remark following Lemma 15.)

if for each $x \in X$, $\tilde{f}$ is constant on $\mu(x)$ and has value $f(x)$. Thus if $u \in \mu(x)$, then $\tilde{f}(u) = f(x)$. We shall say that M has sufficient information for the function f if there is a pair $(\mu,\tilde{f})$ such that $\mu: X \to M$, $\tilde{f}: M \to Z$, $(\mu,\tilde{f})$ is compatible with f, and μ is a locally sectioned correspondence (see Definition 6 below). We shall say then that $(\mu,\tilde{f})$ realizes f. We call the pair $(\mu,\tilde{f})$ a resource allocation process, (briefly, process) with message space M, and choice function $\tilde{f}$.[8/]

The assumption that X is a product of spaces X^i already formalizes the notion that each agent knows directly only his own component of the environment. As noted above, the communication process must preserve the privacy of direct knowledge by requiring that all information acquired by an agent about components of the environment other than his own must come via formal messages. Another way of putting this is that messages emitted by an agent can depend directly only on his own component of the environment, and not on others of which he can have no direct knowledge. We formalize this by means of a subclass of correspondences which preserve privacy. (Hurwicz introduced this term in [6]).

Definition 2. Suppose that $X^1,\ldots,X^n$ is a set of topological spaces and suppose that M is a topological space. A correspondence $\mu: X^1x\ldots xX^n \to M$ is said to be a coordinate correspondence if and only if there are correspondences $\mu_i: X^i \to M$ such that for each $(x^1,\ldots,x^n) \in X^1x\ldots xX^n$, $\mu(x^1,\ldots,x^n) = \mu_1(x^1) \cap \ldots \cap \mu_n(x^n)$.

8/ The performance standard $f: X \to Z$ can be regarded as the choice function of a process $(\mu,\tilde{f})$ with M = X and μ = the identity on X.

(hence X) and Z be topological spaces, and that the choice functions f satisfy certain regularity conditions.

We consider resource allocation processes in which each agent knows directly his own component $x^i \in X^i$ of the environment $x = (x^1,\ldots,x^n)$, and in which any further information is acquired by communication among agents.

Communication takes place by iterative exchange of formal messages until a stationary message is reached. At that stage a joint action is determined on the basis of the stationary message only. We are interested in the "size" of the message space needed to realize a given choice function. We shall study the space of stationary messages. Since the space in which iteration of messages takes place must at least include the stationary messages, we thereby obtain a lower bound on the "size" of the message space.

In what follows, if X and Y are topological spaces, then by a correspondence from X to Y we shall mean a subset $\Gamma \subset X \times Y$ such that the projection of Γ to X covers X. That is, for each $x \in X$ the subset of Y which corresponds to x is nonempty. If Γ is a correspondence, then for $x \in X$, $\Gamma(x) = pr_Y[(x \times Y) \cap \Gamma]$. In what follows, unless otherwise stated, when we say <u>function</u> we shall mean <u>continuous function</u>.

<u>Definition 1.</u> Suppose that X, M, and Z are topological spaces, and suppose that $f: X \to Z$ is a function. A pair which consists of a correspondence $\mu: X \to M$ and a function $\tilde{f}: M \to Z$ is said to be <u>compatible with f</u> if and onl

Let $\bar{M}$ be the set of message complexes $\bar{m} = (\bar{m}^1,\ldots,\bar{m}^n)$ satisfying $g^i(\bar{m}^1,\ldots,\bar{m}^n;\ x^i) = 0,\quad i=1,\ldots,n$. Then the function $\varphi\colon \bar{M} \to Z$ is the outcome function and the pair (f,φ) is a Hurwicz resource allocation process.

Lemma 4. Let $X = \prod_{i=1}^{n} X^i$ and let $M = M^{(n)}$.

a) Let $g^i(m^1,\ldots,m^n;\ x^i) = 0 \quad i=1,\ldots,n$ be the equilibrium equations of a Hurwicz resource allocation process with equilibrium message space $\bar{M}$. (Note that the functions g^i are not necessarily continuous.) There is a coordinate correspondence $\mu\colon X \to \bar{M}$, with coordinates $\mu_i\colon X^i \to \bar{M}$ such that $\bar{m} \in \bar{M}$ satisfies the equilibrium equation $g^i(\bar{m}^1,\ldots,\bar{m}^n;\ x^i) = 0$ $i=1,\ldots,n$ if and only if $\bar{m} \in \bigcap_{i=1}^{n} \mu_i(x^i)$.

b) Let $\mu\colon \prod_{i=1}^{n} X^i \to \bar{M}$ be a coordinate correspondence with coordinates μ_i. There exist (characteristic) functions $g^i\colon \bar{M} \times X^i \to \{0,1\}$ such that $\bar{m} \in \bigcap_{i=1}^{n} \mu_i(x^i)$ if and only if $g^i(\bar{m};\ x^i) = 0$ for $i=1,\ldots,n$.

Proof. Immediate from definition, for $\mu_i(x^i) = \{(m^1,\ldots,m^n) \in \bar{M} \mid g^i(m^1,\ldots,m^n;\ x^i) = 0\}$.

We see from Definition 2 that a coordinate correspondence is a correspondence with a prescribed decomposition. We now give necessary and sufficient conditions that a correspondence be a coordinate correspondence.

Notation: If $x = (x_1,\ldots,x_n)$ and $y = (y_1\ldots,y_n)$ are elements of $M_1 \times\ldots\times M_n$ we shall denote by $x \otimes_j y$ the element $(y_1,\ldots,y_{j-1},x_j,y_{j+1},\ldots,y_n)$.

Definition 3. Let $X = \prod_{i=1}^{n} X^i$, M and Z be topological spaces and let $(\mu, \tilde{f})$. where $\mu: X \to M$ and $\tilde{f}: M \to Z$, be a resource allocation process (with message space M and choice function $\tilde{f}$). We say that $(\mu, \tilde{f})$ preserves privacy if and only if μ is a coordinate correspondence.

We may interprete the correspondences $\mu_i: X^i \to M$, as strategies of communication. Thus $m \in \mu_i(x^i)$ means that the joint message (proposal) m is acceptable to agent i when his environmental component is x^i, if the other agents also agree to m.

The relationship of this model of an allocation process to that of Hurwicz [8] is made clear in Lemma 4 below. Let $X = \prod_{i=1}^{n} X^i$ be the space of environments. In Hurwicz's formulation, the message space M is a product. We may write $M^{(n)} = \prod_{i=1}^{n} M^i$. He defines response functions, such that

$$f^i(m_t^1, \ldots, m_t^n; x^i) = m_{t+1}^i \qquad i = 1, \ldots, n$$

represents the iteration of messages, and

$$g^i(m^1 \ldots m^n; x^i) \equiv f^i(m^1, \ldots, m^n; x^i) - m^i = 0 \qquad i=1, \ldots, n$$

characterizes the equilibrium message complex when the environment is $x = (x^1, \ldots, x^n)$. That f^i depends on x only through x^i expresses the property of privacy. We may call $(g^1, \ldots, g^n) = (0, \ldots, 0)$ the equilibrium equations of the process.

where the last equality one derives from an application of (*). Thus

$\mu_1(v_1) \cap \ldots \cap \mu_n(v_n) = [\bigcup_{x,y,z} \mu(v \otimes_1 (v \otimes_2 x)) \cap \mu(x \otimes_2 y) \cap \mu(v \otimes_3 z)] \cap$

$\bigcap_{i=1}^{4} [\bigcup_w \mu(v \otimes_i w)] =$

$[\bigcup_{x,y,z} \mu(v \otimes_1 (v \otimes_2 (v \otimes_3 x))) \cap \mu(x \otimes_3 z) \cap \mu(x \otimes_2 y)] \cap \bigcap_{i=1}^{4} [\bigcup_w \mu(v \otimes_i w)] =$

$\ldots = [\bigcup_x \ldots \bigcup_w \mu(v) \cap \mu(x \otimes_n w) \cap \ldots] \subseteq \mu(v)$. On the other hand

$\mu_i(v_i) \supseteq \mu(v)$, thus $\mu_1(v_1) \cap \ldots \cap \mu_n(v_n) \supseteq \mu(v)$. This completes the proof.

Given a space of environments $X = \prod_{i=1}^{n} X^i$, a space of actions Z and a choice function $f: X \to Z$, specifying the desired actions for each possible environment, there always exists a privacy-preserving allocation process $(\mu, \tilde{f})$ realizing f. Take $M = X$ and $\mu_i(x^i) = \{(y^1 \ldots y^n) \in X \mid y^i = x^i\}$ $i=1,\ldots,n$. Then $\bigcap_{i=1}^{n} \mu_i(x^i) = \{x\}$. Finally, take $\tilde{f} = f$. The question then arises whether there is a privacy-preserving process realizing f with a "smaller" message space. And, more ambitiously, what is the "smallest" message space M such that there is a privacy-preserving process realizing f with the message space M ?

In order to pose such questions precisely a concept of the informational size of a space is needed. Hurwicz [10] and [11] has posed similar questions using the dimension of Euclidean spaces as a "measure" of size. The intuitive basis of this concept is the notion that more resources (or difficulties of communication) are involved in using e.g., two-dimensional rather than one-dimensional messages. Whatever the merit of this concept of

Lemma 5: Suppose that $X^1,\ldots,X^n$, M are topological spaces and suppose that $\mu = X^1 x \ldots x X^n \to M$ is a correspondence. A necessary and sufficient condition (which we shall call the "crossing condition") that μ be a coordinate correspondence is that for each pair of points $x = (x_1,\ldots,x_n)$ and $x' = (x_1',\ldots,x_n')$ in $X^1 x \ldots x X^n$ and each integer $1 \leq i \leq n$.

(*) $\quad \mu(x) \cap \mu(x') = \mu(x' \otimes_i x) \cap \mu(x \otimes_i x')$.

Proof. First suppose that μ is a coordinate correspondence. Then

$$\mu(x) \cap \mu(x') = \mu_1(x_1) \cap \ldots \mu_n(x_n) \cap \mu_1(x_1') \cap \ldots \cap \mu_n(x_n')$$

$$= [\mu_1(x_1) \cap \ldots \cap \mu_{i-1}(x_{i-1}) \cap \mu_i(x_i') \cap \mu_{i+1}(x_{i+1}) \cap \ldots \cap \mu_n(x_n)] \cap$$

$$[\mu_1(x_1') \cap \ldots \cap \mu_{i-1}(x_{i-1}') \cap \mu_i(x_i) \cap \mu_{i+1}(x_{i+1}') \cap \ldots \cap \mu_n(x_n')] =$$

$$\mu(x' \otimes_i x) \cap \mu(x \otimes_i x').$$

Conversely suppose that $\mu: X^1 x \ldots x X^n \to M$ is a correspondence which satisfies the condition (*). If $y \in X^i$ and $x \in X^1 x \ldots x X^n$, then set $\mu_i(y) = \bigcup_{x \in X^1 x \ldots x X^n} \mu(x_1,\ldots,x_{i-1},y,x_{i+1},\ldots,x_n)$; thus $\mu_i(y)$ is the union of all the values of μ at the points of $X^1 x \ldots x X^n$ which have ith coordinate y. Thus if we set $v = (v_1,\ldots,v_n)$, then $\mu_1(v_1) \cap \ldots \cap \mu_n(v_n) =$

$$\bigcap_{i=1}^n [\bigcup_{u \in X^1 x \ldots x X^n} \mu(v \otimes_i u)] =$$

$$[\bigcup_x \mu(v \otimes_1 x)] \cap [\bigcup_y \mu(v \otimes_2 y)] \cap \bigcap_{i=1}^3 [\bigcup_z \mu(v \otimes_i z)] =$$

$$[\bigcup_{x,y \in X^1 x \ldots x X^n} \mu(v \otimes_1 x) \cap \mu(v \otimes_2 y)] \cap \bigcap_{i=1}^3 [\bigcup_z \mu(v \otimes_i z)] =$$

$$[\bigcup_{x,y \in X^1 x \ldots x X^n} \mu(v \otimes_1 (v \otimes_2 x)) \cap \mu(x \otimes_2 y)] \cap \bigcap_{i=1}^3 [\bigcup_z \mu(v \otimes_i z)]$$

Proof: Suppose that f is locally sectioned. Then f^{-1} is locally sliced by definition. Assume $p \in Y$. Thus there exists an open set $U(p)$ which contains p, and a function $s_p : U(p) \to X$ such that $s_p(u) \in f^{-1}(u)$ for each $u \in U(p)$. Thus $f \circ s_p(u) = u$. The converse is clear.

