Discussion Paper No. 1085

A LOWER BOUND ON COMPUTATIONAL COMPLEXITY GIVEN BY REVELATION MECHANISMS

by

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

March 1994

http://www.kellogg.nwu.edu/research/math/

[1] Department of Mathematics, Northwestern University.

[2] Department of Economics and Kellogg Graduate School of Management, Northwestern University. This research was supported by National Science Foundation Grant No. IRI-9020270.

A Lower Bound on Computational Complexity Given by Relevation Mechanisms

by

Kenneth R. Mount and Stanley Reiter

Introduction

This paper establishes an elementary lower bound on the computational complexity of smooth functions between Euclidean spaces. The main motivation for this comes from mechanism design theory. A typical mechanism design problem consists of a set of possible environments, a goal function, and a set of mechanisms from which choice is to be made. An *environment* includes specification of the possible characteristics of agents, such as possible actions, preferences and resource endowments, and a space of possible outcomes, such as trades among the agents, or allocations. A *goal function* (correspondence) associates a *desired outcome*, or set of them, to each possible environment.

A theory of design of economic mechanisms must eventually take into account the costs of setting up and operating the mechanisms. These costs include informational costs, and incentival costs. Important informational costs include those due to communication requirements and those due to the computations that are required by the mechanism; incentival costs include monitoring and enforcement costs, and deductions from first-best outcomes arising from incentive problems. In this paper we focus on the complexity of computational tasks, because complexity, along with prices of computational resources, determines computation costs.

The complexity of all computations required to operate the mechanism influence the costs associated with the mechanism. Complete analysis of these complexities would require complete specification of the computations involved, as illustrated in [16], but for some purposes it would be useful to have a lower bound on complexity obtained without having to specify in detail how computations are to be performed. In this paper we present such a lower bound applicable to any (smooth or discrete) function. We are particularly interested in functions mapping a product of Euclidean spaces (smooth manifolds) into a Euclidean space, i.e., in functions that are goal functions in a certain class of mechanism design problems.

The lower bound given here generalizes a lower bound due to Arbib and

Spira and described in [2] for the complexity of functions between finite sets. The Arbib-Spira bound is based on the concept of *separator sets* for a function, a concept that corresponds to the variables that the function actually depends on, and counts their number. A counting procedure cannot be used for functions between infinite sets. Instead, our analysis uses an equivalence relation that corresponds to separator sets in the finite case, and also generalizes to functions with infinite domains and ranges. The counting procedure is replaced by construction of a *universal object in a category*, namely the category of *adequate revelation mechanisms.* The universal object is a minimal adequate revelation mechanism called an *essential revelation mechanism.* The dimension (when it exists) of the message space of the universal object gives the number of variables. (Notice that while we have identified the minimum number of variables needed to compute the value of a given function with the dimension of the message space of a certain minimal revelation mechanism, the dimension of this message space is typically not the minimal message space needed to *realize* the given function by a decentralized process. The minimal message space needed to realize the goal function is typically smaller than the message space of the essential revelation mechanism, and is an indicator of communication complexity, rather than computational complexity. We are here concerned with the computational complexity; minimal message spaces are introduced only as a technique of analysis.)

While we use a concept from category theory, our analysis is self-contained and does not require knowledge of category theory beyond the concept of a universal object in a category. This concept is not new to economic theory; Sonnenschein [28] and Jordan [8] have used it in analyzing economic mechanisms. Their work is discussed briefly in section 4.

Revelation mechanisms, and adequate revelation mechanisms, are, of course, subclasses of decentralized verification mechanisms. The size of the message space of such mechanisms has been studied extensively, and conditions have been obtained that provide a lower bound on the dimension of the message space of mechanisms that realize a given goal function. Among these are rank conditions on certain matrices of second partial derivatives of the goal function under study, namely, bordered Hessian matrices. A lower bound on the dimension of the message space of decentralized verification mechanisms which depends of the rank of a bordered Hessian matrix of the goal function is given by Hurwicz, see [5], and a related one by Chen [3]. Abelson [1] gives a lower bound on the *communication complexity* of a distributed computation of a smooth function also involving a rank condition on a bordered Hessian of the function. The lower bound given in this paper on the *computational complexity* of a smooth function also depends on rank conditions on bordered Hessian matrices, but they are different matrices, functional rather than numerical, and different conditions. The lower bounds obtained by Hurwicz, Chen and Abelson, when applied to revelation mechanisms, also yield lower bounds on computational complexity, but these bounds are typically too low. The relation between our results and those of Hurwicz, Chen and Abelson are discussed in section 3.

Analyses of mechanisms found in the literature can be classified using three factors: whether they do or do not take into account (i) costs due to incentives; (ii) costs due to information processing; (iii) whether they deal with static mechanisms, i.e., equilibrium or verification mechanisms, or dynamic ones, i.e., adjustment or learning processes. Further, informational costs include both costs due to communication and those due to computation.

For example, implementation theory takes account of incentives, considers equilibrium mechanisms, but typically ignores informational costs. Message exchange processes, such as the adjustment processes summarized in [5], in some cases take account of incentives, (see [6]) and in some do not. Typically they do take account of informational costs, and are dynamic. Equilibrium message mechanisms are, of course, static, typically take account of communication requirements, and may or may not take account of incentives. In [18], [19], and [20] the models are static and treat both incentives and communication requirements. In [13] the mechanisms are static and only communication requirements are considered. In [26], [9], [15], and [30] incentives are ignored, and the communication requirements of locally stable dynamic mechanisms are analyzed. There are also other types of mechanisms, such as algorithms designed to converge to the value of the goal function starting from an initial state depending on the environment, or to compute the value of the goal function directly, as in [23], and [24].[1]

In each of these cases the complexity of *all* the functions that must be computed in order to operate a mechanism influences the costs associated with the mechanism. The lower bound on computational complexity applies

[1] Computational complexity of mechanisms has not been studied much. We are not aware of any analysis except for the example studied in [16]. However, computational complexity of players or strategies have been studied in repeated games, (see [10], [17], and [25] for example).

to any of these functions. It does so via an analysis that begins by considering the function to be analyzed to be a goal function, and finding the dimension of the universal object in the category of adequate revelation mechanisms that realize that goal function. However, we focus on obtaining a lower bound on the complexity of all the computations entailed by a mechanism that either realizes or implements a given goal function, i.e., a verification mechanism, or a game form, based on the fact that any such mechanism must in fact compute the goal function. Since we make use of the formal structure of informationally decentralized equilibrium or verification mechanisms, to make the exposition self-contained, we give a brief summary of them.

Privacy Preserving Mechanisms

There are N, a finite number, economic agents each of whom has a *space of characteristics*. Let E^i denote the space of characteristics of agent i (such as her preference relations). It is assumed that the information about the joint environment $e = (e^1, \ldots, e^N)$ is distributed among the agents so that agent i knows only her characteristic e^i. Given is a function $F : E^1 \times \ldots \times E^N \rightarrow Z$, called the *goal function* that expresses the goal of economic activity. For example, for each $e = (e^1, \ldots, e^N)$ in $E^1 \times \ldots E^N$, $F(e)$ is the Walrasian allocation (or trade). Agents communicate by exchanging messages drawn from a *message space* denoted M. The final or *consensus message,* also called the *equilibrium message,* for the environment e is given by a correspondence

$$\mu : E^1 \times \ldots \times E^N \rightarrow M.$$

Equilibrium messages are translated into outcomes by an *outcome function* $h : M \rightarrow Z$.

A *mechanism* $\pi = (M, \mu, h)$ is said to *realize* the goal function F [2] on E if for all e in E,

$$F(e) = h(\mu(e)).$$

The mechanism (M, μ, h) is called *privacy preserving* if there exist correspondences $\mu^i : E^i \rightarrow M$, for $i = 1, \ldots, N$, such that for all e in E,

$$\mu(e) = \mu^1(e^1) \cap \mu^2(e^2) \cap \ldots \cap \mu^N(e^N).$$

[2] More generally, F can be a correspondence, in which case the definition of realizing F must be modified, as in [5].

This condition states that the set of equilibrium message complexes acceptable to agent i can depend on the environment only through the component e^i. The component e^i is, according to the assumption made above, everything that i knows about the environment.

From now on we focus on the case in which the characteristics of the agents are given by real parameters. It has been shown (see [5] and the references given there) that the inverse image of a point m in the message space M is a rectangle contained in the level set $F^{-1}(h(m))$. This fact, in the presence of appropriate smoothness conditions, allows one to compute a lower bound on the dimension of the message space of a privacy preserving mechanism that realizes F. (See [7] or [5]). In the smooth case, the dimension of the message space is a measure of its informational size which is in turn an important indicator of certain costs of communication entailed by the mechanism.

Specifically, according to the verification scenario (see [5], p.244), a candidate equilibrium message is announced to each agent, who independently determines whether it is or is not an equilibrium from her standpoint, i.e., an element of $\mu^i(e^i)$. A lower bound on the dimension of the message space determines how much communication or channel capacity is required for a verification mechanism, and therefore a lower bound on at least the capital cost of the communication system.

Going beyond verification mechanisms while still staying in the static framework, we consider mechanisms that find equilibrium, rather than just verifying given candidates. Since equilibrium messages are given as the intersection of individual message correspondences, finding equilibrium entails finding that intersection. In the static framework this amounts to computing the intersection, e.g., in the case of the competitive mechanism, solving the system of excess demand equations set equal to zero.[3]

Suppose that some institution or agent has the task of computing the intersection of the sets $\mu^i(e^i)$. A complete design of the mechanism would specify how the intersection is to be computed, and in what form the agents transmit their messages to the computer. For instance, the program that

[3] The literature on local stability of message equilibria cited above looks at the problem of finding equilibrium as one of converging to it by an adjustment process. That literature shows that we need a larger message space than the smallest one that suffices for static realization. But complexity of computations involved in the adjustment process has not been addressed in that literature.

computes the intersection of sets might accept only a finite number of real numbers as inputs, thereby requiring that the sets $\mu^i(e^i)$ be identified by finitely many real parameters–e.g., $\mu^i(e^i)$ might be a line, or the zeros of a polynomial of degree k. Rather than to require that the mechanisms under consideration be specified completely as to the form in which the message correspondences are transmitted and what algorithm is used to compute the intersection, we seek a lower bound on the complexity of the computation based on information about the goal function alone. That is, a lower bound on the complexity of computing F is also a lower bound on computing F by computing the equilibrium message and the outcome function of a decentralized mechanism. We turn to the problem of finding bounds on the computational complexity of a function.

Complexity of Functions

The complexity of a function F depends in part on the model of computation used. An explicit model of computation is formulated in [14]; as in other models of computation the number of variables on which a function depends determines a lower bound on the complexity of the function. A function of two variables is, other things equal, more complicated than a function of one variable provided that the function of two variables cannot be written as a function of one variable.

Suppose that F is a real valued function defined on the Euclidean space R^2, where the Euclidean space has specified coordinates, x and y. Then the number of coordinates required to compute F is usually easy to estimate by computing the number of nonzero partial derivatives. For example, the function $F(x,y) = x + y^2$ has partials in x and y that are both nonzero. One might be tempted to think that $F(x,y)$ is a function more complex than, say, the function x. However, if one treats R^2 as a differentiable manifold, where smooth coordinate changes are allowed, then the function $F(x,y)$ can be introduced as a coordinate function on R^2, so that R^2 has coordinates $F(x,y)$ and y. Having done that, $F(x,y)$ is a function of the one parameter the value of F, and is no more complex than x. Thus, the possibility of unrestricted (smooth) coordinate changes invalidates using the number of nonzero partial derivatives of F, i.e., the number of variables on which F apparently depends, as an indicator of its complexity.

Another view of this is as follows. Define an equivalence relation according to which two points a and a' in R^2 are equivalent if F takes the same value at a and a'. The level sets of F are the equivalence classes of this equivalence relation. This set of equivalence classes is a one dimensional family (indexed by the values of F), and hence is no more complex than the level sets of the function x.

However, in the case of the computation of a goal function that is defined on a product of manifolds $X^1 \times \ldots \times X^n$ there is a natural restriction on the coordinates changes allowed in the product $X^1 \times \ldots \times X^n$. The restriction is that the only coordinate changes allowed are the ones that are the product of individual coordinate changes in each of the separate spaces X^i. With this restriction on coordinate changes, one can then ask if there is a lower bound on the number of parameters from coordinates systems in X^i required to compute F.

For example if $X = R^2$ with coordinates x_1 and x_2 and $Y = R^2$ with coordinates y_1 and y_2 and if $G(x_1, x_2; y_1, y_2) = x_1 y_1 + x_2 y_2$, then the restriction that a coordinate change is allowable only if it is the product of a coordinate change in X and a coordinate change in Y leads to the conclusion that all four of the parameters x_1, y_1, x_2 and y_2 are required for the evaluation of G. To see this one can describe the level sets the function $G(x_1, x_2; y_1, y_2)$, with the restriction that two points a and b in X are equivalent only if $G(a; \underline{y}) = G(b; \underline{y})$ independent of the point $\underline{y}$ chosen in Y. Then a and b are equivalent only if $a = b$. Indeed, if $a = (a_1, a_2) \neq b = (b_1, b_2)$ where $a_1 \neq b_1$ then there exist y_1 so that $G(a_1, a_2; y_1, 0) \neq G(b_1, b_2; y_1, 0)$. A similar argument applies if $a_2 \neq b_2$. Thus to compute G one needs sufficiently many parameters to distinguish between each two points of X; that is, one needs two parameters from X. Similarly, one needs two parameters from Y.

In the model of [14, 16] there is a network of processors, consisting of a set of processors connected by a directed graph, which computes as follows.

Each processor p receives the values of its inputs, say, $x^1, \ldots, x^s$, from outside the network, or from immediately preceding processors, and computes in one unit of time the value of a function $y = f_p(x^1, \ldots, x^s)$. Here $s \leq r$, r a given parameter, x^i can be a vector of some fixed dimension, say, d, and f_p belongs to a specified class $\mathcal{F}$ of functions. Each processor sends the value of the function it computes to every successor, i.e., to every processor to which it is directly connected, or to outside the network.

A network of this kind is said to compute a function

$$F : E^1 \times E^2 \times \ldots \times E^N \rightarrow Z$$

in time t if there is an initial state of the network such that when the values $e^1, \ldots, e^N$ are constantly fed into the network starting from time 0, the value of $F(e^1, \ldots, e^N)$ appears as output of the network at time t.

A fundamental question then emerges. How long does it take to compute a given function F? The complexity of F relative to the class of networks characterized by r and $\mathcal{F}$ is the minimum over all such networks of the time needed to compute F. (If the time is infinite, then F is said to be not computable by networks in the class characterized by r and $\mathcal{F}$.) A lower bound on the complexity of F depends on the number of variables on which F "really" depends. As we have indicated above, we obtain a lower bound on the time required to compute a function by reformulating the separator set approach of Arbib and Spira.

Separator Sets and Quotients

We next present our formulation of the concept of separator sets for a function in terms of an equivalence relation induced on each of the sets E^i by the function F. To begin with, this is stated set theoretically without topological or smoothness conditions on the sets E^i. The quotient constructions are quite elementary when smoothness conditions are ignored. This makes parts of the construction more transparent. Furthermore, when the E^i are differentiable manifolds the set theoretic constructions are used to establish the existence of certain required functions, for which appropriate smoothness conditions can then be verified.

The cardinality conditions used in the counting arguments of Arbib and Spira are replaced by universal mapping conditions. Universal mapping properties have been used by other authors in order to classify economic mechanisms. In particular [24] characterized a version of the competitive mechanism in relation to a certain class of mechanisms, and [8] established that the competitive mechanism is unique among mechanisms in a somewhat different class by constructing a mapping that shows it is a universal object in that class.

We describe the number of variables required to compute a function by constructing appropriate quotients. The construction we use is a natural generalization of the argument we used in the discussion of the function $G(x_1, x_2; y_1, y_2)$. The construction of a quotient object has the natural set theoretic structure of a universal object. Having done that, the major part of this paper is used to show that under a set of rank conditions on matrices associated with differentiable functions, the quotient object also has the structure of a differentiable manifold. The manifold structure on the quotient is required to be able to conclude that the dimension of the quotient exists as a topological concept and that dimension of the quotient is the number of variables required in order to compute the function. The universal condition guarantees that the quotient object is a space with the least number of variables required to compute the function.

Specifically, for a function $F : E^1 \times \ldots \times E^N \rightarrow Z$ we establish the existence of a collection of sets (E^i/F), $1 \leq i \leq N$,functions $q^i : E^i \rightarrow (E^i/F)$, and a function $F^* : (E^1/F) \times \ldots (E^N/F) \rightarrow Z$ that together satisfy the following conditions. First, the composition

$$F^* \circ (q^1 \times \ldots \times q^N) = F,$$

and second, if there are functions

$$p^i : E^i \rightarrow X^i$$

and

$$H^i : X^1 \times \ldots \times X^N \rightarrow Z$$

for which

$$H \circ (p^1 \times \ldots \times p^N) = F,$$

then there are (one can construct) unique functions

$$\rho^i : X^i \rightarrow (E^i/F), \quad 1 \leq i \leq N,$$

such that

$$\rho^i \circ p^i = q^i,$$

and

$$H = F^* \circ (\rho^1, \ldots, \rho^N).$$

These conditions state that the quotient object $(E^1/F) \times \ldots \times (E^N/F)$ is *universal*, a concept to be discussed further. (The term 'universal object' is used in category theory to describe objects that allow each object of the category to be specified by identifying a mapping to (or from) the universal object [13]).

If the sets E^i are finite, then the cardinality of the set (E^i/F) is an upper bound on the cardinality of the corresponding Arbib-Spira separator sets. Furthermore, each separator set in E^i is the image of a subset of (E^i/F) under some thread of q^i. By a thread of q^i we mean a function t from (E^i/F) to E^i such that $q^i \circ t$ is the identity function.

Next we assume that each E^i is a differentiable manifold with appropriate smoothness. If in some coordinate system $(x_1, \ldots, x_t)$ around a point in E^1 (say) it were possible to ignore the coordinate x_t and still to evaluate F, then knowledge of the coordinates $(x_1, \ldots, x_{t-1})$ would be adequate, at least locally. That is, F would depend on no more than the first $t-1$ variables. In this case the manifold E^i can be replaced, locally, by the quotient induced by the equivalence relation "$(x_1, \ldots, x_{t-1}, x_t) \approx (x_1, \ldots, x_{t-1}, x_t')$" if and only if $F(x_1, \ldots, x_{t-1}, x_t) = F(x_1, \ldots, x_{t-1}, x_t')$. However, it is possible that even if in a given coordinate system no variable can be eliminated, a change of coordinates can be introduced that leads to a reduction of the number of variables required to compute F. Therefore, we seek a "good" coordinate system by looking for a "good" quotient. The equivalence relation we use is "$\approx$".

In the case of smooth manifolds the quotient using the relation "$\approx$" may not have the structure of a smooth manifold for which the quotient map is differentiable. On the other hand, when such a structure does exist, then separator sets are again the image of subsets of the quotient under threads of the quotient map.

Conditions are imposed that ensures that $(E^1/F) \times \ldots \times (E^N/F)$, the quotient object, is a topological manifold. In that case, the dimension of the quotient manifold counts the number of variables required.

When we impose the existence of certain local threads, then this quotient object satisfies the universality conditions.

(We do not know that there is such a universal object that also is as smooth as the original product $E^1 \times \ldots E^N$. Possibly Godement's Theorem ([26], p.LG 3.27) might resolve this difficulty.)

If the quotient map is one-to-one then no reduction in the number of variables is possible no matter what coordinate system is used.

Algebraic Conditions

An algebraic characterization of the number of variables required to compute a given function F is obtained from a theorem of Leontief [11]. Abelson [1] used this result to construct a lower bound on the communication complexity of F in a distributed system. The conditions we use for the construction of a "good" quotient of E^1 where $F : E^1 \times \ldots \times E^N \rightarrow R$, are rank conditions on the bordered Hessian $BH(F)$. The matrix $BH(F)$ has rows indexed by coordinates x_i from E^1, and columns indexed by F and by the coordinates y_j from $E^2 \times \ldots \times E^N$ with the (x_i, F) entry being $(\partial F/\partial x_i)$ and the (x_i, y_j) entry being $(\partial^2 F/\partial x_i \partial y_j)$. The Hessian, $H(F)$, is the sub-matrix of the bordered Hessian that consists of the columns other than column F.

In the case that $N = 2$, when the goal function maps a product $R^{k_1} \times R^{k_2}$ to R, the matrix $BH(F)$ is a submatrix of the Full Bordered Hessian, $FBH(F)$. The Full Bordered Hessian is the Bordered Hessian with a row added indexed by F. The entry in (F, F) position is 0. The (F, y_j) entry is $\partial F/\partial y_j$.

We use conditions on the submatrix $BH(F)$ of the Full Bordered Hessian to guarantee the existence of a manifold structure on the quotient objects (E^i/F). If at each point x of E^1 the matrix $BH\mid_x$ has rank r and $H\mid_{x,y}$ also has rank r at each point x of E^1 and each point y of $E^2 \times \ldots \times E^N$, then the quotient of E^1 under the equivalence relation "$\approx$" is a manifold of dimension r.

As an example, consider the function $K(x_1, x_2, y_1, y_2) =$

$$x_1 y_1 + x_2^2 y_1 + 2x_1 y_2^2 + 2x_2^2 y_2^2 = (y_1 + 2y_2^2)(x_1 + x_2^2)$$

where the variables are all scalars.

No variable can be eliminated and still permit the function to be evaluated in terms of the remaining variables. Indeed, no linear change of coordinates can reduce the number of variables required. This is indicated by the fact that the Hessian of K, with rows and columns indexed by all variables x_1, x_2, y_1, y_2, has rank 4.

However, the (nonlinear) change of coordinates given by

$$\zeta = (x_1 + x_2^2), \eta = (y_1 + 2y_2^2),$$

permits K to be written in terms of only two variables, namely,

$$K(x_1, x_2; y_1, y_2) = \zeta\eta.$$

The matrices $H\mid_{x,y}$ and $BH\mid_x$ both have rank equal to 1.

Universal Objects and Revelation Mechanisms

We have noted that the quotient manifold we construct serves as a universal object. The concept of universal object comes from category theory. Our use of universal objects and their properties does not require the panoply of category theory. To specify the objects, we use a special type of privacy preserving mechanism in which the message space is a product. We do this because our purpose is to find the minimum number of variables each agent separately must send in order that the goal function can be computed. The sum of these numbers across all agents is used to find a lower bound on computation. This sum is *not* a lower bound on communication. Even though the dimensions we seek are not lower bounds on the dimension of messages spaces used in the study of the realization of goal functions, the mechanism paradigm is a very useful way of attacking the problem of discovering the minimum number of variables required to compute a function. In the mechanism we use each agent's message space is his parameter space, i.e. a revelation mechanism. A slight generalization, which we call an *adequate revelation mechanism*, allows the possibility that not all the individual parameters are revealed. If mechanisms of this type that realize a particular function have a universal object, then that object is called the *essential revelation mechanism,* and it is uniquely determined to within isomorphism. This universal object (mechanism) exists when certain Hessian conditions (and some smoothness assumptions) are satisfied. It is the product $(E^1/F) \times \ldots \times (E^N/F)$, with a differentiable manifold structure on each (E^i/F). The universal object gives a lower bound on the number of variables each agent must reveal in order to permit the function F to be evaluated, that is, the number of variables on which F really depends, when nonlinear coordinate changes are allowed.