In order to make these definitions a bit clearer we give the reader two examples. First let G denote the topological space which is the graph in R x R of the function f given by $f(x) = x$ for $x < 1$ and $f(x) = x + 1$ for $1 \leq x$. Let p denote the function from G to R x 0 (R the reals) which carries (x,y) to (x,0). The topological space G is mapped continuously and one-to-one onto the x-axis (the reals). However it is clear that although the point (1,0) is in the image of p, there is no local section to G. Next consider the correspondence from R to G which carries x to (x,x) if $x < 1$ or to (x,x + 1) if $x \geq 1$. This correspondence is clearly not sliced.

For a more interesting example, let C denote the complex numbers and let X denote the subset of C x C satisfying the equation $y^2 - x$. Let p denote the projection from X to C x 0 which carries (x,y) to x. In the neighborhood of (0,0) the map p is not locally sectioned. To see this, note that if such a section exists, then there is a function s from C to the set of (x,y) such that $y^2 - x = 0$. However it is classical (see [13] for example) that there is no continuous square root in the neighborhood of 0. On the other hand if we consider the space $X - \{(0,0)\}$ and the space $C - \{0\}$ with the same projection p, then p is clearly locally sectioned, indeed at any nonzero point we can construct an analytic cross section by use of the Taylor series of $\sqrt{x}$. We can build a correspondence which is not locally sliced in this case as we did before.

informational size, it is not available for spaces which do not have dimension. Further, it does not seem to be the appropriate concept for finite sets. In the next section we study the informational size of topological spaces.

II.2 Informational Size: We will introduce a concept of the informational size of a topological space. For this purpose, we need certain concepts of regularity.

Definition 6. Suppose the X and Y are topological spaces. If $\mu: X \to Y$ is a correspondence from X to Y, then we shall say that μ is locally sliced if the following condition is satisfied:

> for each $p \in X$, there exists an open set U(p) which contains p and a function $s:U(p) \to Y$ such that for each $u \in U(p)$, $s(u) \in \mu(u)$.

The function s will be called a local slice or slice of μ.

Definition 7. If X and Y are topological spaces, then an onto function $f:X \to Y$ is said to be locally sectioned if the correspondence f^{-1} from Y to X is locally sliced.

Lemma 8: Suppose that X and Y are topological spaces. An onto function $f:X \to Y$ is locally sectioned if and only if for each $p \in Y$ there exists an open set U(p) which contains p and a function $s_p:U(p) \to X$ such that for each $u \in U(p)$ $f \circ s_p(u) = u$.

than the image of f.

The next lemma characterizes the message space of minimal size when the message correspondence is not required to preserve privacy.

Lemma 10. If $f:X \to Z$ is a locally-sectioned onto function and if M has sufficient information for f, then M as much information as Z.

Proof: Because M has sufficient information for f there exists a pair $(\mu, \tilde{f})$ which realizes f, and such that $\mu:X \to M$ $f:M \to Z$. Because f is an onto function and $(\mu, \tilde{f})$ realizes f, it follows that $\tilde{f}$ also maps onto Z. To prove our assertion it will suffice to show that the function $\tilde{f}$ is locally sectioned. Thus suppose that $p \in Z$. There is an open set U(p) in Z and a function $s_p:U(p) \to X$ such that $f \cdot s_p = Id_{U(p)}$. Thus there exists an open set V in X which contains f(p) and a function τ: $V \to M$ such that for each $v \in V$, $\tau(v) \in \mu(v)$. The set $V \cap Im(s_p)$ is open in $Im(s_p)$, where $Im(s_p)$ denotes the image under s_p of its domain. Then $s_p^{-1}[V \cap Im(s_p)]$ is open in U(p), and hence $U' = s_p^{-1}[V \cap Im(s_p)]$ is open in Z. Further set $\xi = \tau \circ s_p$: $U' \to M$. Then $\tilde{f} \circ \xi(u) = \tilde{f} \circ \tau \circ s_p(u) = \tilde{f}[\mu(s_p(u))] = g \circ s_p(u) = u$. This completes the proof.

One may ask whether the condition that the correspondence μ be locally sliced is actually required for the definition of information sufficiency. It is easy to see that if we drop the condition, then the Peano function arises as a pathological possibility. Consider the space R x R (R = reals) and the function I = Identity from R x R to R x R. Let π: $R \to R \times R$ denote the space-filling Peano curve. Let μ: $R \times R \to R$ denote the correspondence π^{-1}. Then the function π: $R \to R \times R$ together with μ realizes I, since $\pi \circ \mu = I$. Thus if we were to remove the local slice condition in the definition of sufficiency

Definition 9. Suppose that X and Y are topological spaces. We shall say that Y has as much information as X if and only if there exists a locally sectioned function from Y to X. We shall say that Y has strictly more information than X, if Y has as much information as X, but X does not have as much information as Y.

With this definition it follows that R x R (R = real numbers) has strictly more information than R. To see this, note that the function which projects R x R onto its first factor is a locally sectioned function. Therefore R x R has as much information as R. On the other hand, if R were to have as much information as R x R, then there would have to be a function p: R → R x R which is onto and locally sectioned. Suppose that x ∈ R x R. There would have to be a function s:U → R for an open set U containing x such that $p \circ s = Id_U$. Thus U would be homeomorphic to a subset of R (that is homeomorphic to the image of s). It follows that one could embed a two-dimensional disc in a one-dimensional space. However this is impossible.

As we mentioned above, we are interested in the message space of minimal informational size sufficient for a given function. If we do not restrict the processes considered to those which preserve privacy, it is intuitively clear that the minimal message space should be that consisting of the values of the given function. I.e., the least information one could expect to be sufficient to compute the value of a function f is the value of f itself. Indeed a concept of informational size which did not have this as an implication would be suspect. As we shall see below, (Example following Lemma 13) if a privacy preserving process is required, then the size of the minimal message space sufficient for a given function f is generally larger

Definition 12. Suppose that F is a nonempty set of functions from a topological space X to a topological space Z. We shall say that M has sufficient information for the family F if M has sufficient information for each $f \in F$.

We next establish the analogue of Lemma 10 for a class of functions.

Lemma 13. Suppose that F is a nonempty set of functions from a topological space X to a topological space Z. Suppose further that there exists a topological space M and a function $\varphi: M \to Z$ such that for each $f \in F$ there exists a correspondence $\mu_f: X \to M$ such that the pair (μ_f, φ) realizes f. Suppose also that the following condition is satisfied:

> If $p \in Z$, there exists a function $f \in F$ and an open set $V \subset X$ such that f(V) is a neighborhood of p, and f as a function from V to f(V) is locally sectioned.

Then M has as much information as Z.

Proof: We shall show that the function $\varphi: M \to Z$ is locally sectioned. There exists an open set U(p) which contains p and a function $f \in F$ such that f carries an open set in M onto U, $(f^{-1}(U(p))) \cap V$, where f(v) is an open set in X which covers a neighborhood of p. Because f has a local section, there exists a function $s_f: U \to X$ such that $f \circ s_f = Id_U$. The correspondence μ_f has a slice on a neighborhood of $s_f(p)$. Suppose that σ_f is such a slice of μ_f. Then the function $\sigma_f \circ s_f$ is a slice of the correspondence φ^{-1}.

From Lemma 10, we see that the informational size of the minimal message space of a process $(\mu, \tilde{f})$ realizing $f: X \to Z$, but not necessarily preserving privacy,

of information, the pathological situation that R is sufficient for the identity function $I: R \times R \to R \times R$ would result.

We now extend the concept of a space having sufficient information for a function to that of a space having sufficient information for a class of functions.

One technique of proof which we shall use involves the consideration of a restricted class of environments in order to achieve a lower bound for the information required for a process. In order to justify this procedure it is necessary to consider only those processes whose relevant properties are inherited under restriction to subspaces (see for example Corollary 34 where this line of argument is used.)

Definition 11.

(i) Let X^i $i=1,\ldots,n$ be topological spaces and let $f: \prod_{i=1}^{n} X^i \to Z$ be a function. We say that a space M has <u>minimal information for f relative to a class of allocation processes having a property $\mathcal{P}$</u> if and only if there exists a process with property $\mathcal{P}$ and message space M which realizes f, and such that if N is a space for which there exists an allocation process with property $\mathcal{P}$ which has message space N and which realizes f, then N has as much information as M.

(ii) We shall call a process $(\mu, \tilde{f})$ with message space M and which has property $\mathcal{P}$, a <u>$\mathcal{P}$-process</u> if for any subspaces Y^i of X^i $i=1,\ldots,n$, the restriction of $(\mu, \tilde{f})$ to $\prod_{i=1}^{n} Y^i$ with message space M also has property $\mathcal{P}$.

Let $\mu_1 = X^1 \to \{\alpha,\beta,\gamma\} = M$

be given by $\mu_1(1) = \{\alpha\}$; $\mu_1(2) = \{\beta,\gamma\}$,

and let $\mu_2: X^2 \to M$ be given by $\mu_2(1) = \{\alpha,\beta\}$ $\mu_2(2) = \{\alpha,\beta\}$. Then $\mu_1 \cap \mu_2$ is given by Table II.

2	α	β
1	α	γ
X^2 / X^1	1	2

TABLE II.

Taking $\tilde{f}$ such that $\tilde{f}(\alpha) = \tilde{f}(\gamma) = a$ and $\tilde{f}(\beta) = b$, we see that $(\mu,\tilde{f})$ realizes f with message space $M = \{\alpha,\beta,\gamma\}$. Note that M is informationally larger than Z, and that M is not a product inside $X^1 \times X^2$.

We will find the following simple result useful in Section III.

Lemma 14. Suppose $\prod_{i=1}^{n} X^i$, Z and M are topological spaces, and suppose $f: \prod_{i=1}^{n} X^i \to Z$ is a continuous function.

is the same as the informational size of the image of f in Z. Imposing the further condition that the process preserve privacy, i.e., that μ be a coordinate correspondence, will in general require a message space of larger informational size; somewhere "between" the image of f and the informational size of X.

The following example illustrates this increase in informational size. It also shows that the increase in generality provided by not requiring the message space to be a product space is significant, since in this example the message space of minimal informational size for a coordinate correspondence is not a product inside X.

Example: Let $X^1 = X^2 = \{1,2\}$, and suppose $f: X^1 \times X^2 \to \{a,b\} = Z$, is given by Table I.

2	a	b
1	a	a
X^2 / X^1	1	2

TABLE I.

The correspondence $\nu: X^1 \times X^2 \to Z$ which has the minimal message space is given by a table identical to Table I, and $\tilde{f}$ for this correspondence is identity on Z.