The remainder of the paper is organized as follows. Section 1 contains the set theoretic constructions used subsequently. Definitions of F-equivalence, of adequate and essential revelation mechanisms are given. It is established (Lemma 1.1 and Theorem 1.1) that the essential revelation mechanism for a given function is the smallest adequate revelation mechanism for F. Moreover, we show that it is the (unique) adequate revelation mechanism that serves as a universal object in the category of adequate revelation mechanisms.

Section 2 deals with the case where the sets E^i (or X^i) are smooth manifolds and F is smooth. Simple conditions are given that ensure that the quotient sets are topological manifolds.

The matrices used in the analysis are defined, and the concept of differentiable separability is defined. The main results concerning universality of the essential revelation mechanism for a function are established.

In Section 3 we discuss the relations between our constructions and the Theorems of Hurwicz, Chen and Abelson.

In Section 4 we include a presentation of the universality results of Sonnenschein and Jordan.

The results on adequate revelation mechanisms in Section 2 require a slightly altered version of Leontief's theorem. This is related to a result announced by [1]. The three propositions, Lemma A.1, Theorem A.2 and Theorem A.3 present this material. They and their proofs are given in Appendix A. Appendix A also includes an example of the constructions required.

Section 1. Initial set theoretic constructions

Notation. If X_j, $1 \leq j \leq n$, are sets, then $X_{<-j>}$ denotes the set

$$X_1 \times \ldots \times X_{j-1} \times X_{j+1} \times \ldots \times X_n.$$

If $x \in X_j$ and if $z = (z_1, \ldots, z_{j-1}, z_{j+1}, \ldots, z_n) \in X_{<-j>}$, then $x \int_j z$ denotes the element

$$(z_1, \ldots, z_{j-1}, x, z_{j+1}, \ldots, z_n) \text{ of } X_1 \times \ldots \times X_n.$$

F-Equivalence

Definition 1.1. Suppose that X_i, $1 \leq i \leq n$, and Y are sets, suppose that $F : \prod_{i=1}^n X_i \to Y$ is a function, and suppose that $1 \leq j \leq n$. Two points x and x' in X_j are F-equivalent in X_j if for each $z \in X_{<-j>}$, $F(x \int_j z) = F(x' \int_j z)$.

It is elementary that F-equivalence in X_j is an equivalence relation on points of X_j. Denote by (X_j/F) the collection of F-equivalence classes of X_j. Set q_j equal to the quotient map from X_j to (X_j/F).

The following lemma establishes the sense in which the set $(X_1/F) \times \ldots \times (X_n/F)$ is the smallest product set through which F factors.

Lemma 1.1. *Suppose that $X_1, \ldots, X_n$, and Y are sets and suppose that $F : X_1 \times \ldots \times X_n \to Y$ is a function. There is a unique function $F^* : (X_1/F) \times \ldots \times (X_n/F) \to Y$ that makes the Diagram 1.1 commute. Furthermore, if $Z_1, \ldots, Z_n$ are sets, and if there are functions $g_i : X_i \to Z_i$, $1 \leq i \leq n$, and a function $G : Z_1 \times \ldots \times Z_n \to Y$ that makes Diagram 1.2 commute, then there are uniquely determined maps $g_1^*, \ldots, g_n^*$, $g_i^* : Z_i \to (X_i/F)$, that make Diagram 1.3 commute.*

$$\begin{tikzcd}
X_1 \arrow[d, "q_1"] & \times & \cdots & \times & X_n \arrow[d, "q_n"'] \arrow[r, "F"] & Y \\
(X_1/F) & \times & \cdots & \times & (X_n/F) \arrow[ur, "F^*"'] &
\end{tikzcd}$$

Diagram 1.1

$$\begin{tikzcd}
X_1 \arrow[d, "g_1"] & \times & \cdots & \times & X_n \arrow[d, "g_n"'] \arrow[r, "F"] & Y \\
Z_1 & \times & \cdots & \times & Z_n \arrow[ur, "G"'] &
\end{tikzcd}$$

Diagram 1.2

Proof of Lemma 1.1.

We first show that if $g_i : X_i \to Z_i$ and $G : \prod_1^n Z_i \to Y$ are functions that make Diagram 1.2 commute, then we can factor the map $\prod_1^n g_i$ through the product $\prod_1^n (X_i/F)$. If $z \in Z_i$, choose $x, x' \in X_i$ such that $g_i(x') = g_i(x) = z$. For each $w \in X_{<-i>}$, set

$$g(w) = (g_1(w_1), \ldots, g_{i-1}(w_{i-1}), g_{i+1}(w_{i+1}), \ldots, g_n(w_n)) \in Z_{<-i>}.$$

Then

$$F(x \underset{i}{\int} w) = G(g_i(x) \underset{i}{\int} g(w)) = G(g_i(x') \underset{i}{\int} g(w)) = F(x' \underset{i}{\int} w).$$

It follows that for each i, $q_i(x) = q_i(x')$. Therefore setting $g_i^*(z) = g_i(x)$ defines a function g^*i from Z_i to $X_i/F)$. It is clear that Diagram 1.3 commutes.

To see the uniqueness of the maps g_i^*, note that if $h_i^* : Z_i \to (X_i/F)$, $1 \leq i \leq n$, are maps that make Diagram 1.3 commute when used in place of the maps g^*i, then for each $z \in Z_i$ and each $x \in X_i$ so that $g_i(x) = z$, it follows that

$$g_i^*(z) = g_i^*(g_i(x)) = q_i(x) = h_i^*(g_i(x)) = h_i^*(z).\Box$$

$$\begin{tikzcd}
X_1 \arrow[dd, "g_1"'] \arrow[dr, "q_1"] & & & & X_n \arrow[dl, "q_n"'] \arrow[dr, "F"] \arrow[dd, "g_n", "F^*"'] & \\
& (X_1/F)\times & \cdots & \times\,(X_n/F) \arrow[rr, "F^*"] & & Y \\
Z_1 \arrow[ur, "g_1^*"'] & & & & Z_n \arrow[ul, "g_n^*"] \arrow[ur, "G"'] &
\end{tikzcd}$$

Diagram 1.3

Adequate and Essential Revelation Mechanisms

Definition 1.2. Suppose that X_i ,$1 \leq i \leq n$, and Z are sets and suppose that $F : X_1 \times \ldots \times X_n \to Z$ is a function. An *adequate revelation mechanism realizing* F is a triple $(g_1 \times \ldots \times g_n, M_1 \times \ldots \times M_n, h)$ that consists of:

(i) a product of sets $M_1 \times \ldots \times M_n$,

(ii) a collection of functions $g_i : X_i \to M_i$, $1 \leq i \leq n$,

(iii) a function $h : M_1 \times \ldots \times M_n \to Z$, such that for each

$$(x_1, \ldots, x_n) \in X_1 \times \ldots \times X_n, \quad F(x_1, \ldots, x_n) = h(g_1(x_1), \ldots, g_n(x_n)).$$

Using the notation of Lemma 1.1, the triple

$$(q_1 \times \ldots \times q_n, (X_1/F) \times \ldots \times (X_n/F), F^*)$$

is an adequate revelation mechanism called the *essential revelation mechanism.*

If $(g_1 \times \ldots \times g_n, M_1 \times \ldots \times M_n, h)$ is an adequate revelation mechanism, then $M_1 \times \ldots \times M_n$ is an *adequate revelation message space.* The map $g_1 \times \ldots \times g_n$ is the *message function* of the adequate revelation mechanism.

Universality of the Essential Revelation Mechanism

The following theorem is a restatement of Lemma 1.1 in terms of adequate revelation mechanisms. It establishes the sense in which the essential revelation mechanism is the smallest adequate revelation mechanism. It states that not only is $M_1 \times \ldots \times M_n$ the product with the smallest cardinality that can be used as the message space for an adequate revelation mechanism, but it is also the case that for every other product space that acts as a message space for an adequate revelation mechanism that realizes F there is a product map onto $M_1 \times \ldots \times M_n$. This is characteristic of a universal object in the sense of category theory. Theorem 1.1 states that the essential revelation mechanism is a universal object in the category of adequate revelation mechanisms.

Theorem 1.1. *Suppose that X_i, $1 \leq i \leq n$, and Z are nonempty sets and suppose that $F : X_1 \times \ldots \times X_n \rightarrow Z$ is a function.*

(i) The triple

$$(q_1 \times \ldots \times q_n, (X_1/F) \times \ldots \times (X_n/F), F^*)$$

is an adequate revelation mechanism that realizes F;

(ii) The message function for any other adequate revelation mechanism factors through $(X_1/F) \times \ldots \times (X_n/F)$;

(iii) The set $(X_1/F) \times \ldots \times (X_n/F)$ is the smallest set in cardinality that can be used as an adequate revelation message space for a mechanism that realizes F;

(iv) Finally, the essential revelation mechanism is the unique adequate revelation mechanism (to within isomorphism) through which all adequate revelation mechanisms that realize F factor.

Section 2. The topological case.

When the X_i are topological manifolds and when F is continuous, it is in general not true that the sets (X_i/F) are manifolds. Even a high degree of smoothness of F is insufficient to guarantee that (X_i/F) is a topological manifold. However, when the (X_i/F) are Hausdorff, a fairly simple condition on the Jacobian of F coupled with a global separation condition does imply that the (X_i/F) are manifolds. When these conditions are satisfied, the essential revelation mechanism has the structure of a manifold, and the dimensions of the (X_i/F) can be used to establish a lower bound on the number of variables, i.e. the number of functions in a coordinate system, that must be passed to a central processor in order to compute F. This number determines a lower bound for the complexity of the function F.

In this section we introduce the concept of differentiable separability, which is the Jacobian condition that will be used. We then give simple global conditions on the function F to ensure that the sets (X_i/F) are topological manifolds. We begin with some concepts from differential geometry (c.f.[4]).

Definition 2.1. Let X and Y be differentiable manifolds. Let $\Phi : X \to Y$ be a differentiable mapping. If at a point $p \in X$ the mapping Φ has maximum rank, and if dim X $\geq$ dim Y, then Φ is said to be a *submersion at p.* If Φ is a submersion at each point of X, then Φ is a *submersion.* If a map $g : X \to Y$ is a submersion, then it is known(c.f.[4,p.9]) that the map can be linearized (rectified). That is, if dim(X)=n, dim(Y)=m, and if $p \in X$, we can choose coordinates $x_1, \ldots, x_n$ in a neighborhood U of p, and coordinates $y_1, \ldots, y_m$, in a neighborhood of g(p) so that for each $q \in U$, $g(q) = (x_1(q), \ldots, x_m(q))$.

Next we introduce a collection of matrices that are generalizations of matrices used by Leontief in [11].

Suppose $E^1, \ldots, E^n$, are Euclidean spaces of dimensions $d(1), \ldots, d(n)$, such that the space E^i, $1 \leq i \leq n$ has coordinates $\underline{x}_i = (x_{i1}, \ldots, x_{id(i)})$. Assume that $(\underline{p}_1, \ldots, \underline{p}_n)$ is a point of $E^1 \times \ldots \times E^n$, and assume that U_i is an open neighborhood of the point $\underline{p}_i$, $1 \leq i \leq n$. We assume that F is a real valued C^2-function defined on $U_1 \times \ldots \times U_n$. We require four matrices.

(I): The matrix

$$BH(F : x_{i1}, \ldots, x_{id(i)}; x_{11}, \ldots, x_{i-1d(i-1)}, x_{i+11}, \ldots, x_{nd(n)}) =$$

$$BH(F : \underline{x}_i; \underline{x}_{<-i>})$$

is a matrix that has rows indexed by $x_{i1}, \ldots, x_{id(i)}$ and columns indexed by $F, x_{11}, \ldots, x_{(i-1)d(i-1)}, x_{(i+1)1}, \ldots, x_{n\,d(n)}$. The entry in the x_{iu} row and in the F column is $\partial F/\partial x_{iu}$. The entry in row x_{iu} and in column x_{jw} is $\partial^2 F/\partial x_{iu}\partial x_{jw}$.