However ν is not a coordinate correspondence because it fails to satisfy the crossing condition of Lemma 5 .

Equivalently,

$$h \circ \mu_1(x_1) \cap \ldots \cap h \circ \mu_n(x_n) \cap h \circ \mu_1(y_1) \cap \ldots \cap h \circ \mu_n(y_n)$$

$$= h \circ \mu_1(x_1) \cap \ldots \cap h \circ \mu_j(y_j) \cap \ldots \cap h \circ \mu_n(x_n) \cap h \circ \mu_1(y_1)$$

$$\cap \ldots \cap h \circ \mu_j(x_j) \cap \ldots \cap h \circ \mu_n(y_n)$$

or,

$$h\left[\bigcap_{i=1}^{n} \mu_i(x_i) \cap \bigcap_{i=1}^{n} \mu_i(y_i)\right] = h\left[\bigcap_{i=1}^{n} \mu(x \textcircled{x}_j y)\right]$$

Since h is a 1-1 function, this condition is satisfied if and only if μ satisfies the crossing condition. Since μ is a coordinate correspondence, so is $h \circ \mu$.

Since h is a homeomorphism, h^{-1} is a function and hence so is $\tilde{f} \circ h^{-1}$. This function is compatible with $h \circ \mu$, since $v,v' \in h \circ \mu(x,y)$ if and only if $h^{-1}(v) \in \mu(x,y)$ and $h^{-1}(v') \in \mu(x,y)$. Since $\tilde{f}$ is compatible with μ, $\tilde{f}(h^{-1}(v)) = \tilde{f}(h^{-1}(v'))$ if $h^{-1}(v) \in \mu(x,y)$ and $h^{-1}(v') \in \mu(x,y)$. Hence $v,v' \in h \circ \mu(x,y)$ implies $\tilde{f} \circ h^{-1}(v) = \tilde{f} \circ h^{-1}(v')$.

Finally $(h \circ \mu, \tilde{f} \circ h^{-1})$ realizes f, since

$\tilde{f} \circ h^{-1}$ $h \circ \mu = \tilde{f} \circ \mu$, which realizes f.

Remark:

As we have noted at the end of section II. 1, the concept of dimension is inappropriate for a study of the size of finite sets. However the concept of informational size of this chapter applies to finite sets. We note first that the concept of information introduced in II applies to discrete topological spaces and functions between them. Indeed, if we suppose that X is a topological space with the discrete topology, then a topological space X has

Suppose that Y^i is a subspace of $X^i (i = 1,\ldots,n)$ and assume that M has minimal information for the restriction of f to $\prod_{i=1}^{n} Y^i$ among $\mathcal{P}$-processes. If there exists a $\mathcal{P}$-process such that M has sufficient information for f on $\prod_{i=1}^{n} X^i$, then M has minimal information for f on $\prod_{i=1}^{n} X^i$.

Proof: Note that if $(\nu,\tilde{f})$ is a pair which realizes f, then the correspondence ν^*, which is the restriction of ν to the subspace $\prod_{i=1}^{n} Y^i$, is a coordinate correspondence from $\prod_{i=1}^{n} Y^i$ to M which with $\tilde{f}$ realizes f.

Lemma 15. Let $X^1,\ldots,X^n$, W and V be topological spaces; let $\mu = \mu_1 x \ldots x \mu_n : \prod_{i=1}^{n} X^i \to W$ be a coordinate correspondence on $\prod_{i=1}^{n} X^i$ and let $h: W \to V$ be a homeomorphism of W to V.

Then

$$h \circ \mu = h \circ \mu_1 x \ldots x\, h \circ \mu_n : \prod_{i=1}^{n} X^i \to V$$

where

$$h \circ \mu_1 x \ldots x\, h \circ \mu_n (x_1,\ldots,x_n) =$$

$$h(\mu_1(x_1)) \cap \ldots \cap h(\mu_n(x_n))$$

is a coordinate correspondence on V.

Further if f is a function on $\prod_{i=1}^{n} X^i$ to Z and $\tilde{f}: W \to Z$ is such that $(\mu,\tilde{f})$ realizes f, then the function $\tilde{f} \circ h^{-1}: V \to Z$ together with the coordinate correspondence $h \circ \mu$ realizes f.

Proof: The correspondence $h \circ \mu$ is a coordinate correspondence if and only if it satisfies the crossing condition of Lemma 5. I.e., for all $x = (x_1,\ldots,x_n)$ and $y = (y_1,\ldots,y_n)$ in $\prod_{i=1}^{n} X^i$,

$$h \circ \mu(x_1,\ldots,x_n) \cap h \circ \mu(y_1,\ldots,y_n) = h \circ \mu\,(x_1,\ldots,x_{j-1},y_j,x_{j+1},\ldots,x_n)$$

$$\cap\, h \circ \mu(y_1,\ldots,y_{j-1},x_j,y_{j+1},\ldots,y_n)$$

MINIMALITY OF THE COMPETITIVE MESSAGE SPACE

III. The objective of this section is to show that every message space sufficient for the class of Pareto-satisfactory allocation processes on convex environments and satisfying certain regularity conditions is at least as large (informationally) as the competitive message space. Pareto-satisfactoriness of an allocation process involves three properties; namely, 1) non-wastefulness, 2) unbiasedness and 3) essential single-valuedness [Hurwicz 8]. Hurwicz describes the performance of an allocation process by a correspondence associating a set of outcomes with each possible environment and applies the criterion of Pareto-satisfactoriness to that correspondence. We shall strengthen these criteria to state that: 1) the outcomes associated with an environment are Pareto-optimal for that environment, 2) every allocation that is Pareto-optimal for a given environment is a possible outcome after some suitable redistribution of the initial endowments and 3) if more than one outcome is associated with an environment, then all such outcomes are Pareto-indifferent.[9/]

We shall consider a subclass E of the class of all convex environments, namely, those in which utility functions are "Cobb-Douglas." On this subclass of environments we consider the correspondence that associates with each environment the set of all allocations which are Pareto-optimal in that environment. (We might have considered instead the class of Pareto-optimal allocations at least as preferred by everyone to his initial endowment.) We next consider all functions which are (continuous) selections from this correspondence. There is at least one such selection, since the function which selects the (unique) competitive equilibrium for each environment is

---

9/ This is a strengthening of Hurwicz's condition of essential single valuedness in that he requires only that all outcomes associated with an equilibrium message be Pareto-indifferent. We use the stronger requirement in keeping with our insistence that the process have a unique solution in each environment.

as much information as Y if and only if the cardinality of Y is less than or equal to the cardinality of X, and Y has the discrete topology.

In order to see this note that if Y has the discrete topology and the cardinality of Y is no larger than the cardinality of X, then it is obvious that X has as much information as Y. Conversely, assume X has as much information as Y. Then there is a continuous function f from X onto Y which is locally sectioned. Because f is onto, the cardinality of X is at least as great as that of Y. Next, if $p \in Y$, then there is an open neighborhood U of p and a continuous function $s:U \to X$ such that fos is the identity on U. Thus U is homeomorphic to a subspace of X. Because X is discrete, U must have the discrete topology, and in particular p is an open set.

Finally, note that an immediate consequence of the previous discussion is that if $E_1,\ldots,E_n$ is a finite collection of sets where each E_α $\alpha=1,\ldots,n$ has the discrete topology and if $f:E_1x\ldots xE_n \to Z$ is a function onto a discrete topological space Z. then there exists a message space X which has minimal information among all message spaces sufficient for f. Furthermore X has the discrete topology.

It seems worthwhile to remark that here one could equally well use the Hausdorff metric topology on sets.

It is well-known that for this class of environments the excess demand function $\xi^i: S \times E^i \to R^l$ is a continuous function on $S \times E^i$, and for each $e^i \in E^i$, $\xi^i(\cdot, e^i)$ is differentiable.

Definition 16. For $e \in E$, $(p,y) \in S \times R^{nl}$ is a competitive equilibrium for e, where p is a competitive equilibrium price for e and y is a competitive equilibrium trade for e, if

1) $\sum_{i=1}^{n} \xi^i(p,e^i) = 0$

2) $p \cdot \xi^i(p,e^i) = p \cdot y^i = 0 \quad i=1,\ldots,n.$

For $e \in E$, a competitive equilibrium exists and is unique; if p is the competitive price for e then $p_j > 0$, $j=1,\ldots,l$ [1, p.225 and Theorem 6, p. 222].

Let $\Omega: E \to R^{nl}$ be the correspondence that associates with each $e \in E$ the set of all allocations $x = (x^1,\ldots,x^n) \in R^{nl}$ such that x is Pareto-optimal for e.

Let $Du^i(x^i)$ denote the normalized derivative of u^i evaluated at x^i, using the normalization $\sum_{j=1}^{l} Du^i_j(x^i) = 1$. Thus,

$$Du^i: R^{l+} \to S.$$

It is well-known that necessary and sufficient conditions that x be Pareto-optimal for e, i.e., $x \in \Omega(e)$ are:

1) $x^i \in R^{l+} \quad i=1,\ldots,n$

2) $\sum_{i=1}^{n} x^i = \sum_{i=1}^{n} w^i$

3) there exists $p \in S$ such that $Du^i(x^i) = p, \quad i=1,\ldots,n,$

i.e., x is a redistribution of the initial endowment which is individually

continuous (using the topology for environments introduced below).

We shall also require that the selections have the property that if an "initial point" is Pareto-optimal, the process stays there.

We shall show that for the set E of Cobb-Douglas environments a lower bound for the informational size of message spaces can be established, and then, applying Lemma 13 suitably, it follows that the same lower bound applies to any class of environments containing E.

We consider a class of exchange economies with l commodities and n consumers. Let the commodity space be R^l and let the admissible consumption set of each consumer be R^{l+}, the non-negative orthant of R^l. Let $S = \{ p \in R^l \mid \sum_{i=1}^{l} p_i = 1,\ p_i > 0 \quad i=1\ldots l \}$, and note that S is homeomorphic to $I^{l-1} = \{p \in R^{l-1} \mid p_i > 0,\ i=1,\ldots,l-1 \ \sum_{i=1}^{l-1} p_i < 1\}$. A consumer $i \in \{1,\ldots,n\}$ is characterized by a pair (u^i, w^i) where $u^i \in U^i$ is his utility function and $w^i \in R^{l+}$ is his resource endowment. We take

$$U^i = \{ u:R^l \to R \mid u(x) = \prod_{j=1}^{l} x_j^{\alpha_j}, \alpha_j > 0 \quad j=1,\ldots,l \}.$$

We write $E^i = U^i \times R^l$ and $E = E^1 x \ldots x E^n$.

Let $\xi^i: S \times E^i \to R^l$ be the excess demand function of consumer i. Thus $\xi^i(p,e^i)$ is the excess demand of consumer i when his utility is u^i, his endowment is w^i and the price vector is p.

We shall now introduce a topology on $U^i \times R^{l+}$; for $x \in R^l$, $\| x \| = \max_j |x_j|$, and for u, u' in U^i, let $d(u,u') = \max_j |\alpha_j - \alpha'_j|$, where $u(x) = \prod_j x_j^{\alpha_j}$ and $u'(x) = \prod_j x_j^{\alpha'_j}$. [10/] We give E^i the product topology, and let E have the product topology of the E^i.

Definition 18. By a non-wasteful performance function on E we shall mean a continuous selection ω from Ω satisfying the condition that if $e = \langle (u^i, w^i) \rangle$ is such that $w \in \Omega(e)$, then $\omega(e) = w$. An allocation process that realizes a non-wasteful performance function is also called non-wasteful on E.