(II): The matrix $H(F : \underline{x}_i; \underline{x}_{<-i>})$ is the submatrix of $BH(F : \underline{x}_i; \underline{x}_{<-i>})$ that consists of the columns indexed by $x_{uv}, \quad u \in \{1, \ldots, i-1, i+1, \ldots, n\}$ and $1 \leq v \leq d(u)$. In other words, we derive H from BH by eliminating the column indexed by the function F.

In case that the number of Euclidean spaces is two, so that $F : E^1 \times E^2 \rightarrow R$, we use a slightly less cumbersome notation. Suppose that E^1 has coordinates $(x_1, \ldots, x_p)$ and E^2 has coordinates $(y_1, \ldots, y_q)$. We use as row indices for $BH(F : x_1, \ldots, x_p; y_1, \ldots, y_q)$ the variables $x_1, \ldots, x_p$ and as column indices F, $y_1, \ldots, y_q$. The $(x_i, F)^{th}$ entry in $BH(F : x_1, \ldots, x_p; y_1, \ldots, y_q)$ is $\partial F/\partial x_i$ and the $(x_i, y_j)^{th}$ entry is $\partial^2 F/\partial x_i \partial y_j$.

The matrices $H(F : \underline{x}_i; \underline{x}_{<-i>})$ and $BH(F : \underline{x}_i; \underline{x}_{<-i>})$ are matrices of functions in the coordinates $\underline{x}_1, \ldots, \underline{x}_n$ of $E^1 \times \ldots \times E^n$. The conditions we place on the matrices BH and H require that some, but not all, of the variables are to be evaluated at a point. When that partial evaluation takes place we indicate this by adding an asterisk to the H or BH. Specifically,

(III): The matrix $BH^*(F : \underline{x}_i; \underline{x}_{<-i>})[\underline{x}_i, \underline{p}_{<-i>}]$ is the matrix that results from evaluating the variables $\underline{x}_1, \ldots \underline{x}_{i-1}, \underline{x}_{i+1}, \ldots, \underline{x}_n$ of the entries of $BH(F : \underline{x}_i; \underline{x}_{<-i>})$ at the point $p_{<-i>} = (\underline{p}_1, \ldots, \underline{p}_{i-1}, \underline{p}_{i+1}, \ldots, \underline{p}_n)$. The matrix $BH^*(F : \underline{x}_i; \underline{x}_{<-i>})[\underline{x}_i, \underline{p}_{<-i>}]$ is a function of the variables $x_{i1}, \ldots, x_{id(i)}$ alone.

(IV): Similarly, the matrix

$$H^*(F : \underline{x}_i; \underline{x}_{<-i>})[\underline{x}_i, \underline{p}_{<-i>}]$$

is the submatrix of

$$BH^*(F : \underline{x}_i; \underline{x}_{<-i>})[\underline{x}_i, \underline{p}_{<-i>}]$$

derived by deleting the column indexed by F.

Differential Separability

Definition 2.2. Suppose $X_1, \ldots, X_n$ are differentiable manifolds, where for each $1 \leq i \leq n$, X_i has dimension $d(i)$. Suppose that $p_i \in X_i, \quad 1 \leq$

$i \leq n$, and suppose that for each i, $\phi_{i1}, \ldots, \phi_{id(i)}$ is a coordinate system in an open neighborhood U_i of p_i. Suppose that $F : \prod_{i=1}^{n} X_i \rightarrow R$ is a C^2-function. Assume that for $1 \leq i \leq n$, $\phi_i = \prod_j \phi_{ij}$ maps U_i into an open neighborhood V_i of the origin 0_i of a Euclidean space $E^i = R^{d(i)}$ and that ϕ_i carries p_i to 0_i. We assume that E^i has coordinates $x_{i1}, \ldots, x_{id(i)}$. The function F is said to be *differentiably separable of rank* $(r_1, \ldots, r_n)$ *at the point* $(p_1, \ldots, p_n)$ *in the coordinate system* $\phi_{11}, \ldots, \phi_{nd(n)}$ if for each $1 \leq i \leq n$, the matrices $BH(F \circ (\prod \phi_t)^{-1} : x_{i1}, \ldots, x_{id(i)}; x_{<-i>})$ and $H^*(F \circ (\prod \phi_t)^{-1} : x_{i1}, \ldots, x_{id(i)}; x_{<-i>})[x_i, 0_{<-i>}]$ have rank r_i in a neighborhood of $(0_1, \ldots, 0_n)$. If F is differentiably separable of rank $(r_1, \ldots, r_n)$ at $(p_1, \ldots, p_n)$, and if $r_i = \dim(X_i)$ for each $1 \leq i \leq n$, then we will say that F is *differentiably separable at* $(p_1, \ldots, p_n)$.

The following lemma notes that the ranks of the Hessians used in the previous definition are unchanged by coordinate changes. The proof is a simple computation.

Lemma 2.1. *Suppose that for* $1 \leq i \leq n$, X_i *and* Y_i *are* C^2- *manifolds and suppose that* $h_i : Y_i \rightarrow X_i$ *is a* C^2-*diffeomorphism. Assume that* $g : \prod_{i=1}^{n} Y_i \rightarrow R$ *and* $F : \prod_{i=1}^{n} X_i \rightarrow R$ *are* C^2- *functions such that* $g = \prod h_i \circ F$. *Suppose that* $(q_1, \ldots, q_n) \in \prod_i Y_i$ *and let* $h_i(q_i) = (p_i)$. *If F is differentiably separable of rank* $(r_1, \ldots, r_n)$ *at* $(p_1, \ldots, p_n)$, *then g is differentiably separable of rank* $(r_1, \ldots, r_n)$ *at* $(q_1, \ldots, q_n)$.

We can now define the term differentiably separable for a function defined on a differentiable manifold.

Definition 2.3. If X_i, $1 \leq i \leq n$, are C^2-manifolds, the function $F : X_1 \times \ldots \times X_n \rightarrow R$ is differentiably separable of rank $(r_1, \ldots, r_n)$ at the point $(p_1, \ldots, p_n)$ if there is a coordinate system $\{\phi_{ij}\}$ at the point $(p_1, \ldots, p_n)$ such that F is differentiably separable of rank $(r_1, \ldots, r_n)$ at the point $(p_1, \ldots, p_n)$ in the coordinate system $\phi_{11}, \ldots, \phi_{nd(n)}$.

The Number of Variables On Which F Really Depends

If $F : X_1 \times \ldots \times X_n \rightarrow R$ is differentiably separable of rank $(r(1), \ldots, r(n))$ at a point $(p_1, \ldots, p_n)$, then it is possible to write F as a function of variables $\{y_{11}, \ldots, y_{1r(1)}, \ldots, y_{n1}, \ldots, y_{nr(n)}\}$. This assertion, Lemma 2.2, is a restatement of Theorem A.3. The proof of Theorem A.3 can be found in Appendix A together with an example of the construction.

Lemma 2.2. *Suppose that for $1 \leq i \leq n$, X_i is a $C^{k+1}-$manifold, $k \geq 2$. Assume,*

(i) $F : X_1 \times \ldots \times X_n \to R$ is a $C^{k+1}-$function,

(ii) $(p_1, \ldots, p_n)$ is a point on $X_1 \times \ldots \times X_n$,

(iii) X_i, has coordinates $\underline{x}_i$.

A necessary condition that in a neighborhood of the point $(p_1, \ldots p_n)$ F can be written in the form

$$G(y_{11}, \ldots, y_{1r(1)}, \ldots, y_{n1}, \ldots, y_{nr(n)}),$$

where $(y_{i1}, \ldots, y_{id(i)})$ is a coordinate system on X_i, is that the matrix $BH(G : \underline{x}_i; \underline{x}_{<-i>})$ has rank at most $r(i)$ for each i.

Furthermore, a sufficient condition for F to be written in the form

$$G(y_{11}, \ldots, y_{1r(1)}, \ldots, y_{n1}, \ldots, y_{nr(n)}),$$

for a C^k-function G in a neighborhood of a point $(p_1, \ldots, p_n)$, is that F is differentiably separable of rank exactly $(r(1), \ldots, r(n))$ at $(p_1, \ldots, p_n)$.

Rank Conditions and Construction of an Essential Revelation Mechanism for F.

Lemma 2.2 suggests that in the case of a differentiable function F satisfying the rank conditions stated in the lemma it is possible to construct an essential revelation mechanism whose message space is a topological manifold. We now carry out the construction suggested by the lemma. The main result is given in Theorem 2.1 and in Corollary 2.1.1.

Definition 2.4. Suppose that X_i, $1 \leq i \leq n$ and Z are C^k- manifolds and suppose that $F : X_1 \times \ldots \times X_n \to Z$ is a differentiable function. The triple $(g_1, \ldots, g_n, M_1 \times \ldots \times M_n, h)$ that consists of spaces $M_1 \times \ldots \times M_n$, maps $g_1, \ldots, g_n$, $g_i : X_i \to M_i$, $1 \leq i \leq n$, and function $h : M_1 \times \ldots \times M_n \to Z$ is an *adequate C^k-revelation mechanism that realizes F* if;

(i) each of the spaces M_i is a C^k-manifold,

(ii) each of the functions g_i, $1 \leq i \leq n$, and h is a C^k- differentiable function,

(iii) each g_i, $1 \leq i \leq n$, has a local thread at each point of M_i,

(iv) $h \circ (\prod_i g_i) = F$.

Definition 2.5. Suppose that $F : X_1 \times \ldots \times X_n \to Z$ is a differentiable map from a product of differentiable manifolds $X_1, \ldots, X_n$ to a differentiable manifold Y. The function F *factors through a product of manifolds* $Z_1 \times \ldots \times Z_n$ if there are submersions $g_i : X_i \to Z_i$, and a differentiable mapping $h : Z_1 \times \ldots \times Z_n \to Y$ such that the diagram in Diagram 2.1 commutes.

$$\begin{tikzcd}
X_1 \arrow[d, "g_1"] & \times & \cdots & \times & X_n \arrow[r, "F"] \arrow[d, "g_n"'] & Y \\
Z_1 & \times & \cdots & \times & Z_n \arrow[ur, "h"'] &
\end{tikzcd}$$

Diagram 2.1

It has not been established that the essential revelation mechanism is an adequate C^k-revelation mechanism, because the construction given in Theorem 2.1 ignores all topological and differentiable structure.

The general outline of the method we use to put a structure on the (X_i/F) is straightforward. We first show that when the rank of $BH(F : x_i; x_{<-i>})$ is the same as the dimension of X_i, then for each two points x and x' in X_i, there is an element $y \in X_{<-i>}$ such that $F(x,y) \neq F(x',y)$. Therefore, the set (X_i/F) is X_i. We next appeal to Lemma 2.2. This lemma shows that if the rank of $BH(F : x_i; x_{<-i>})$ at a point is r_i, then in a neighborhood of the point there is a coordinate system $\{x_{i1}, \ldots, x_{id(i)}\}$ and a function G such that the subset that consists of the coordinates $F(x_1, \ldots, x_{nd(n)}) = G((x_{i1}, \ldots, x_{ir}) \int_i x_{<-i>})$. We can use the remaining set of coordinates in X_i to determine a subspace S of X_i by setting $x_{i(r+1)} = 0, \ldots, x_{id(i)} = 0$. The set S is a submanifold of X_i and the restriction of F to the space $S \times X_{<-i>}$ has the property that $BH(restriction(F) : x_{i1}, \ldots, x_{ir}; X_{<-i>})$ has rank the dimension of S. On S, the restriction of F separates points (at least in a neighborhood) and therefore the map from S to (X_i/F) is one-to-one. Some technical fiddling with quotient topologies makes the quotient map, locally, a homeomorphism. Therefore, at least locally, the space (X_i/F) has the same structure as S. The rest of the proof consists of adding enough restrictions to ensure that the local argument can be carried out globally on $X_1 \times \ldots \times X_n$.