Definition 19. A function $\rho: E \to E$ is a redistribution if $\rho(\langle (u^i, w^i) \rangle) = \langle (u^i, \bar{w}^i) \rangle$ and $\sum_{i=1}^{n} \bar{w}^i = \sum_{i=1}^{n} w^i$.

A redistribution ρ may be written as product $\mathrm{Id}_{U^i} \times \bar{\rho}_{z^i}(u^i, w^i) = (u^i, w^i + z^i)$ with parameter $z = (z^1, \ldots, z^n) \in R^{nl}$, where $\sum_{i=1}^{n} z^i = 0$.

We shall write $\rho_z(e) = (\mathrm{Id}_{U^i} \times \bar{\rho}_{z^i}) \times \ldots \times (\mathrm{Id}_{U^n} \times \bar{\rho}_{z^n})(e^1, \ldots, e^n) = \langle (u^i, w^i + z^i) \rangle$, where $e^i = (u^i, w^i)$.

Definition 20. A performance function ω is called unbiased (and any allocation process compatible with that performance function is called unbiased) if given $e \in E$ and any point $x \in \Omega(e)$, there exists a redistribution ρ such that $\omega \circ \rho(e) = x$.

An allocation process that realizes a non-wasteful, unbiased performance function on E is Pareto-satisfactory on E.[12/]

Definition 21. We define $\bar{\Omega}: E \to R^{nl}$ by,

$$\bar{\Omega}(e) = \{(y^1, \ldots, y^n) \in R^{nl} \mid y = x - w, \text{ for } x \in \Omega(e), e = \langle (u^i, w^i) \rangle\}.$$

Let $\bar{\omega}$ denote the continuous selection from $\bar{\Omega}$ corresponding to ω; i.e.,

$$\bar{\omega}(e) \equiv \omega(e) - w, \text{ where } e = \langle (u^i, w^i) \rangle.$$

12/ A selection from Ω is automatically non-wasteful. A non-wasteful performance function is (strongly) essentially-single-valued on E, since strict concavity of utility functions implies that the relevant Pareto-indifference classes are points.

admissible and such that there is a "mutual tangency" of all utility functions at the respective x^i.

Writing $y^i = x^i - w^i$ $i=1,\ldots,n$, we may state the same condition in terms of trades;

1') $y^i \in R^l$ $i=1,\ldots,n$

2') $\sum_{i=1}^{n} y^i = 0$

3') there exists $p \in S$ such that $Du^i(y^i + w^i) = p$, $i=1,\ldots,n$.

Lemma 17. The correspondence $\Omega: E \to R^{nl+}$ is upper semi-continuous on E.

Proof: Let $\{e_j\}$ denote a sequence of environments converging to e and let $x_j \in R^{nl}$, $x_j \in \Omega(e_j)$, such that $x_j \to x$. We must show that $x \in \Omega(e)$. Note that $e_j \to e$ if and only if, for $e_j = <(u_j^i, w_j^i)>$,[11] $e = <(u^i, w^i)>$, $u_j^i \to u^i$, $w_j^i \to w^i$ for $i=1,\ldots,n$. By the definition of convergence of utility functions, $u_j^i \to u^i$ if and only if $\overline{Du_j^i(z^i)} \to \overline{Du^i(z^i)}$ for all $z^i \in R^{l+}$ $i=1,\ldots,n$.

Now, $x_j \in \Omega(e)$ if and only if

1) $x_j^i \in R^{l+}$ $i=1,\ldots,n$

2) there exists $p \in S$ such that $Du_j^i(x_j^i) = p_j$ $i=1,\ldots,n$

3) $\sum_{i=1}^{n} x_j^i = \sum_{i=1}^{n} w_j^i$.

Now, $x_j \to x$ implies $x_j^i \to x^i$ for $i=1,\ldots,n$, and, by convergence of $u_j^i \to u^i$, it follows that $Du_j^i(x_j^i) \to Du^i(x^i)$ for $i=1,\ldots,n$, i.e., $p_j \to Du^i(x^i) \equiv p$ for $i=1,\ldots,n$.

Further $x_j^i \to x^i$, $w_j^i \to w^i$ and $\sum_{i=1}^{n} x_j^i = \sum_{i=1}^{n} w_j^i$ for $j=1,\ldots,n$ imply $\sum_{i=1}^{n} x^i = \sum_{i=1}^{n} w^i$. Hence $x \in \Omega(e)$.

---

[11] We shall sometimes use the notation

"$<(u^i, w^i)>$" for "$((u^1,w^1),(u^2,w^2),\ldots,(u^n,w^n))$."

Let $\bar{e}^i = \left(\prod_{j=1}^{\ell} x_j^{\bar{\alpha}_j^i} \; ; \; \bar{w}^i \right)$ and write $\sum_{j=1}^{\ell} \bar{\alpha}_j^i = \bar{\beta}^i$, $i=1,\ldots,n$,

then,

$$\xi_j^i(p;\bar{e}^i) = \frac{\sum_{k=1}^{\ell-1} p_k \bar{w}_k^i}{p_j \bar{\beta}^i} \cdot \alpha_j^i - \bar{w}_j^i \text{, where } p_j > 0,\ j=1,\ldots,\ell-1, i=1,\ldots,n,$$

which, for some $\bar{p} \in I^{\ell-1}$, satisfies

$$\bar{y}_j^i = \xi_j^i(\bar{p},\bar{e}^i) = \frac{\sum \bar{p}_k \bar{w}_k^i \bar{\alpha}_j^i}{\bar{p}_j \bar{\beta}^i} - \bar{w}_j^i \qquad \text{for } i=1,\ldots,n-1.$$

Let $y^i \in N(\bar{y}^i)$ and write $y^i = \bar{y}^i + \delta$, where $\delta \in R^{\ell-1}$ and $|\delta| < \epsilon$. Then set

$$y_j^i = \frac{\sum_k \bar{p}_k \bar{w}_k^i}{\bar{p}_j \bar{\beta}^i} \cdot \alpha_j^i - \bar{w}_j^i$$

and, solving for α_j^i,

$$\alpha_j^i = [y_j^i + \bar{w}_j^i] \cdot \frac{\bar{p}_j \bar{\beta}^i}{\sum_{k=1} \bar{p}_k \bar{w}_k^i} = \bar{\alpha}_j^i + \delta_j \cdot \left[\frac{\bar{p}_j \bar{\beta}^i}{(\sum \bar{p}_k \bar{w}_k^i)} \right].$$

Hence for $e^i = \left(\prod_j X_j^{\alpha_j^i}, \bar{w}^i \right)$, $\xi^i(\bar{p},e^i) = y^i$, $i=1,\ldots,n-1$. Taking

$y_\ell^i = - \frac{\sum_{j=1}^{\ell-1} \bar{p}_j y_j^i}{\bar{p}_\ell}$ for $i=1,\ldots,n-1$ and taking e^n to satisfy $\xi^n(\bar{p},e^n) = \sum_{i=1}^{n-1} \xi^i(\bar{p},e^i)$,

we see that $f(e) = (y^1,\ldots,y^{n-1})$. Set $s_{\bar{y}^i}^i(y^i) = e^i$ for $i=1,\ldots,n-1$ and

set $s^n(y^1,\ldots,y^{n-1}) = e^n$. Then the function

$$s_{\bar{y}^1}^1 \times s_{\bar{y}^2}^2 \times \ldots \times s_{\bar{y}^{n-1}}^{n-1} \times s^n : N(\bar{y}^1) \times \ldots \times N(\bar{y}^{n-1}) \to E$$

We note that if ω is the performance map of a Pareto-satisfactory process and if $z = \omega(\bar{e}) - \bar{w}$, where $\bar{e}$ is a given element of E, and for $\rho: E \to E$, such that $\rho_z(e) \equiv <(u^i, w^i + z^i)>$, then $\bar{\omega}(\rho(\bar{e})) = 0$.

Definition 22. Let $f: E \to R^k$, be the function associating with each $e \in E$, the unique competitive equilibrium trade for e.

Note that we may take $k = (n-1)(l-1)$, because for each i the demand function has only $l - 1$ independent components, since

$$\xi_n^i(p, e^i) \equiv - \frac{\sum_{j=1}^{l-1} p_j \cdot \xi_j^l(p, e^i)}{p_l}$$

and the equations $y^n = - \sum_{l=1}^{n-1} \xi^l(p, e^i)$ leave only (n-1) independent excess demands of consumers.

It is well-known that,

Lemma 23. The function f is a continuous function on E.

Proof. The function f is an upper semi-continuous correspondence on E. For $e \in E$, competitive equilibrium is unique. It follows that f is a function, and hence a continuous function.

Lemma 24. The function f is a locally sectioned function.

Proof.[13] Let $\bar{y} \in R^{(n-1)(l-1)}$, $\bar{y} = f(\bar{e})$ for some $\bar{e} \in E$, and for $\epsilon > 0$ let $\bar{N}(\bar{y})$ be an ϵ-neighborhood of $\bar{y}$ in $R^{(n-1)(l-1)}$. Then we may assume $\bar{N}(\bar{y}) = \sum_{l=1}^{n-1} N(\bar{y}^i)$ when $N(\bar{y}^i)$ are ϵ-neighborhoods of $\bar{y}^i$ in R^{l-1}.

---

[13] This proof establishes a stronger property than that asserted in Lemma 24, namely, that there is a local inverse for f through any point $\bar{e}$ such that $f(\bar{e}) = \bar{y}$.

Lemma 26. The correspondence μ is a locally sectioned continuous function.

Proof: We have already noted that μ is a function. That it is continuous in $<(\mu^i, w^i)>$ follows from the fact that the demand functions are continuous in the parameters α^i, w^i. We show next that μ is locally sectioned.

Let $(p,y) \in S \times R^{(n-1)(\ell-1)}$, and let $e \in E$, $e = <(\mu^i, w^i)>$ such that $\mu(e) = \{(p,y)\}$. Hence $x^i = y^i + w^i > 0$. Then there exists $\varepsilon > 0$ such that for $U_\varepsilon(p,y)$ an open set containing (p,y), if $\bar{p},\bar{y} \in U_\varepsilon(p,y)$ then $\bar{x}^i = w^i + \bar{y}^i > 0$.

First, define

$$y_\ell^i = - \frac{\sum_{j=1}^{\ell-1} \bar{p}_j \bar{y}_j^k}{\bar{p}_\ell}, \quad i = 1,\ldots,n-1, \text{ and let } \bar{z}^i \equiv (\bar{y}^i, y_\ell^i). \text{ Then}$$

$\bar{p} \cdot \bar{z}^i = 0$ for $i = 1,\ldots,n-1$. Further let $\bar{z}^n = - \sum_{i=1}^{n-1} \bar{z}^i$, so that $\sum_{i=1}^{n} \bar{z}^i = 0$.

Now the equations

$$\frac{\alpha_j^i}{\alpha_1^i} \frac{\bar{x}_1^i}{\bar{x}_j^i} = \frac{\bar{p}_j}{\bar{p}_1} \qquad \begin{matrix} j = 1,\ldots,\ell \\ i = 1,\ldots,n \end{matrix}$$

can be solved for each i for the $\ell-1$ ratios

$\frac{\alpha_j^i}{\alpha_1^i}$, determining

$$\frac{\bar{\alpha}_j^i}{\bar{\alpha}_1^i} = \frac{\bar{p}_j}{\bar{p}_1} \cdot \left(\frac{\bar{x}_j^i}{\bar{x}_1^i} \right) \qquad j = 2,\ldots,\ell; \quad i = 1,\ldots,n. \tag{27}$$

A normalization (e.g. $\bar{\alpha}_1^i = \bar{p}_1$; or $\sum_{j=1}^{\ell} \bar{\alpha}_j^i = 1$) suffices to determine $\bar{\alpha}^i$ uniquely.