Theorem 2.2. *Suppose that X_i, $1 \leq i \leq n$, is a Euclidean space of dimension $d(i) \geq 1$. Suppose that for each $1 \leq i \leq N$, U_i is an open neighborhood of the origin 0_i of X_i and suppose that F is a C^3- function differentiably separable at each point $(p_1, \ldots, p_n) \in U_1 \times \ldots \times U_n$. Then there is an open neighborhood U of p_i such that for each pair of points x and x' in U, $x \neq x'$, there is a point $w \in U_{<-i>}$ such that $F(x, w) \neq F(x', w)$.*

Proof. The matrix $H(F : x; y)[0, 0]$ has rank $d(i)$, by assumption. Set $X = X_i$, set $X_{<-i>} = Y$, set $\dim(X_{<-i>}) = N$, and set $m = d(i)$. We can change coordinates in X and Y separately to coordinates z in X and w in Y so that the new matrix $H(F : z; w)[0, 0]$ has a 1 in the $z_j \times w_j$ position, $1 \leq j \leq m$, and zero in all the other positions. The Taylor series expansion for $F(z_1, \ldots, z_m, w_1, \ldots, w_N)$ then has the form $F(z, w) =$

$$F(0,0) + u \circ z + v' \circ w + w \circ z + z^T Q z + w^T Q' w + P(z^*, w^*)[z, w]$$

where Q and Q' are square matrices, u and v' are vectors in R^m and R^N respectively, $v' \circ w$ denotes inner product, z^T denotes the transpose of the column vector z, and where $P(z^*, w^*)[z, w]$ is a cubic polynomial in the variables $(z_1, \ldots, z_m, w_1, \ldots, w_N)$ with coefficients that are continuous functions on $U \times V$ evaluated at some point $z^* \in U$ and $w^* \in V$. These coefficients of P are bounded on a ball that is a compact neighborhood of $(0, 0) \in U' \times V'$, $U' \subseteq U$ and $V' \subseteq V$. Then for z, $z' \in U'$ and $w \in V'$, $\mid F(z, w) - F(z', w) \mid =$

$$\mid u \circ (z - z') + w \circ (z - z') + z^T Q z' + P(z'^*, w'^*)[z', w] - P(z^*, w^*)[z, w] \mid .$$

The vector $(z - z') \neq 0$ and the w is to be chosen in the set V'. Set $z'^T Q z' - z^T Q z = K$, set $u \circ v = L$, and set $(z - z') = v$. To complete the proof, it will suffice to show that the function

$$w \circ v + P(z^*, w^*)[z', w] + P(z^*, w^*)[z, w] + K + L$$

is not constant on the ball V'. For this it will suffice to show that the function

$$Q = w \circ v + P(z^*, w^*)[z', w] - P(z^*, w^*)[z, w]$$

is not constant on the ball V'. The function $P(z^*, w^*)[z', w] - P(z^*, w^*)[z, w]$ is a homogeneous cubic $\Sigma_{\alpha,\beta} a_{\alpha,\beta} z^\alpha w^\beta$ in the variables $w_1, \ldots, w_N$ with coefficients $\{a_{\alpha,\beta}(z, z', w, w')\}$ that are functions bounded on $U' \times V'$. Set $w = tv$. The powers of the constants $z_1, \ldots, z_m$ can be combined with the coefficients $a_{\alpha,\beta}$ and therefore $Q = t \mid v \mid^2 + a(t)t^3$, where the $a(t)$ is also bounded as a function of t. If $a(t) = 0$ identically in t, then because $v \neq 0$, different values of t produce different values of Q. If $a(t) \neq 0$, and $\mid v \mid^2 + a(t)t^2 = c$ (a constant), then $a(t) = (c - \mid v \mid^2)/t^2$, and therefore $a(t)$ is not bounded as t approaches 0. Therefore Q is not a constant. □.

We now give conditions on a function F that is differentiably separable of rank $(r_1, \ldots, r_n)$, so that each of the sets (X_i/F), with the quotient topology, has the structure of a C^0–manifold of dimension r_i. Under these conditions the set theoretic essential revelation mechanism is a topological essential revelation mechanism.

Definition 2.6. If X_i, $1 \leq i \leq n$, are topological spaces, then a real valued function $F : X_1 \times \ldots \times X_n \rightarrow R$ *induces strong equivalence* on X_i, if the following condition is satisfied for each $x, x' \in X_i$, such that $x \neq x'$; there is an open neighborhood U of a point $q \in X_{<-i>}$, such that $F(x \,/_i\, u) = F(x' \,/_i\, u)$ for each $u \in U$, then $F(x \,/_i\, z) = F(x' \,/_i\, z)$ for all $z \in X_{<-i>}$.

It is relatively easy to find classes of functions that induce strong equivalence. Suppose the X_i are Euclidean spaces with coordinates x_{ij}, $1 \leq i \leq n$, $\quad 1 \leq j \leq d(i)$. If for each $1 \leq i \leq n$, $\beta(i) = (\beta(i1), \ldots, \beta(id(i)))$ is a sequence of nonnegative integers, denote by $x_i^{\beta(i)}$ the monomial $x_{i1}^{\beta(i1)} \ldots x_{id(i)}^{\beta(id(i))}$, and denote by $x_1^{\beta(1)} \ldots x_n^{\beta(n)}$ the product of the monomials $x_i^{\beta(i)}$. Write

$$F(x_1, \ldots, x_n) = \Sigma_{\beta(1),\ldots,\beta(n)} A_{\beta(1)\ldots\beta(n)} x_2^{\beta(2)} \ldots x_n^{\beta(n)},$$

where $A_\beta(x_1)$ are polynomials in x_1. Then for x_1, $x_1' \in X_1$, $F(x_1, x_{<-1>}) = F(x_1', x_{<-1>})$ for $x_{<-1>}$ in an open set in $X_{<-1>}$, if and only if $[A_\beta(x_1) - A_\beta(x_1')]x_2^{\beta(2)} \ldots x_n^{\beta(n)} = 0$ for the $x_2, \ldots, x_n$ chosen arbitrarily in an open set in $X_2 \times \ldots \times X_n$. However, a polynomial vanishes in an open set if and only if each of its coefficients is zero. Therefore if $F(x_1, x_{<-1>}) = F(x_1, x_{<-1>})$ for the $x_{<-1>}$ chosen in some open set, it follows that for each β, $A_\beta(x_1) - A_\beta(x_1') = 0$. That is, F induces a strong equivalence relation on X_1.□

Theorem 2.3. *Suppose that X_i, $1 \leq i \leq n$ are C^4-manifolds of dimensions $d(1), \ldots, d(n)$, respectively. Suppose $F : X_1 \times \ldots \times X_n \to R$ is a C^4-function that is differentiably separable on $X_1 \times \ldots \times X_n$ of rank $(r(1), ..., r(n))$ where each $r_i \geq 1$. Assume that F induces strong equivalence in X_i for each i. If*

(i) the spaces (X_i/F) are all Hausdorff,

(ii) quotient map $q_i : X_i \to (X_i/F)$ is open for each $1 \leq i \leq n$.

Then, for each $1 \leq i \leq n$, the space (X_i/F) (with quotient topology) is a topological manifold (i.e. a C^0-manifold). Furthermore, the quotient map $q_i : X_i \to (X_i/F)$ has a local thread in the neighborhood of each point.

Proof. Suppose that $p_i^* \in (X_i/F)$, $\;1 \leq i \leq n$. Choose a point $p_i \in X_i$, $\;1 \leq i \leq n$, such that $q_i(p_i) = p_i^*$. Because the function F is differentiably separable of rank $(r(1), ..., r(n))$ at the point $(p_1, \ldots, p_n)$, it follows from Lemma A.3 that for $1 \leq i \leq n$, there is an open neighborhood $U_{<-i>}$ of $p_{<-i>}$ in $X_{<-i>}$, an open neighborhood U_i of the point p_i, and a coordinate system $x_i = \{x_{i1}, \ldots, x_{id(i)})$ in X_i such that $x_i(p_i) = (0, \ldots, 0)$ and a C^3-function G defined in a neighborhood of the origin, such that

$$F(x_1, \ldots, x_n) = G((x_{i1}, \ldots, x_{ir(i)}) \underset{i}{\int} z)$$

for each $z \in U_{<-i>}$. Denote by S_i^* the set of elements $\{x_{i1}, \ldots, x_{ir(i)}, 0, \ldots, 0)\}$ that lie in U_i. Choose in S_i^* a compact neighborhood S_i of (0,...,0) (in the induced topology on S_i^*). The map q_i carries the set U_i to an open set of (X_i/F) because we have assumed that q_i is an open map. We have assumed that the equivalence relation induced on $X_{<-i>}$ by F is strong, therefore the equality

$$F(x_{i1}, \ldots, x_{ir(i)}, b_1, \ldots, b_{d(i)-r(i)} \underset{i}{\int} z_{<-i>}) =$$

$$F((x_{i1}, \ldots, x_{ir(i)}, 0, \ldots, 0) \underset{i}{\int} z_{<-i>})$$

implies that $q_i(x_{i1}, \ldots, x_{id(i)}) = q_i(x_{i1}, \ldots, x_{ir(i)})$ for each $(x_{i1}, \ldots, x_{id(i)})$ in U_i. Therefore, $q_i(U_i) = q_i(S^* *_i)$. The set S_i^* was constructed so that q_i is one-to-one on S_i^*. By assumption, the space (X_i/F) is Hausdorff, therefore the restriction of q_i to S_i is a homeomorphism from S_i to a neighborhood N_i of p_i^*. Denote by s_i the inverse of q_i on N_i. It follows that the point $p_i^* \in X_i$ has a neighborhood N_i that is homeomorphic to a neighborhood of the origin of the space $R^{r(i)}$. Furthermore, the function s_i is a thread of q_i on the set N_i.□

The following corollary states that the essential revelation mechanism is a C^0-essential revelation mechanism. In this case, under the assumptions made about F, each C^0-adequate revelation mechanism factors through the C^0-essential revelation mechanism.

Corollary 2.3.1. *Suppose that X_i, $1 \leq i \leq n$ are C^4-manifolds and that X_i has dimension $d(i)$. Assume that $F : X_1 \times \ldots \times X_n \rightarrow R$ is a real valued function on F that satisfies the following conditions:*

(i)there are integers $(r(1), ..., r(n))$, $1 \leq r(i) \leq d(i)$, such that at each point $(p_1, \ldots, p_n) \in X_1 \times \ldots \times X_n$, F is differentiably separable of rank $(r(1), ..., r(n))$,

(ii) for each i, the map $q_i : X_i \rightarrow (X_i/F)$ is open and (X_i/F) is Hausdorff,

(iii) for each i, F induces a strong equivalence relation on X_i.

Then the triple

$$(q_1 \times \ldots \times q_n, (X_1/F) \times \ldots \times (X_n/F), F^*)$$

where;

(1)each (X_i/F) is given the quotient topology,

(2) the maps $q_i : X_i \rightarrow (X_i/F)$ is the quotient map,

(3) $F^* : (X_1/F) \times \ldots \times (X_n/F) \rightarrow R$ is such that

$$F^*(q_1(x_1), \ldots, q_n(x_n)) = F(x_1, \ldots, x_n)$$

for each $(x_1, \ldots, x_n) \in X_1 \times \ldots \times X_n$, is an adequate C^0-revelation mechanism that realizes F. The space (X_i/F) has dimension $r(i)$. Furthermore, if a triple

$$(g_1 \times \ldots \times g_n, Z_1 \times \ldots \times Z_n, G)$$

is such that $g_i : X_i \rightarrow Z_i$, $G : Z_1 \times \ldots \times Z_n \rightarrow R$, and the triple is an adequate revelation mechanism that realizes F, then there are continuous maps $g_i^* : Z_i \rightarrow (X_i/F)$ such that the diagram in Diagram 1.3 commutes, with $Y = R$.