This construction serves to define a function $t_{(p,y)}: S \times R^{(n-1)(\ell-1)} \to E$. Note that $t_{(p,y)}(\bar{p},\bar{y}) = (\bar{e},w)$ where $e = <(u^i,w^i)>$, $\bar{e} = (u^i,w^i)$ with $\bar{u}^i$ determined by the $\bar{\alpha}^i$ given in equation (27).

is clearly continuous, since for each component i, α^i is continuous in δ, for fixed $\bar{p}$, $\bar{y}^i$, $\bar{e}^i$. ∎

It follows from Lemma 10 that $Y \equiv f(E)$ is informationally minimal for correspondences realizing f.

We introduce a coordinate correspondence μ and a function $\tilde{f}$ such that $(\mu, \tilde{f})$ realizes f.

Definition 25. Let

$$\mu_1 x \ldots x \mu_n : E^1 x \ldots x E^n \to W.$$

where for k=1,...,n;

$$\mu_k(e^k) = \left\{ (p,y^1,\ldots,y^n) \in S \times R^{n(l-1)} \mid y_j^k = \xi_j^k(p,e^k) \right.$$
$$\left. -y_j^k = \sum_{\substack{i=1 \\ i\neq k}}^{n} y_j^i \qquad j=1,\ldots,l-1, \right\}$$

and $$\bigcap_{k=1}^{n} \mu_k(e^k) = \left\{ (p,y^1,\ldots,y^n) \in S \times R^{n(l-1)} \mid y_j^k = \xi_j^k(p,e^k) \right.$$
$$\left. k=1,\ldots,m, \quad \sum_{k=1}^{n} y_j^k = 0 \quad j=1,\ldots,l-1. \right\}$$

Taking account of the condition $\sum_{i=1}^{n} y^i = 0$ and of the budget constraints $p \cdot y^i = 0$ i = 1,...,n, we see that the values of $\mu = \bigcap_{i=1}^{n} \mu_i$ are in a subspace of S x Y of dimension n(l-1). Since S has Euclidean dimension l-1, Y has dimension (n-1)(l-1), equal to that of the image of f.

For e ∈ E the equations $\sum_i \xi^i(p,e^i) = 0$ have a unique solution. Hence $\mu(e)$ consists of a single point for each e ∈ E, i.e., μ is a function.

We define $\tilde{f}: S \times Y \to R^{nl}$ by

$$\tilde{f}(p,y) = y.$$

Lemma 29. Suppose that $\bar{y} \in Y$ and suppose that $\bar{p}, \bar{\bar{p}} \in S$ such that $\bar{p} \neq \bar{\bar{p}}$.

1) there exists elements $\bar{e}$, $\bar{\bar{e}}$ in E such that $f(\bar{e}) = f(\bar{\bar{e}}) = \bar{y}$ and

$$\mu(\bar{e}) = (\bar{p},\bar{y}) \neq (\bar{\bar{p}},\bar{y}) = \mu(\bar{\bar{e}})$$

and 2) if $\bar{e}$ and $\bar{\bar{e}}$ are elements of E such that $\mu(\bar{e}) = (\bar{p},\bar{y}) \neq (\bar{\bar{p}},\bar{y}) = \mu(\bar{\bar{e}})$

then, 3) $f(\bar{e} \otimes_j \bar{\bar{e}}) \neq \bar{y}$. [14/]

Proof. Lemma 26 shows that we may choose elements $\bar{e}$ and $\bar{\bar{e}}$ in E such that $\mu(\bar{e}) = (\bar{p},\bar{y})$ and $\mu(\bar{\bar{e}}) = (\bar{\bar{p}},\bar{y})$. In order that $(\bar{p},\bar{y}) = \mu(\bar{e})$ one must have that $\sum_{i=1}^{n} \bar{y}_i = 0$ and $Du^{-i}(\bar{y}^{-i} + \bar{w}^{-i}) = \bar{p}$, $i=1,\ldots,n$. Similarly $\mu(\bar{\bar{e}}) = (\bar{\bar{p}},\bar{y})$ implies that $\sum_{i=1}^{n} \bar{y}_i = 0$ and $Du^{\bar{=}i}(\bar{y}^{-i} + \bar{w}^{\bar{=}i}) = \bar{\bar{p}}$, $i=1,\ldots,n$. Now suppose that $f(\bar{e} \otimes_j \bar{\bar{e}}) = \bar{y}$. Then there exists $p \in S$ satisfying the conditions $\sum_{i=1}^{n} \bar{y}_i = 0$, $Du^{\bar{=}j}(\bar{y}^{-j} + \bar{w}^{\bar{=}j}) = p$ and $Du^{-i}(\bar{y}^{-i} + \bar{w}^{-i}) = p$ for $i \neq j$. But $Du^{j}(\bar{y}^{-j} + \bar{w}^{\bar{=}j}) = \bar{\bar{p}}$ and $Du^{-i}(\bar{y}^{-i} + \bar{w}^{-i}) = \bar{p}$. Thus it follows that $p = \bar{p} \neq \bar{\bar{p}} = p$ which is a contradiction. Hence $f(\bar{e} \otimes_j \bar{\bar{e}}) \neq \bar{y}$.

Lemma 30. Suppose that $\nu: E \to X$ is a privacy preserving correspondence and that with the function $g:X \to Y$, the pair (ν,g) realizes f on E. If e and $\bar{e}$ are elements of E such that $\mu(e) \neq \mu(\bar{e})$, then $\nu(e) \cap \nu(\bar{e}) = \emptyset$.

Proof. Suppose $\mu(e) = (p,y)$ and $\mu(\bar{e}) = (\bar{p},\bar{y})$. $\mu(e) \neq \mu(\bar{e})$ implies either $y \neq \bar{y}$ or $p \neq \bar{p}$. If $y \neq \bar{y}$, then $g(\nu(e)) = f(e) \neq f(\bar{e}) = g(\nu(\bar{e}))$, since both $(\mu,\tilde{f})$ and (ν,g) realize f on E. Hence $\nu(e) \cap \nu(\bar{e}) = \emptyset$. So we may suppose $y = \bar{y}$ and $p \neq \bar{p}$. Note that $\nu(e) \cap \nu(\bar{e}) \neq \emptyset$ implies $g(\nu(e)) = g(\nu(\bar{e}))$. Since ν is a coordinate correspondence (preserves privacy) ν satisfies the crossing condition, i.e., $g(\nu(e \otimes_j \bar{e})) = g(\nu(\bar{e}))$. But by Lemma 29, 2) if

---

[14/] The idea in this Lemma is similar to an argument first made by Hurwicz [10] and later also by Starrett [15], in connection with certain examples.

The function $t_{(p,y)}$ is continuous at $(\bar{p},\bar{y})$. Let $(p(k),y(k))$ be a (non-constant) sequence converging to $(\bar{p},\bar{y})$. Then, since w^i is constant independently of $(p(k), y(k))$, and since $u(k)$ is determined by

$$\frac{\alpha_j^i(k)}{\alpha_1^i(k)} = \frac{p_j(k)}{p_1(k)} \cdot \frac{\left(y_j^i(k) + w_j^1\right)}{(y_1^i(k) + w_1^i)} \qquad j = 2,\ldots,l,\ i = 1,\ldots,n$$

(together with a normalization), it follows that $u^i(k) \to \bar{u}^i$. (Note that $p_1(k) \neq 0$, $(y_1^i(k) + w_1^i) \neq 0$.)

Hence $t_{p,y}$ is a continuous local inverse for μ.

Lemma 28. Let $\omega: E \to R^{nl}$ be a Pareto-satisfactory performance map. Then ω can be written as the composition of a redistribution ρ_z, depending on e and $\omega(e)$, with the fixed function f.

Proof. Let $e \in E$ and $\omega(e) = x$. Since ω is Pareto-satisfactory, $x \in \Omega(e)$ and for ρ given by $z = x - w$, $\rho_z(\bar{e}) = <(\bar{u}^i,(\bar{w}^i + z))>$ for $\bar{e} \in E$. Note that $\omega(\rho_z(e)) = x$, and $\bar{\omega}(\rho_z(e)) = 0$. But $f(\rho_z(e)) = 0$ since there exists $p \in S$ such that $Du^i(w^i + z^i) = p$ for $i = 1,\ldots,n$ and $y^i = 0$, for $i = 1,\ldots,n$ satisfies $p.y^i = 0$ and $\sum_{i=1}^{n} y^i = 0$. Hence, for all $e \in E$,

$$\bar{f}[\rho_z(e)] = f[\rho_z(e)] = 0.$$

All that this amounts to is the observation that, for environments in the class E, every Pareto optimum is a competitive equilibrium for some suitable initial endowment.

Let $e \in E$ and $\omega(e) = x$. Then it follows from $\bar{\omega}(\rho_x(e)) = f(\rho_x(e))$, that $\bar{\omega} = f$ on a subset $G = \{e \in E \mid e \in f^{-1}(0)\} = \{e = <(u^i,w^i)> \in E \mid x \in \Omega(e)\}$.

It follows from the upper semi-continuity of ν that the correspondence ν^{-1} is upper semi-continuous. (The graph of ν^{-1} is the same as that of ν; and a correspondence is upper semi-continuous if and only if its graph is closed.) Regarded as a correspondence, μ is upper semi-continuous, since it is a continuous function. The composition of two upper semi-continuous correspondences is upper semi-continuous. Since the composition $\mu \circ \nu^{-1}$ is a function, it is therefore continuous. [2, Theorems in Chapter VI, pp. 109-111].

The function φ is onto S x Y, since ν^{-1} is onto E and μ is onto S x Y.

We now show that φ is locally sectioned. Let $(p,y) \in S \times Y$ and let U be an open neighborhood of (p,y) in S x Y such that $t_{(p,y)}: U \to E$ is a local section of μ.

Since ν is a locally sliced correspondence, given $e \in E$ there exists an open set H which contains e, and a continuous function $v: H \to X$ such that $v(\bar{e}) \in \nu(\bar{e})$ for $\bar{e} \in H$.

Given H, by continuity of $t_{(p,y)}$, there exists an open subset $V \subset U$ such that $t_{(p,y)}(V) \subset H$. The function $\Psi \equiv v \circ t: V \to X$ is a local section for φ, since it is continous and satisfies $\Psi \circ \varphi = Id_V$. The last equality is established as follows:

Let $(\bar{p},\bar{y}) \in V$ and let $\bar{e} = t_{(p,y)}(\bar{p},\bar{y})$.

Then $v(\bar{e}) \in \nu(\bar{e})$ or $\bar{e} \in \nu^{-1}(v(\bar{e}))$. Hence $\Psi \circ \varphi(\bar{p},\bar{y}) = \mu(\bar{e}) = (\bar{p},\bar{y})$.

Thus, $\Psi \circ \varphi = Id_V$.

Corollary 32. Under the hypotheses of Theorem 31 and if X is a separable metric space, then the dimension of X is at least that of S x Y.

e and $\bar{e}$ are elements of E such that $f(e) = f(\bar{e}) = \bar{y}$ and $\mu(e) \neq \mu(\bar{e})$ then for $j \in \{1,\ldots,n\}$ $f(e \otimes_j \bar{e}) \neq f(\bar{e})$. The hypothesis that (ν,g) realizes f on E implies $g(\nu(e \otimes_j \bar{e})) = f(e \otimes_j \bar{e}) \neq f(\bar{e}) = g(\nu(\bar{e}))$. Hence $g(\nu(e \otimes_j \bar{e})) \neq g(\nu(\bar{e}))$, which is a contradiction.