Proof. We have already shown in Theorem 2.3 that the triple $(q_1 \times \ldots \times q_n, (X_1/F) \times \ldots \times (X_n/F), F^*)$, is an adequate revelation mechanism that realizes F. Suppose that $z_i^* \in Z_i$. Denote $(g_1(w), \ldots, g_{i-1}(w), g_{i+1}(w), \ldots, g_n(w))$ by $g_{<-i>}(w)$, for each $w \in X_{<-i>}$. Choose an element $x_i^* \in X_i$ such that $g_i(x_i^*) = z_i^*$. Suppose that x_i', $x_i^* \in X_i$, such that $g_i(x_i^*) = g_i(x_i') = z_i^*$. Then for each

$$w \in X_{<-i>}, \quad F(x_i^* \underset{i}{\int} w) = G(g_i(x_i^*) \underset{i}{\int} g_{<-i>}(w)) =$$
$$G(g_i(x_i') \underset{i}{\int} g_{<-i>}(w)) = F(x_i' \underset{i}{\int} w).$$

Therefore $q_i(x_i^*) = q_i(x_i')$. Set $g_i^*(z_i^*) = q_i(x_i^*)$. Because the map $g_i : X_i \rightarrow Z_i$ has a thread in the neighborhood of each point, there is a neighborhood N of the point z_i^* and a thread $s_i : N \rightarrow X_i$ such that $g_i(s_i(z^*)) = g_i(z^*)$ for each z^*N. Then $g_i^*(z^*) = q_i(s_i(z^*))$. Because both q_i and s_i are continuous, it follows that the map g_i^* is continuous. □.

The Results of Abelson, Chen and Hurwicz

In [5](p.291), Hurwicz considered realizing a function F from a product $R^2 \times R^2$ to R. Assume that the first factor of the product $R^2 \times R^2$ has coordinates a_1, a_2 and that the second factor has coordinates b_1, b_2. Hurwicz showed that if a realization of the function F exists that uses a message M space of dimension 2 with coordinates m^1,and m^2, and if the realization uses messages correspondences $\mu^1(a_1, a_2) = \{(m^1, m^2) | g^1(m^1, m^2; a_1 a_2) = 0\}$ and $\mu^2(b_1, b_2) = \{(m^1, m^2) | g^2(m^1, m^2; b_1 b_2) = 0\}$ for agent $i = 1, 2$ and if Jacobian $(\partial g^i / \partial m^j)_{i,j=1,/,2}$ is nonsingular, then the determinant,

$$\begin{vmatrix} 0 & F_{b_1} & F_{b_2} \\ F_{a_1} & F_{a_1 b_1} & F_{a_1 b_2} \\ F_{a_2} & F_{a_2 b_1} & F_{a_2 b_2} \end{vmatrix} = 0; \quad (\text{Eq.}*).$$

for all (a, b). That is, the Full Bordered Hessian FBH(F) must have rank at most 2. He further showed,([5], p. 293),

Theorem(Hurwicz). *Let $F : \Theta^1 \times \Theta^2 \rightarrow \mathcal{R}$ have nonvanishing first partials derivatives and let it satisfy equation Eq.$*$ on Θ. Then there exist smooth functions $G^1$and G^2 such that F is realized by (g^1, g^2, M, h) with*

$$\begin{aligned} g^1(m, a) &\equiv m^2 - G^1(m^1, a), \quad a \in \Theta^1, \\ g^2(m, b) &\equiv m^2 - G^2(m^1, b), \quad b \in \Theta^2, \ ' \end{aligned}$$

and

$$M \equiv \mathcal{R}^2, \quad m = (m^1, m^2), m^i \in \mathcal{R}, \quad i = 1, 2.$$

In [3](p. 259), Chen generalized the Hurwicz result on necessary conditions to the case of a goal function $P : R^{k_1} \times R^{k_2} \rightarrow R$. (Chen uses the notation $BH(P)$ for the Full Bordered Hessian of P.) Chen's theorem states:

Theorem(Chen). *Let $P : R^{k_1} \times R^{k_2} \to R$ be a C^2 function. If P can be realized in an open set $U \subseteq R^{k_1} \times R^{k_2}$ by an efficient privacy-preserving mechanism with a message space of dimension n, then* $\operatorname{rank} FBH(P) \leq n$ *in U.*

This condition on the Full Bordered Hessian can be restated as the condition that all $(n+1)\times(n+1)$ submatrices of $FBH(P)$ have determinant zero. Further, Chen uses the differential ideal constructions of [7], to generalize the Hurwicz necessary condition to find necessary conditions for a goal function $F : R^{k_1} \times \ldots \times R^{k_l} \to R^m$, to be realized by a privacy preserving mechanism with a message space of dimension n.

While the Bordered Hessian used by Hurwicz and Chen is also used in our constructions, the conditions placed on the Bordered Hessian vary with the purpose. The differences, and similarities between the conditions used by Hurwicz and Chen and the conditions we use are best indicated via an example. The example we consider is one due to Hurwicz and can be found in [5].

Consider two agents each with parameter space R^2, where the first agent has coordinates x and z in her space and the second agent has coordinates x' and z' in his space. We assume they are to realize the goal function $f(x, z, x', z') = (z - z')/(x - x')$. The Hurwicz result, and Chen's generalization states that the function f can be realized by a mechanism using a message space of dimension 2 only if the determinant of the Full Bordered Hessian of f is zero. Further, Hurwicz shows that if f has nonvanishing first partials, there is a mechanism that realizes f if the Full Bordered Hessian has determinant zero. Indeed, if a message space of dimension 2 has coordinates f and p, if the first agent signals sufficient information to indicate the line with equation $p + xf = z$ and if the second agent indicates the line with equation $p + x'f = z'$, then these two lines intersect in a point with coordinates $((z - z')/(x - x'), (xz' - x'z)/(x - x'))$. The required realization is thus achieved. Furthermore, the Full Bordered Hessian of f is

$$\begin{pmatrix} 0 & (z-z')/(x-x')^2 & -1/(x-x') \\ -(z-z')/(x-x')^2 & -2(z-z')/(x-x')^3 & 1/(x-x')^2 \\ 1/(x-x') & 1/(x-x')^2 & 0 \end{pmatrix}.$$

We, however, are interested in the number of parameters required to compute the intersection of the two lines with equations $p + xf = z$ and $p +$

$x'f = z'$, and we wish to make no assumption that the agents are constrained to use the coordinates x, z, x', z'. We also assume that when one computes the intersection then one also computes the function f, perhaps with the use of an outcome function. Thus we apply our conditions directly to the function f. Because we are interested in what each agent must reveal in order to compute f, we must examine each agent separately. In the case of agent 1, we first find the rank of the matrix $BH(f : x, z; x', z')$. This matrix has two rows, and it is easy to see that the rank is 2. Further the Hessian

$$\begin{pmatrix} -2(z-z')/(x-x')^3 & 1/(x-x')^2 \\ 1/(x-x')^2 & 0 \end{pmatrix}$$

has rank 2. It then follows that two parameters are required for the computation of the intersection and further in the neighborhood of each point of Agent 1's parameter space there is a coordinate system consisting of two parameters that can be used to compute f. In this case, of course, one can use the parameters x and z. We then examine Agent 2. A similar pair of computations shows that two parameters are required from agent 2, and two such parameters are available. Thus for us, four parameters in all are required for the computation.

Next consider an example given by Abelson [1] in connection with communication complexity. Let

$$\Phi(X, Y) = \Sigma_{k=1}^{n}(y_k x_1^k + x_k y_1^k)$$

where $X = (x_1, \ldots, x_n)$, $Y = (y_1, \ldots, y_n)$. Here it is assumed that processor P_1 knows X and processor P_2 knows Y. The Full Bordered Hessian for this example is

$$\begin{pmatrix} 2 & 2x_1 & \ldots & kx_1^{k-1} & y_1 + \Sigma_{i=1}^{k} i\, y_i x_1^{i-1} \\ 2y_1 & 0 & \ldots & 0 & y_1^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ ky_1^{k-1} & 0 & \ldots & 0 & y_1^k \\ x_1 + \Sigma_{i=1}^{k} i\, x_i y_1^{i-1} & x_1^2 & \ldots & x_1^k & 0 \end{pmatrix}.$$

As shown by Chen in [3], the submatrix that consists of the first two and the last two rows is a matrix of rank 4. Chen's Theorem gives 4 as a bound on the dimension of message spaces that realize Φ. Chen also offers a mechanism that realizes Φ with a four dimensional message space. If the message space has coordinates $m_1, \ldots, m_4$, then the messages $m_1 = x_1$, $m_2 = y_1$,, $m_3 = \Sigma_{i=1}^k x_i m_2^i$, and $m_4 = \Sigma_{i=1}^k y_i m_1^i$, together with the outcome function $h(m_1, \ldots, m_4) = m_3 + m_4$ realizes Φ.

Abelson used the Hessian $H(F)$, the matrix that has rows indexed by the variables of the first processor and columns indexed by the variables of the second processor, to give a lower bound on the amount of information transfer required in a multistage distributed computation. His theorem states:

Theorem 2 (Abelson [1]). *Let $\Phi : X \times Y \to \mathcal{R}$ be a C^2-function, let $p \in X \times Y$, and let R be the rank of the matrix of second-order partials derivatives $\Delta_{ij} = \partial^2 \phi / \partial x_i \partial y_j$ at p [the Hessian $H(\Phi)$ at p]. Then any multistage distributed computation which computes Φ in a neighborhood of p must have total information transfer ar least R between P_1 and P_2 not the notation we have introduced (assuming that the functions computed at each stage are all C^2.)*

In the case of the function Φ, the Hessian used by Abelson has rank 2, thus a distributed computation of Φ must interchange at least two parameters. This can be done, for instance, by having processor P_1 send the value of x_1 to P_2 and P_2 send the value of y_1 to P_1. Then, knowing the value of x_1, P_2 can compute the first term of Φ, and send it to P_1, who has computed the second term of Φ, knowing y_1, and then can calculate the sum. The total number of variables transmitted, including the value of Φ is 4. But notice that it is not possible to eliminate any of the 2N variables X,Y and compute Φ. In this example, the matrices BH and H do not have the same rank, for $N \geq 3$. Here the quotient object exists as a differentiable manifold of dimension N, but this fact is derived directly from the equivalence relation "$\approx$" and not from the ranks of BH and H.

The Jordan and Sonnenschein Theorems on the Universality of the Competitive Mechanism

Sonnenschein studied sub-correspondences of the core net trade correspondence(a CCTC) that associates with each pure exchange economy $\mathcal{E}$ a set of net trades which result in core allocations for $\mathcal{E}$. A private representation of a CCTC, g consists of a triple (A, μ, f), where A is a message space, μ is a correspondence from the set of $\mathcal{E}$ to A, and f is a function from A to the set of trades. A consumer is a pair (U, ω), where U is a continuous real valued function with domain Ω and $\omega \in \operatorname{int}\Omega_n$. $\mathcal{C}$ denotes the set of all consumers, and $\mathcal{F}$ is the set of all functions with domain an initial segment of the positive integers and range $\mathcal{C}$. The principal result of [28] is given under the conditions placed by the following axiom:

Axiom S. *A CCTC g with private representation (A, μ, f) is said to satisfy Axiom S if for all $\mathcal{E}^1 = [(U^1, \omega^1), \ldots, (U^m, \omega^m)] \in \mathcal{F}$ and all $a \in A$, there exists $\mathcal{E}^2 = [(U^1, \omega^1), \ldots, (U^m, \omega^m), (U^{m+1}, \omega^{m+1}), \ldots, (U^{m+r}, \omega^{m+r})] \in \mathcal{F}$, such that $a \in \mu(\mathcal{E}^2)$.*

The result of Sonnenschein is then:

Theorem. *If (A, μ, f) is a private representation of the CCTC g, and if (A, μ, f) satisfies Axiom S, then there exists a unique function $\phi : A \to P$, such that the following triangle commutes:*

$$\begin{tikzcd}
R_n & & \mathcal{C} \times \mathcal{P} \arrow[ll, "e"'] \\
& & \mathcal{C} \times \mathcal{A} \arrow[ull, "f"'] \arrow[u, "1_{\mathcal{C}} \times \phi"']
\end{tikzcd}$$

In [8], Jordan approached the problem of characterizing price mechanisms by studying privacy preserving mechanisms defined on a space of economies E^*. For an economy with L commodities, $R^L_{++} = \{x \in R^L :$

$x_j > 0$ for each j$\}$, and $R^L_+ = \{x \in R^L : x_j \geq 0$for each j$\}$. For each function $u^i : R^L :_+ \rightarrow R \cup \infty$, set

$$C^i = \begin{cases} R^L_{++} \text{ if the closure in} R^L_+ \text{of the set} \\ \{x : u^i(x) \geq u^i(\omega^i)\} \text{ is contained in} \\ R^L_{++} \text{for each } \omega^i \in R^L_{++}, \\ \\ R^L_+ \text{ otherwise.} \end{cases}$$

For each i, U^{*i} denotes the set of utility functions that are continuous and real valued on C^i, strictly monotone on C^i, and that are either strictly quasi-concave on C^i, or concave on C^i. $E^* = \prod_i(R^L_{++} \times U^{*i})$. Jordan introduces the concept of a *noncoercive* allocation mechanism. A mechanism (μ, M, g) is noncoercive if for each $e = (\omega^i, u^i)_i$, and each $y \in g[\mu(e)]$, $u^i(\omega^i + y^i) \geq u^i(\omega^i)$ for each i. Jordan sets $M_c = \{(p, y) \in \Delta \times Y; py^i = 0$ for each i.$\}$ and he denotes by μ_c the message correspondence for the competitive allocation mechanism. Jordan then proves:

The Uniqueness Theorem. *Suppose that (μ, M, g) is an allocation mechanism on E^* which is*

(i) nonwasteful;

(ii) noncoercive ;

(iii) informationally decentralized (privacy preserving);

and if

(iv) M is a connected K(L-1) dimensional manifold;

(v) the restriction of μ to E, the set of Cobb-Douglas Environments, is a continuous function;

(vi) $\mu(E)$ is closed in M.

Then there is a homeomorphism $h : M \rightarrow M_c$ such that

(a) $h[\mu^i(\omega^i, u^i)] = \mu^i_c(\omega^i, u^i)$ for each i and each $(\omega^i, u^i) \in R^L_{++} \times U^{*i}$;

(b) $h[\mu(e)] = \mu_c(e)$ for each $e \in E^*$;

and

(c) $g_c \circ h = g$.

A diagram that represents Jordan's result is Diagram 4.1.

$$\begin{tikzcd}
E^* \arrow[r, "\mu_c"] \arrow[d, "\mu"] & M_c \arrow[d, "g_c"] \\
M \arrow[ur, "h"] \arrow[r, "g"'] & Y
\end{tikzcd}$$

Diagram 4.1.

The results of Sonnenschein and Jordan each can be interpreted as characterizing the price mechanism as a universal object in a class of realizations. Sonnenschein and Jordan each exhibit the existence of a map from each allocation mechanism that is privacy preserving to the price mechanism. To prove universality of the price mechanism one need only establish that the map constructed can be used to reconstruct the given allocation mechanism.

Appendix A.

Leontief and Abelson Theorem

Suppose that $F(x_1, \ldots, x_N)$ is a function of N variables which has continuous partial derivatives to order d. For each sequence $\alpha = (\alpha(1), \ldots, \alpha(N))$ of nonnegative integers, denote by $\mid \alpha \mid$ the sum $\alpha(1) + \ldots + \alpha(N)$. We denote by $D(x_1^{\alpha(1)} \ldots x_N^{\alpha(N)}; F)$ the derivative $\partial^{|\alpha|} F / \partial x_1^{\alpha(1)} \ldots x_N^{\alpha(N)}$. Set $\partial^0 F / \partial x_j^0 = F$. *Notation.* If F is a function of one variable and G is a real valued function of a vector x, then $(F \circ G)(x)$ denotes the composition $F(G(x)$.

The following statement is a classical result sometimes referred to as the "General Theorem on Functional Dependence" c.f.[29].

Theorem A.1. *Suppose that $\underline{x} = (x_1, \ldots, x_m)$ and $\underline{y} = (y_1, \ldots, y_n)$ are sets of real variables and suppose $F(\underline{x}, \underline{y})$ and $G(\underline{x})$ are real valued C^1-functions defined on a neighborhood U of the point $(p, q) = (p_1, \ldots, p_m, q_1, \ldots q_n)$ that satisfy the following conditions.*

(i)

$$\begin{pmatrix} D(x_1; F) & \ldots & D(x_m; F) \\ D(x_1; G) & \ldots & D(x_m; G) \end{pmatrix}$$

is a matrix of rank at most one,

(ii) at p, $D(x_1; G) \neq 0$.

Then there is a function $C(w, y)$, w a real variable, such that $F(x, y) = C(G, y)$ in some neighborhood of (p, q).

Proof. Because of assumption (ii), the equation $w - G(x_1, \ldots, x_m) = 0$ has a unique solution in a neighborhood U' of (p,q). Thus, there is a function $c(w, x_2, \ldots, x_m)$ such that $w = G(c(w, x_2, \ldots, x_m), x_2, \ldots, x_m)$ and such that $c(G(x_1, \ldots, x_m), x_2, \ldots, x_m) = x_1$. Set

$$C(w, x_2, \ldots, x_m, y) = F(c(w, x_2, \ldots, x_m), x_2, \ldots, x_m, y.$$

Then

$$D(x_j; C) = D(x; F) D(x_j; c) + D(x_j; F)$$

for $j > 1$. Because

$$w = G(c(w, x_2, \ldots, x_m), x_2, \ldots, x_m),$$

it follows that $0 = D(x_1; G)D(x_j; c) + D(x_j; G)$ for $j > 1$. Further, by condition (i), there is an Ω so that $D(x_j; F) = \Omega D(x_j; G)$ for $1 \leq j \leq m$. Therefore $D(x_j; C) = \Omega[D(x_1; G)D(x_j; c) + D(x_j; G)] = 0$. Hence the function C is independent of the variables $x_2, \ldots x_m$ and we can write $C(w, x_2, \ldots, x_m, y) = C(w, y)$. Then

$$C(G(x_1, \ldots, x_m), y) =$$
$$F(c(G(x_1, \ldots, x_m), x_2, \ldots, x_m), x_2, \ldots, x_m, y) = F(x_1, \ldots, x_m, y).\Box$$

Leontief's Theorem

Leontief proved the following result in [11].

Theorem A.2. *Suppose F is a function of variables $x_1, \ldots, x_m, \ldots, y_1, \ldots, y_n$. Set $F_i = D(x_i; F)$, $\quad 1 \leq i \leq m$. Assume that $(p, q) = (p_1, \ldots, p_m, q_1, \ldots, q_n)$ is a set of values for the variables $(x_1, \ldots, y_1, \ldots, y_n)$. A necessary and sufficient condition that there exist functions $C(w, y_1, \ldots, y_n)$ and $G(x_1, \ldots, x_m)$ such that $F(x, y) = C(G(x), y)$ in a neighborhood U of the point (p, q) is that;*

(i) for each $1 \leq i, \quad j \leq m$ and each $1 \leq k \leq n$, $(\partial/\partial y_k)[F_i/F_j] = 0$,

(ii) for some j, $F_j(x_1, \ldots, x_m)(p, q) \neq 0$.

Proof. Form the matrix

$$M = \begin{pmatrix} F_1 & \ldots & F_m \\ F_1^* & \ldots & F_m^* \end{pmatrix}$$

where $F_j^* = D(x_j; F(x; q))$. For the point q, $D(x_j; F)(y) = D(x_j; F(x; q))$. Condition (i) implies that the derivative $D(y_k; F_i/F_j) = 0$. Thus the ratio F_i/F_j is independent of y. Also at (p;q), $F_i^*/F_j^* = F_i(x, q)/F_j(x, q)$. It follows that $F_i^*/F_j^* = F_i/F_j$ for all (x,y). Therefore the matrix M has rank at most one. Further, by assumption, $F_j(p, q) \neq 0$ for some j. The previous theorem shows that we can write $F(x, y) = C(G(x), y).\Box$

Corollary A.2.1. *A necessary and sufficient condition that there exist functions C(w,y) and G(x) such that F(x,y) = C(G(x),y) in a neighborhood of (p,q) is that the matrix BH(F:x;y) have rank at most one in a neighbor hood of (p, q) and $D(x_j; F)(p, q) \neq 0$, for some j.*

Proof. The necessity of the given rank condition has already been demonstrated. Set $F_j = D(x_j; F)$. Theorem A.2 shows that to prove the sufficiency of the rank condition on BH(F:x y), we need only prove that $D(y_k; F_i/F_j) = 0$ for each i,j, and k. But $D(y_k; F_i/F_j) = [D(y_k; F_i)F_j - D(y_k; F_j)F_i]/F_j^2$. By assumption, $\Omega(F_1, \ldots, F_m)^t = (D(x_1 y_k; F), \ldots, D(x_m y_k; F))^t$ (M^t denotes the transpose of M). Thus $\Omega D(x_i; F) = D(x_i y_k; F) = D(y_k; F_i)$ for each i and k. Therefore $D(y_k; F_i/F_j) = 0$ for all k. □

Corollary A.2.2. *Suppose $F(x; y)$ is a C^2-function of variables*

$$\underline{x} = (x_1, \ldots, x_m) \text{ and } \underline{y} = (y_1, \ldots, y_n).$$

A necessary condition that there are functions $C(u, v)$, $A(\underline{x})$, and $B(\underline{y})$ such that $F(\underline{x}; \underline{y}) = C(A(\underline{x}), B(\underline{y}))$ is that the matrices $BH(F : \underline{x}; \underline{y})$ and $BH(F : \underline{y}; \underline{x})$ each have rank at most one. Further,if for some $1 \leq j \leq m$ and some $1 \leq k \leq n$, $D(x_j; F)(p, q) \neq 0$, and $D(y_k; F)(p, q) \neq 0$, then the rank condition is also sufficient for the existence of C, A and B such that $F = C(A, B)$.

Proof. Because $BH(F : \underline{x}; \underline{y})$ has rank at most one and $D(x_j; F) \neq 0$ for some j, it follows from Theorem A.2 that $F(x; y) = C(A(x), y)$ for some A and C. To complete the proof, it will suffice to prove that $C(w, y)$ satisfies the conditions of Corollary A.2.2 using y_j's as the $x_j's$ and w as x_1. For convenience of notation, assume that $D(x_1; F)(p, q) \neq 0$. Then

$$C(w, y) = F(h(w, x_2, \ldots, x_m), x_2, \ldots, x_m; y_1, \ldots y_n).$$

Therefore

$$D(y_j; C) = D(y_j; F(h(w, x_2, \ldots, x_m), x_2, \ldots, x_m); y))$$

and $D(wy_j; C) = D(x_1 y_j; F)D(w; h)$. By hypothesis there is a Θ such that $D(x_1 y_j; F) = \Theta D(y_j; F)$ for each j. Therefore

$$D(wy_j; C) = \Theta D(y_j; F)D(w; h) = \Theta D(y_j; C)D(w; h).$$

Therefore, by Theorem A.2, C(w,y) = G(w,B(y)) if for some y_j, and for

$$w_0 = F(p; q), \quad D(y_j; C(w, y))(p; q) \neq 0.$$

However, from the proof of Theorem A.2,

$$C(w, y) = F(h(w, x_2, \ldots, x_m), x_2, \ldots, x_m; y)$$

where $h(F(x_1,\dots,x_m;q),x_2,\dots,x_m)=x_1$. If $w_0=F(p;q)$, because $C(w,y)$ is independent of the variables $x_2,\dots,x_m$, it follows that

$$C(w_0,y)=F(h(F(p;q),p_2,\dots,p_m;y)=F(p;y).$$

Therefore $D(y_j;C)=D(y_j;F(p;y))\neq 0$ for some j.□

Corollary A.2.3. *Suppose that x_{ij}, $1\leq i\leq r$, $1\leq j\leq d(i)$ are r ordered sets of variables. Denote by x_i the set of variables $(x_{i1},\dots,x_{id(i)})$. Assume*

$$p=(p_1,\dots,p_p)=(p_{1\,1},\dots,p_{r\,d(r)})$$

is a point. Necessary conditions that in some neighborhood of the point p there are functions G, A_j, $1\leq j\leq r$ such that

$$F(x_{1\,1},\dots,x_{r\,d(r)})=G(A_1(x_1),\dots,A_r(x_r))$$

is that each matrix $BH(F:x_j;x_1,\dots,x_{j-1},x_{j+1},\dots,x_r)$ has rank at most one. The condition is also sufficient if for each j, there exists a k(j) such that the derivative

$$D(x_{j\,k(j)};F(p_1,\dots,p_{j-1},x_j,p_{j+1},\dots,p_r))\neq 0.$$

Our results on adequate revelation mechanisms require a slightly altered version of Leontief's Theorem. This version is closely related to a result announced by Abelson(c.f.[1]). We begin with a lemma.