We are now in a position to answer the question posed at the end of Section 2.7. We shall show that any privacy preserving message correspondence which "computes" the competititve equilibrium has a message space which is at least as large as that of the competitive process.

Theorem 31. Let $\nu:E \to X$ be a locally sliced upper semi-continuous coordinate correspondence and $g:X \to Y$ a function such that (ν,g) realizes f on E. Then X has as much information as S x Y.

Proof. To show that X has as much information as S x Y it suffices to find a locally sectioned map of X onto S x Y. We shall show that $\varphi \equiv \mu \circ \nu^{-1}:X \to S \times Y$ is such a map, where $\nu^{-1}(x) = \{e \in E \mid x \in \nu(e)\}$. We show first that φ is a function. To this end, we show that, for $x \in X$, if e and e' belong to $\nu^{-1}(x)$ then $\mu(e) = \mu(e')$. To see this, suppose that $\mu(e) \neq \mu(e')$. Since e and e' belong to $\nu^{-1}(x)$, $g(\nu(e)) = g(\nu(e')) = g(x)$. Since (ν,g) realizes f, $f(e) = g(\nu(e)) = g(\nu(e')) = f(e') \equiv y$. By Lemma 30 if e and e' belong to $f^{-1}(y)$ and $\mu(e) \neq \mu(e')$, then $\nu(e) \cap \nu(e') = \emptyset$. But $x \in \nu(e) \cap \nu(e')$ which is a contradiction. Hence $\mu(e) \neq \mu(e')$ is false, i.e., $\mu(e) = \mu(e')$.

Thus, μ is constant on the sets $\nu^{-1}(x)$, for $x \in X$. Since μ is a function so is $\mu \circ \nu^{-1}$.

homeomorphism of $C \setminus \{p\}$ to I and carries p to $h(p) = 1/2$. Using the mapping $h \times Id_Y : C \times Y \to I \times Y$, the correspondence

$$\nu = (h \times Id_Y)^{-1} \circ \mu : E \to C \times Y$$

is a privacy-preserving correspondence from E onto C x Y. Moreover, ν is locally sectioned because except for the point p, ν is the inverse of a homeomorphism; that is, $h \times Id_Y$ is the required section. The pair consisting of ν and π_Y, the projection of C x Y onto Y, realizes f on E. However, C x Y has less information than I x Y, since there is no locally-sectioned, continuous function from C x Y onto I x Y.

However, without upper semi-continuity of the message correspondence, local comparison of the informational size of message spaces sufficient for f is possible.

Theorem 35. Let $\nu : E \to X$ be a locally-sectioned, coordinate correspondence and $g : X \to Y$ a function such that (ν, g) realizes f on E. Let X be a Hausdorff space. Then a subset of X is locally homeomorphic to S x Y.

Proof. Given a point $(p,y) \in S \times Y$ we shall construct an open set U containing (p,y) and a function $h : U \to X$ such that U and h(U) are homeomorphic.

Given (p,y), since μ has a local section there exists an open set U^* containing (p,y) and a function $t : U \to E$ such that $\mu \circ t = Id_U$. Hence t is 1-1 from U to t(U). Let $e = t(p,y)$. Since ν is a locally-sliced correspondence, given $e \in E$ there is an open set H containing e and a function $v : H \to X$ such that $v(\bar{e}) \in \nu(\bar{e})$ for all $\bar{e} \in H$.

Since t is continuous and S x Y Euclidean there is a compact neighborhood $\bar{U} \subset U$ such that $t(\bar{U}) \subset H$. We now show that v is 1-1 on $t(\bar{U})$.

If $\bar{e}$ and $\bar{\bar{e}}$ are distinct points of $t(\bar{U})$, then $\mu(\bar{e}) \neq \mu(\bar{\bar{e}})$, since t is 1-1 from $\bar{U}$ to $t(\bar{U})$ and μ is the inverse of t on $t(\bar{U})$. It follows from Lemma 30 that $\nu(\bar{e}) \cap \nu(\bar{\bar{e}}) = \emptyset$. Since v is a selection from ν, it follows that $v(\bar{e}) \neq v(\bar{\bar{e}})$.

Definition 33. Let $\mathcal{P}$ denote the property: "the message correspondence is upper semi-continuous."

An allocation process which has property $\mathcal{P}$ is a $\mathcal{P}$-process in the sense of Definition 11, since upper semi-continuity of a correspondence is preserved under restriction to a subspace.

Corollary 34. Let $\mathcal{E} \equiv \prod_{i=1}^{n} \mathcal{E}^i$ be a class of environments containing E such that $f:E \to Y$ is the restriction of $f^*: \mathcal{E} \to Y$. If $(\nu^*, \tilde{f}^*)$ is a $\mathcal{P}$-process which realizes f^* on $\mathcal{E}$ with message space M, then M has as much information as $S \times Y$.

Proof. By Lemma 14, the restriction of $(\nu^*, \tilde{f}^*)$ to E is a $\mathcal{P}$-process realizing f on E with message space M, which has less information than $S \times Y$, contradicting the conclusion of Theorem 31.

We note that, as is well-known, the message space $S \times Y$ of the competitive process has sufficient information for f on a large class of convex environments. It can also be shown that the competitive equilibrium correspondence μ is upper semi-continuous on that class of convex environments.

If in Theorem 31 the hypothesis of upper semi-continuity of the message correspondence is removed, then the conclusion of Theorem 31 no longer follows. The following example shows this:

Example.

In this example $I = n = 2$; hence S is the simplex in R^2 homeomorphic to the open unit interval I in R. Let C be the unit circle in R^2, and suppose $p \in C$. The set $C \setminus \{p\}$ is homeomorphic to I. Hence there is a function h, not necessarily continuous on all of C, from C to R which is the above

Now, the function $h = \gamma \circ t : \bar{U} \to X$ is 1-1 and continous on $\bar{U}$, since it is the composition of two 1-1 and continuous functions. Since $\bar{U}$ is compact and S x Y and X are Hausdorff, it follows that $h(\bar{U})$ is compact. Hence, h is a homeomorphism between $\bar{U}$ and $h(\bar{U}) \subset X$ [5, Theorem p.141].

Corollary 36. [15] Let X satisfy the hypotheses of Theorem 35. If, in addition, X is Euclidean, then the dimension of X is at least that of S x Y.

Proof. By Theorem 35 there is a subset of X homeomorphic to a set with interior in S x Y. The dimension of X is thus at least that of S x Y.

According to Theorem 35 any privacy preserving process which "computes" competitive equilibria on the class E (and hence on any class of environments including E) must use a message space which has locally at least as much information as S x Y. Corollary 36 states that if the message space of such a privacy preserving process is Euclidean, then its dimension is at least that of the message space of the competitive process. If in addition to preserving privacy, the message correspondence is upper semi-continuous, then according to Theorem 31 the message space has (globally as well as locally) as much information as S x Y. Finally, as Corollary 32 states, if the message correspondence is privacy preserving and upper semi-continuous and if the message space is a separable metric space, then its dimension is at least that of S x Y.

15/ The result that no Euclidean message space whose dimension is less than that of the competitive message space is sufficient for a Pareto-satisfactory process on the class of convex environments has also been obtained independently by Hurwicz [7].

IV. Suppose that $f:E_1x...xE_n \to Z$ is a function from a finite set $E_1x...xE_n$ onto a finite set Z. In this section we will describe a construction which determines in a finite number of steps a triple consisting of a set X, a privacy-preserving correspondence $\mu:E_1x...xE_n \to X$ which is onto, and a function $\tilde{f}:X \to Z$ such that the pair $(\mu,\tilde{f})$ realizes f, and such that X has minimal information among message spaces which are sufficient for f.

We note first that the concept of information introduced in Chapter II applies to discrete topological spaces and functions between them. The following assertion is almost obvious.

Lemma 37. Suppose that X is a topological space with the discrete topology. A topological space Y has less information than X if and only if the cardinality of Y is less than or equal to the cardinality of X, and Y has the discrete topology.

Proof. If Y has the discrete topology and the cardinality of Y is no larger than the cardinality of X, then it is obvious that X has more information than Y. Conversely, assume Y has less information than X. Then there is a continuous function f from X onto Y which is locally sectioned. Because f is onto, the cardinality of X is at least as great as that of Y. Next, if $p \in Y$, then there is an open neighborhood U of p and a continuous function $s:U \to X$ such that fos is the identity on U. Thus U is homeomorphic to a subspace of X. Because X is discrete, U must have the discrete topology, and in particular p is an open set.

The following is an immediate consequence of Lemma 37.

$B[x_\alpha;\alpha \in A]/I$, where I is the ideal generated by the elements $x_\alpha^2 - x_\alpha \quad \alpha \in A$. We shall denote the coset $x_\alpha + I$ again by x_α.

Note that if B is a Boolean algebra, if R is a Boolean algebra which contains B, and if R is generated as a B-algebra by elements $a_1,\ldots,a_n$ of R, then there exists a unique B-algebra homomorphism f from $B\{x_1,\ldots,x_n\} = B\{x_i;\ i \in \{1,\ldots,n\}\}$ to R such that $f(x_i) = a_i$.

The constructions described below depend on the following result.

Theorem 40: Suppose the $E_1x\ldots xE_n$ are finite sets and suppose that Z is a finite set. There exists a set X and a privacy preserving correspondence $\mu:E_1x\ldots xE_n \to X$ which satisfies the following conditions:

1) if $f:E_1x\ldots xE_n \to Z$ is a function onto Z, then there exists a subset $X(f) \subset X$ and a function $\tilde{f}$ from X(f) to Z such that the pair consisting of the restriction of μ to X(f) and $\tilde{f}$, realizes f.

2) if (ν,g) is an allocation process which realizes f, and if ν carries $E_1x\ldots xE_n$ onto Y, then there exists a function φ from Y onto a subset $\varphi(Y) \subset X(f)$ such that the restriction of μ to $\varphi(Y)$, together with the restriction of $\tilde{f}$ to $\varphi(Y)$ realizes f. Furthermore $\nu = \varphi^{-1}\mu$ and $g = \tilde{f}\,\varphi$.

Proof: Let B = B(Z) (the Boolean algebra of the set Z) and form the Boolean algebra $B' = B\{x(e_1,\ldots,e_n);(e_1,\ldots,e_n) \in E_1x\ldots xE_n\}$. We set $B^* = B'/J$, where J is the ideal in B' generated by the elements $x(e_1,\ldots,e_n)\ x\ (e_1',\ldots e_n') + x(\sigma(i,e_i')(e_1,\ldots e_n)\ x\ (\sigma(i,e_i)(e_1',\ldots,e_n'))$ [the notation $\sigma(\cdot,\cdot)$ was introduced in Lemma 5 of II] for all $1 \leq i \leq n$ and all pairs

Theorem 38 . Suppose that $E_1,\ldots,E_n$ is a finite collection of sets where each E_α $\alpha=1,\ldots,n$ has the discrete topology. Assume that $f:E_1x\ldots xE_n \to Z$ is a function onto a discrete topological space Z. There exists a message space X which has minimal information among all message spaces sufficient for f. Furthermore X has the discrete topology.

It follows from Theorem 38 that in order to find a message space which has minimal information for a function f from a finite product of discrete spaces to a discrete space we need only construct the set with minimum cardinality which has sufficient information for a privacy-preserving message process, and then give that set the discrete topology.

To continue our discussion we shall require the algorithms of Boolean algebras and Boolean rings. We refer the reader to [3] for this material.

We shall denote by Z the ring of integers, and we let Z/2Z denote the 2-field; that is a field with two elements 0 and 1,where $1\cdot 1 = 1$ and $1 + 1 = 0$. A Boolean algebra B is then a Z/2Z algebra such that $r^2 = r$ for all $r \epsilon B$. We shall assume that B has an identity element.

It is well known (see [3]) that if X is a finite set, then the ring of Z/2Z -valued functions on X (under pointwise addition and multiplication) is a Boolean algebra. Denote this algebra by B(X). Conversely if B is a finite Boolean algebra, then there exist a set X such that B is exactly the ring of Z/2Z -valued functions on X.

Definition 39: If B is a Boolean algebra and A is a finite set, then we shall denote by $B[x_\alpha, \alpha \epsilon A]$ the polynomial ring in indeterminates $x_\alpha(\alpha \epsilon A)$ with coefficients in B. We shall denote by $B\{x_\alpha;\alpha \epsilon A\}$ the Boolean algebra

the set with characteristic function $\rho(e_1,\ldots,e_n)$. Then $c_p \cdot \rho(e_1,\ldots,e_n) = c_p$. Thus $0 = c_p \cdot \rho(e_1,\ldots,e_n)(1 + c_{f(e_1,\ldots,e_n)})$. Thus $p \in \tilde{f}^{-1}(f(e_1,\ldots,e_n))$. Note that the characteristic function of the set $\mu(e_1,\ldots,e_n) \cap X(f)$ is exactly the image of $\rho(e_1,\ldots,e_n)$ in $B(X(f))$. Thus, the pair consisting of the restriction of μ to $X(f)$ (given by the correspondence which carries $(e_1,\ldots,e_n)$ to the set with characteristic function the image of $\rho(e_1,\ldots,e_n)$) and the function $\tilde{f}$ realizes f.

Finally, suppose (ν,g) realizes f, where ν carries $E_1x\ldots xE_n$ onto a set Y. Let B(Y) denote the Boolean algebra of Y. Because g carries Y onto Z, B(Y) is a B(Z) algebra by a 1-1 map $j:B(Z) \to B(Y)$. For each $(e_1,\ldots,e_n)$ let $d(e_1,\ldots,e_n)$ denote the characteristic function of the set $\nu(e_1,\ldots,e_n)$ in Y. Then $d(e_1,\ldots,e_n) \cdot d(e_1',\ldots,e_n') = d(\sigma(e_i',i)(e_1,\ldots,e_n)) \cdot d(\sigma(e_i,i)(e_1',\ldots,e_n'))$, because ν was assumed to be privacy preserving. Furthermore $\nu(e_1,\ldots,e_n) \subset g^{-1}(f(e_1,\ldots,e_n))$; thus $d(e_1,\ldots,e_n) \cdot jc_{f(e_1,\ldots,e_n)} = d(e_1,\ldots,e_n)$. It follows that if we define a homomorphism h from $B(Z)\{X(e_1,\ldots,e_n);$ $(e_1,\ldots,e_n) \in E_1x\ldots xE_n\}$ to the sub- B(Z)-algebra of B(Y) generated by B(Z) and the elements $d(e_1,\ldots,e_n)$ by setting $h(1) = 1$, and $h(x(e_1,\ldots,e_n) = d(e_1,\ldots,e_n)$, then h carries the ideal J to zero. Thus, h may be extended to a homomorphism h' from $B^* = B/J$ to B(Y). Further h' sends the generators of K(f) to zero; thus h' determines a B(Z) algebra homomorphism, h", from $B^*/K(f) = B(X(f))$ to B(Y). Let H denote the kernel of h". Then B(X(f))/H is a B(X(f)) algebra. Therefore B(X(f))/H is the Boolean algebra of some subset Y' of X(f). Also B(X(f))/H is a sub-B(Z)- algebra of B(Y). Thus there is a function φ from Y to Y'. Suppose now that $p \in \nu(e_1,\ldots,e_n)$. This means that p is a point at which the function $d(e_1,\ldots,e_n)$ takes on the

$(e_1,\ldots,e_n),(e'_1,\ldots,e'_n)$ in $E_1x\ldots xE_n$. Because $E_1,\ldots,E_n$ and Z are finite sets, the algebra B and the algebra B' are finite. Thus B^* is a finite Boolean algebra,and hence there is a finite set X such that $B^* = B(X)$. Denote by $\rho(e_1,\ldots,e_n)$ the element in B^* which is the coset $x(e_1,\ldots e_n) + I$. The element $\rho(e_1,\ldots,e_n)$ is the characteristic function of some set $\mu(e_1,\ldots,e_n) \subset X$. We shall show that the correspondence which carries $(e_1,\ldots,e_n)$ to $\mu(e_1,\ldots,e_n)$ is privacy preserving. Lemma 5 of II states that we need only show that for each $(e_1,\ldots,e_n)$ and $(e'_1,\ldots,e'_n)$ in $E_1x\ldots xE_n$, $\mu(e_1,\ldots,e_i,\ldots,e_n) \cap \mu(e'_1,\ldots,e'_n) = \mu(e_1,\ldots,e_{i-1},e'_i,e_{i+1},\ldots,e_n) \cap \mu(e'_1,\ldots,e'_i,e_i,e'_{i+1},\ldots,e'_n)$. In terms of characteristic functions, this is equivalent to

$$(41)\quad \rho(e_1,\ldots,en) \cdot \rho(e'_1,\ldots,e'_n) = \rho(\sigma(i,e'_i)(e_1,\ldots,e_n) \cdot \rho(\sigma(i,e_i)(e'_1,\ldots,e'_n)$$

because if S and T are sets,then the characteristic function of the set $S \cap T$ is the product of the characteristic functions of S and T. Because $1 = -1$ in B^*, (41) is equivalent to the condition that

$$(42)\quad x(e_1,\ldots,e_n) \cdot x(e'_1,\ldots,e'_n) + x(\sigma(i,e'_i)(e_1,\ldots,e_n))\, x(\sigma(i,e'_i)(e'_1,\ldots,e'_n))$$

is a member of J.

However (42) is a generator for J.

Now suppose that $f:E_1x\ldots xE_n \to Z$ is a function onto Z. For each set $z \subset Z$, denote by c_z the characteristic function of the set z. Now denote by K(f) the ideal of B^* which is generated by the elements $\rho(e_1,\ldots,e_n)(1 + c_{f(e_1,\ldots,e_n)})$. The algebra $B^*/K(f)$ is a homomorphic image of B^*. Thus, there exists a subset X(f) of X such that $B(X(f)) = B^*/K(f)$. The algebra B(X(f)) contains an isomorphic copy of the Boolean algebra B(Z). If $i:B(Z) \to B(X(f))$ is the inclusion map, then there exists [3;§20] a function $\tilde{f}:X(f) \to Z$ such that for each $y \in B(Z)$, i(y) is the characteristic function of the set $\tilde{f}^{-1}(w)$,where $c_w = y$. Suppose that p is in

Now form the algebra $B(Z)\{x_{ij} ; 0 \leq i, j \leq 1\}$. Thus $B(Z)\{x_{ij}\} = (Z/2Z)\{x, y\}\{x_{00}, x_{01}, x_{10}, x_{11}\}$.

The set S which has this as its Boolean algebra consists of all the 6 - tuples of 0's and 1's. Thus S consists of $2^6 = 64$ points. If $p = \{\bar{x}, \bar{y}, \bar{x}_{00}, \bar{x}_{01}, \bar{x}_{10}, \bar{x}_{11}\}$ is a point of S, then the inclusion map $B(Z) \to B(Z)\{x_{ij}\}$ corresponds to the function which carries p to $(\bar{x}, \bar{y})$. The set which has characteristic function x_{ij} is the set of all points $\{x,y,...\}$ where $x_{ij} = 1$. Now consider the algebra $B(X) = B(Z)\{x_{ij}\}/I$, where I is the ideal generated by $x_{00}x_{11} + x_{10}x_{01}$. The algebra B(X) has as set X the collection of points in S where the function $x_{00}x_{11} + x_{10}x_{01}$ is zero. Thus the points of X are of the form $(x,y,\bar{x}_{00},\bar{x}_{01},\bar{x}_{10},\bar{x}_{11})$ where (x,y) is arbitrarily chosen, and $\bar{x}_{00}\bar{x}_{11} + \bar{x}_{10}\bar{x}_{01} = 0$. It is easy to catalogue these points. They are of the following form: (x,y,0,0,0,0), (x,y,0,0,1,0), (x,y,0,1,0,0), (x,y,0,0,0,1), (x,y,0,1,0,1), (x,y,0,0,1,1), (x,y,1,0,1,0), (x,y,1,1,0,0), (X,y,1,1,1,1), (x,y,1,0,0,0). Thus X consists of 40 points. Furthermore it is easy to exhibit the correspondence μ. For example $\mu(00) = \{(x,y,1,0,1,0), (x,y,1,1,0,0), (x,y,1,1,1,1)\}$. Next we assume that a function $f: E_1 \times E_2 \to Z$ is given. We introduce the ideal generated by the $x_{ij}^{(c_{f(ij)}+1)}$ where $ij \in E_1 \times E_2$. This expresses the condition that the inverse image of f(ij) in X has an empty intersection with the complement of the set $\mu(ij)$. This ideal corresponds to a subset of X, namely the subset which consists of all points $(x,y,a_{00},a_{01},a_{10},a_{11})$ such that in each $\mu(ij)$ the points have the form $(f(ij),a_{00},a_{01},a_{10},a_{11})$. If, for example, f(0,0) = (0,0), then the only points of $\mu(0,0)$ which can lie on X(f) are the points (0,0,1,0,0,0), (0,0,1,1,0,0), (0,0,1,1,1,1). Let us suppose the function f is as follows: f(0,0) = (0,0), f(1,1) = (1,1), f(1,0) = f(0,1) = (0,1). Thus, the set X(f) must be contained in the set of points

value 1. Denote by $\bar{x}(e_1,\ldots,e_n)$ the image of $x(e_1,\ldots,e_n)$ in $B(Y') = B(X(f))/H$. Then $\bar{x}(e_1,\ldots,e_n)\,\varphi(p) = d(e_1,\ldots,e_n)(p) = 1$. Thus the image of p lies in the subset of Y' which has characteristic function $\bar{x}(e_1,\ldots,e_n)$, and this is precisely the set which is the intersection of $\mu(e_1,\ldots,e_n)$ with Y'. Conversely, if $q \in \mu(e_1,\ldots,e_n) \cap Y'$, then $\bar{x}(e_1,\ldots,e_n)(q) = 1$. Thus, if $y \in \varphi^{-1}(q)$, then $d(e_1,\ldots,e_n)(y) = \bar{x}(e_1,\ldots,e_n)(\varphi(y)) = 1$. We have shown, therefore, that the correspondence ν is precisely $\varphi^{-1}\circ\mu$.

Next we note that the function φ is onto because the homomorphism from B(Y') to B(Y) is 1-1. (See [3]p.20).

Finally, because the homomorphism from B(Y') to B(Y) carries K(f) to zero, $\tilde{f}\circ\varphi = q$.

The force of this theorem is to reduce the search for a minimal message space to an examination of the ideal structure of B(X). We see from Theorem 40 that given a function $f:E_1x\ldots xE_n \to Z$ we can construct a Boolean algebra B(X(f)),which is the Boolean algebra of a subset of X. We also see that the minimal message space for f is given by a subset of X(f) with the required correspondence being the restriction of μ to this set. Thus, to find the minimal message space we need only construct a set S of smallest cardinality with a Boolean algebra which contains B(Z) such that B(S) is an image of B(X(f)) under a B(Z)-algebra homomorphism.

To illustrate this theorem we shall now work through an example in detail. Consider the case of two agents each with two possible environments. Thus, we set $E_1 = \{0,1\}$, $E_2 = \{0,1\}$ and $E_1x\,E_2 = \{(0,0),(0,1)(1,0)(1,1)\}$. We shall assume that the function $f:E_1x\,E_2 \to Z$ takes values in a set Z with four elements. We shall represent Z as the collection of pairs (a,b) where $a,b \in Z/2Z$. Thus we look upon Z as the set of homomorphisms of $Z/2Z\{x,y\}$ to Z/2Z.

REFERENCES

1. Arrow, K. J., and F. Hahn, General Competitive Analysis, Holden Day, San Francisco, 1971.

2. Berge , C., Topological Spaces, (Translated by E. M. Patterson,) Macmillan, New York, 1963.

3. Davis, Otto A. and Andrew Whinston, "Externalities, Welfare, and the Theory of Games," Journal of Political Economy, June, 1962, pp. 241-62.

4. Davis, Otto A. and Andrew B. Whinston, "On Externalities, Information and the Government-Assisted Invisible Hand," Economica, August, 1966 pp. 303-318.

5. Hayek, F. A. (ed.), Collectivist Economic Planning, Routledge and Kegan Paul Lts., London, 1935.

6. Hayek, F. A. The Road to Serfdom, London, 1946.

7. Hayek, F. A., "The Use of Knowledge in Society," American Economic Review, Vol. XXXV, 1945, pp. 519-520.

8. Hurwicz, L., "Optimality and Informational Efficiency in Resource Allocation Processes," Mathematical Methods in the Social Sciences, 1959, Ed., Arrow, K. J., S. Karlin and P. Suppes, Stanford University Press, Stanford, California, 1960, pp. 27-48.

9. Hurwicz, L., "On Informationally Decentralized Systems," Ch. 14, Decision and Organization, Ed. McGuire, C. B., and Roy Radner.

10. Hurwicz, L., "On Decentralizability in the Presence of Externalities," 1966 Econometric Society Meeting, San Francisco, December 1966.

11. Hurwicz, L., "On the Dimensional Requirements of Informationally Decentralized Pareto-Satisfactory Processes," (manuscript) presented at the Conference Seminar on Decentralization, Northwestern University, Evanston, Illinois, February 1972.

12. Kelley, John L., General Topology, University Series in Higher Mathematics, Van Nostrand Company, Inc., New York, 1955.

13. Knopp, K. Elements of the Theory of Functions Vol. II, Dover Publications 1953, New York.

14. Robbins, Lionel C., The Great Depression, New York, MacMillan and Co., 1934.

15. Starrett, David, An example presented at the Conference Seminar on Decentralization, University of California, Berkeley, June, 1971.

16. Wellisz, Stanislaw, "On External Diseconomies and the Government-Assisted Invisible Hand," Economica, 1964, pp. 345-362.

$\{(0,0,1,0,1,0),\ (0,0,1,1,0,1),\ (0,0,1,1,1,1)\}$

$\{(1,1,0,0,0,1),\ (1,1,0,1,0,1),\ (1,1,0,0,1,1),\ (1,1,1,1,1,1)\}$

$\{(1,0,0,1,0,1),\ (1,0,1,1,0,0),\ (1,0,1,1,1,1)\}$

$\{(1,0,0,0,1,1),\ (1,0,1,0,1,0),\ (1,0,1,1,1,1)\}$

Now $c_{01}x_{(01)} \neq x_{(01)}$ on $(0,0,1,1,1,1)$, $c_{01}\,x_{(01)} \neq x_{(01)}$ on $(1,1,1,1,1,1)$, $c_{(00)}\,x_{(00)} \neq x_{(00)}$ on $(1,0,1,1,1,1)$ and $c_{(00)}\,x_{(00)} \neq x_{(00)}$ on $(1,0,1,1,1,1)$. Thus, X(f) consists of the points of the sets:

$\mu(00) = \{(0,0,1,0,1,0),\ (0,0,1,1,0,1)\}$

$\mu(01) = \{(1,1,0,0,0,1),\ (1,1,0,1,0,1),\ (1,1,0,0,1,1)\}$

$\mu(10) = \{1,0,0,1,0,1),\ (1,0,1,1,0,0)\}$

$\mu(11) = \{\ 1,0,0,0,1,1),\ (1,0,1,0,1,0)\}$.

Now, to find a minimal message space we must choose at least one point from each $\mu(ij)$. In this case, since the μ's do not intersect, we may choose 4 distinct points.

The general construction for a minimal message space is then precisely the following process. After the construction of X(f) one need only choose one point in each of the $\mu(ij)$. This selection must be carried out so as to minimize the number of points chosen. This can be done as follows. For each point in X(f) write down all the $\mu(ij)$ which contain it. Pick a point P such that a maximal number of $\mu(ij)$'s contains it. Delete all the $\mu(ij)$'s which contain this point P. This determines a new collection of $\mu(ij)$'s containing points other than P. Repeat the process with this new collection.

l - l.c. letter "ell"

m - l.c. letter "m"

m' - l.c. letter "m" super prime

m^1 - l.c. letter "m" superscript number 1

m'_{i-1} - l.c. letter "m" super prime subscript l.c. letter "i" minus 1

m'_{i+1} - l.c. letter "m" super prime subscript l.c. letter "i" plus 1

m_2 - l.c. letter "m" subscript number 2

m_3 - l.c. letter "m" subscript number 3

M - Capital letter "M"

M_1 - Capital letter "M" subscript number 1

M_n - Capital letter "M" subscript l.c. letter "n"

n - l.c. letter "n" (subscripts and superscripts)

p - l.c. letter "p"

$\mathcal{P}$ - Script " $\mathcal{P}$ " (handwritten)

q - l.c. letter "q"

r - l.c. letter "r"

R - Capital letter "R"

s - l.c. letter "s"

s_p - l.c. letter "s" subscript l.c. letter "p"

s_p^{-1} - l.c. letter "s" super minus 1, sub l.c. letter "p"

t - l.c. letter "t"

u - l.c. letter "u"

U - Capital letter "U"

u' - l.c. letter "u" prime

v - l.c. letter "v"

v' - l.c. letter "v" prime

V - Capital letter "V"

W - Capital letter "W"

List of Symbols

a - l.c. letter "a"

A - Capital letter "A"

b - l.c. letter "b"

B - Capital letter "B"

C - Capital letter "C"

d - l.c. letter "d"

D - Capital letter "D"

e - l.c. letter "e"

(e) - l.c. letter "e" on parentheses

$\bar{e}$ - l.c. letter "e" bar

$\overline{\overline{e}}$ - l.c. letter "e" double bar

e^{i} - l.c. letter "e" super l.c. letter :i"

e' - l.c. letter "e" super prime

E - Capital letter "E"

E^{i} - Capital letter "E" super l.c. letter "i"

E' - Capital letter "E" super prime

$\mathcal{E}$ - Script letter "$\mathcal{E}$" (handwritten)

f - l.c. letter "f"

$\tilde{f}$ - l.c. letter "f" tilde

$\tilde{f}^{*}$ - l.c. letter "f" asterisk

F - Capital letter "F"

g - l.c. letter "g"

g^{i} - l.c. letter "g" super l.c. letter "i"

h - l.c. letter "h"

h^{-1} - l.c. letter "h" superscript minus number 1

I - Capital letter "I"

k - l.c. letter "k"

K - Capital letter "K"

$>$ - Greater than

$\geq$ - Greater than or equal to

$=$ - equals

$\neq$ - Not equal

$\equiv$ - identical

$-$ - minus

$\cdot$ - times

$*$ - asterisk

$\emptyset$ - Phase

$|$ - Single parallel

$||$ - Double parallel

$\rightarrow$ - yields

$[\ ]$ - left and right brackets

$\{\ \}$ - left and right braces

$\backslash$ - Diagonal reverse

α - Greek l.c. letter alpha

β - Greek l.c. letter Beta

$\bar{\beta}^{i}$ - Greek letter Beta bar superscript l.c. letter "i"

γ - Greek l.c. letter Gamma

Γ - Greek capital Gamma

σ - Greek letter Sigma

ρ - Greek letter Rho

$\bar{\rho}^{h}$ - Greek letter Rho bar superscript l.c. letter "h"

ν - Greek letter Nu

ξ - Greek letter Xi

φ - Greek letter Phi

τ - Greek letter Tau

x - 1.c. letter "x"

x_{j-1} - 1.c. letter "x" subscript 1.c. letter "j" minus 1

x_{j+1} - 1.c. letter "x" subscript 1.c. letter "j" plus 1

x^{m} - 1.c. letter "x" superscript 1.c. letter "m"

x_{1} - 1.c. letter "x" subscript number 1

x_{n} - 1.c. letter "x" subscript 1.c. letter "n"

X - Capital letter "X"

X^{i} - Capital letter "X" superscript 1.c. letter "i"

X^{1} - Capital letter "X" superscript number 1

X^{n} - Capital letter "X" superscript 1.c. letter "n"

y - 1.c. letter "y"

y^{1} - 1.c. letter "y" superscript number 1

y^{n} - 1.c. letter "y" superscript 1.c. letter "n"

y^{i} - 1.c. letter "y" superscript 1.c. letter "i"

y_{j+1} - 1.c. letter "y" subscript 1.c. letter "j" plus number 1

y_{j-1} - 1.c. letter "y" subscript 1.c. letter "j" minus number 1

Y - Capital letter "Y"

Y^{i} - Capital letter "Y" superscript 1.c. letter "i"

Z - Capital letter "Z"

$\bigcap$ - Large intersection

$\bigcup$ - Large union

$\cap$ - Small intersection

$\cup$ - Small union

$\subset$ - Is contained

$\subseteq$ - Contained or equals

$\supseteq$ - Containing or equals

$\otimes$ - product sign

$<$ - Less than

$\leq$ - Less than or equal to

Ω - Greek letter Omega

$\bar{\Omega}$ - Greek letter Omega bar

ω - Greek letter l.c. Omega

$\bar{\omega}$ - Greek letter l.c. Omega bar

Ψ - Greek letter Psi

π - Greek letter l.c. Pi

Π - Greek letter Capital Pi

μ - Greek letter Mu

$\mu_{}$ - Greek letter Mu subscript l.c. letter "i"

μ_1 - Greek letter Mu subscipt number one

ϵ - Greek letter Epsilon

0 - zero

1 - number one

2 - number two

3 - number three

I - Roman numeral one (for tables)

II - Roman numeral two (for tables)

$f \circ s$ - l.c. letter f times l.c. letter s

$f \circ s_p$ - l.c. letter f times l.c. letter s subscript l.c. letter p

$\prod_{i=1}^{n}$ - Greek letter capital Pi super l.c. letter "n" sub l.c. letter i equals 1

$f: X \to Z$ l.c. letter f such that cap X yields capital Z

$f(x)$ - l.c. letter f times l.c. letter x in parentheses

$\tilde{f}: M \to Z$ l.c. letter f tilde such that cap M yields cap Z

$\tilde{f}(u) = f(x)$ l.c. letter f tilde times l.c. letter u equals l.c. letter f times l.c. letter x

pr_X - l.c. letter p, l.c. letter r subscript cap "X"

pr_Y - l.c. letter p, l.c. letter r subscript cap "Y"

$\mu(x)$ - Mu times l.c. letter "x"

$(\mu, \tilde{f})$ - Mu comma l.c. letter "f" tilde