Lemma A.1. *Suppose that X and Y are Euclidean spaces of dimensions m and n, respectively. Assume that X has coordinates $(x_1,\dots,x_m)$ and Y has coordinates $(y_1,\dots,y_n)$. Assume that $F_1,\dots,F_N$ are functions from $X\times Y$ to R that are defined on a neighborhood $U\times V$ of a point (a,b), $a\in X$ and $b\in Y$. A necessary condition that there are functions*

$$A_1(x_1,\dots,x_m),\dots,A_r(x_1,\dots,x_m),$$

functions

$$G_i(W_1,\dots,W_r,y_1,\dots,y_n),\ 1\leq i\leq N,$$

such that

$$F_i(x_1, \ldots, x_m, y_1, \ldots, y_n) = G_i(A_1, \ldots, A_r, y_1, \ldots, y_n),\ 1 \le i \le N,$$

for each $(x_1, \ldots, x_m) \in U$ *and* $(y_1, \ldots, y_n) \in V$ *is that the matrix*

$$BH(F_1, \ldots, F_N : x_1, \ldots, x_m; y_1, \ldots, y_n)$$

has rank less than or equal to r at each point of $U \times V$.

Proof. Because

$$F_i(x_1, \ldots, x_m, y_1, \ldots, y_n) = G_i(A_1, \ldots, A_r, y_1, \ldots, y_n),$$

it follows that

$$D(x_j; F_i) = \Sigma_{s=1}^{r} D(A_s; G_i) D(x_j; A_s)$$

and $D(x_j y_k; F_i) = D(y_k A_s; G_i) D(x_j; A_s)$. Each of the columns is a linear combination of the r columns $(D(x_1; A_i), \ldots, D(x_m; A_i))^t$, $1 \le i \le r$. Therefore the matrix BH[x,y] has rank at most r. □

The next theorem shows that for a product of Euclidean spaces, if F is a differentiably separable function of ranks $(r_1, \ldots, r_n)$, then the rank r_i give the number of variables required from the space X_i in order to compute the function. The theorem is stated for the more general situation of a sequence of functions $F_1, \ldots, F_N$ because the proof of the more general assertion is complicated only by the notation and the conclusion is applicable to the case of the vector function that computes a Walrasian equilibrium when there are more than two commodities.

Theorem A.3. *Suppose that* X *and* Y *are Euclidean spaces of dimensions* m *and* n*, respectively. Suppose that* X *has coordinates* $x_1, \ldots, x_m$ *and that* Y *has coordinates* $y_1, \ldots, y_n$*. Assume that* $p \in X$, $q \in Y$*, that* U *is a neighborhood of* p*,* V *is a neighborhood of* q*, and that* F_i, $1 \le i \le N$*, is a* $C^{k+1}-$*function,* $k \ge 2$*, from* $U \times V$ *to* R*. Then,*

(i) a necessary condition that there is a neighborhood $W \times V$ *of a point* $(p', q) \in R^r \times V$*,* C^k*-functions,* $k \ge 2$*,*

$$G_1(W_1, \ldots, W_r, y_1, \ldots, y_n), \ldots, G_N(W_1, \ldots, W_r, y_1, \ldots, y_n)$$

defined on $W \times V$, and C^k-functions $A_1(x_1, \ldots, x_m), \ldots, A_r(x_1, \ldots, x_m)$ defined on $U \times V$ such that

$$F_i(x_1, \ldots, x_m, y_1, \ldots, y_n) =$$

$$G_i(A_1(x_1, \ldots, x_m), \ldots, A_r(x_1, \ldots, x_m), y_1, \ldots, y_n),$$

for $1 \leq i \leq N$, is that the matrix $BH(F_1, \ldots, F_n : x_1, \ldots, x_p; y_1, \ldots, y_q)$ has rank less that or equal to r at each point of $U \times V$.

(ii) If $BH(F_1, \ldots, F_N : x_1, \ldots, x_m; y_1, \ldots, y_n)$ has rank at most r in the neighborhood $U \times V$, and if $H^*(F_1, \ldots, F_N : x_1, \ldots, x_m; y_1, \ldots, y_n)[x, q]$ has rank r at each point of U, then there is a point (p', q) in $R^r \times Y$, a neighborhood $W \times V$ of (p', q), a neighborhood $U' \times V'$ of (p,q), C^k-functions $G_1, \ldots, G_N$, defined on $W \times V'$, and C^k-functions $A_1(x_1, \ldots, x_m), \ldots, A_r(x_1, \ldots, x_n)$ defined on a neighborhood of p, such that on $U' \times V'$,

$$Fi_(x_1, \ldots, x_m, y_1, \ldots, y_n) =$$

$$G_i(A_1(x_1, \ldots, x_m), \ldots, A_r(x_1, \ldots, x_m), y_1, \ldots, y_n),$$

$1 \leq i \leq N$, for each $(x_1, \ldots, x_m) \in U'$ and $(y_1, \ldots, y_q) \in V'$.

The proof shows how to construct the functions A_i and G_j.

An Example of The Coordinate Construction

As an example, we carry out the constructions for the function

$$F(x_1, x_2, x_3; y_1, y_2, y_3, y_4) =$$

$$x_1(y_1 + y_3 + y_1y_4) + x_2(y_2 + y_3 - y_1y_4) + x_2^2(y_1 + y_3 + y_1y_4) + x_3^2(y_2 + y_3 - y_1y_4).$$

It is relatively easy to see that F can be written in the form

$$y_1(x_1 + x_2^2) + y_2(x_2 + x_3^2) + y_3(x_1 + x_2 + x_2^2 + x_3^2) - y_1y_4(x_1 - x_2 + x_2^2 - x_3^2) =$$

$$y_1z_1 + y_2z_2 + y_3(z_1 + x_2) - y_1y_4(z_1 - z_2).$$

We first construct the matrix BH(F:x;y)=

$$\begin{pmatrix} y_1 + y_3 + y_1y_4 & 1 + y_4 & 0 & 1 & y_1 \\ \begin{array}{c}(y_2 + y_3 - y_1y_4 + \\ 2x_2(y_1 + y_3 + y_1y_4))\end{array} & -y_4 + 2x_2(1 + y_4) & 1 & 1 + 2x_2 & -y_1 + 2x_2y_1 \\ 2x_3[y_2 + y_3 - y_1y_4] & -2x_3y_4 & 2x_3 & 2x_3 & -2x_3y_1. \end{pmatrix}$$

The matrix BH(F:x;y) has rank at most 2, and for the point

$$(x_1, x_2, x_3; y_1, y_2, y_3, y_4) = (0,0,0;1,1,1,1) = (p,q), BH^*(F : x; y)[x,q] =$$

$$\begin{pmatrix} 3 & 2 & 0 & 1 & 1 \\ 1+6x_2 & -1+4x_2 & 1 & 1+2x_2 & -1+2x_2 \\ 2x_3 & -2x_3 & 2x_3 & 2x_3 & -2x_3 \end{pmatrix}.$$

It is an easy exercise to check that BH* has rank 2 in R^3. Furthermore, the matrix $H^*(F : x; y)[p,q] =$

$$\begin{pmatrix} 2 & 0 & 1 & 1 \\ -1 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

has rank 2. Theorem A.3 states that there are two functions A and B with variables $x_1, \ldots, x_3$, and a function C of two variables such that F = C(A,B). To construct A and B, we first compute the derivatives $D(y_i; F), \quad 1 \leq i \leq 4$. The derivatives are

$$D(y_1; F) = x_1 + x_2^2 + x_1y_4 - x_2y_4 + x_2^2y_4 - x_3^2y_4,$$

$$D(y_2; F) = x_2 + x_3^2, \quad D(y_3; F) = x_1 + x_2 + x_2^2 + x_3^2,$$

and

$$D(y_4; F) = x_1y_1 - x_2y_1 + x_2^2y_1 - x_3^2y_1.$$

At the point q these derivatives are

$$D(y_1; F) = 2x_1 - x_2 + 2x_2^2 - x_3^2, \quad D(y_2; F) = x_2 + x_3^2,$$

$$D(y_3; F) = x_1 + x_2 + x_2^2 + x_3^2,$$

and

$$D(y_4; F) = x_1 - x_2 + x_2^2 - x_3^2.$$

The 2 × 2 submatrix of H^* whose entries are in the first two rows and columns has rank 2. This is equivalent to the observation that the functions $D(y_1; F) = 2x_1 - x_2 + 2x_2^2 - x_3^2$, and $D(y_2; F) = x_2 + x_3^2$, are independent at the point p. It is the conclusion of the theorem that the functions $D(y_1; F) = 2x_1 - x_2 + 2x_2^2 - x_3^2$, and $D(y_2; F) = x_2 + x_3^2$, can be used as the functions A and B. To check this, set $w_1 = 2x_1 - x_2 + 2x_2^2 - x_3^2$, and $w_2 = x_2 + x_3^2$. We can solve these equations for x_1 and x_2, using the Implicit Function Theorem [4,p.7], because we have already observed that the necessary rank condition is satisfied using the first two rows and first two columns of $H^*(F : x; y)[p, q]$. In this case, of course, the solutions are easily written down. That is, $x_2 = w_2 - x_3^2$, and $x_1 = (1/2)(w_1 + w_2 - 2w_2^2 + 4w_2x_3^2 - 2x_3^4)$. The final computation in the proof of Theorem A.3 shows that if we substitute these functions in the original function F, we derive the function a function $G(w_1, w_2; y_1, \ldots, y_4)$ that is independent of the variable x_3. Indeed,

$$G(w_1, w_2; y_1, y_2, y_3, y_4) =$$

$$(w_1y_1)/2 + (w_2y_1)/2 + w_2y_2 + (w_1y_3)/2 + (3w_2y_3)/2 + (w_1y_1y_4)/2 - (w_2y_1y_4)/2.$$

If we set

$$A_1 = 2x_1 - x_2 + 2x_2^2 - x_3^2,$$

and

$$A_2 = x_2 + x_3^2,$$

then

$$G(A_1, A_2; y_1, y_2, y_3, y_4y4) = F.$$

Proof of Theorem A.3.

We now turn to the formal proof of Theorem A.3.

Proof. Condition (i) has already been established in Lemma A.1. We turn to the proof of (ii). Because the matrix $H^*(F_1, \ldots, F_n : x_1, \ldots, x_p; y_1, \ldots, y_q)[x, q]$ has rank r in the set U, there is neighbor hood U'' of p and an $(r \times r)-$submatrix of

$$H^*(F_1, \ldots, F_n : x_1, \ldots, x_p; y_1, \ldots, y_q)[x, q]$$

that has nonzero determinant everywhere in U''. We can assume, without loss of generality, that the rows of the submatrix are indexed by $x_1, \ldots, x_r$ and that the columns are indexed by $(F_{\alpha(1)}, y_{\beta(1)})), \ldots, (F_{\alpha(r)}, y_{\beta(r)})$. The functions of $x = (x_1, \ldots, x_p)$,

$$A_1 = D(y_{\beta(1)}; F_{\alpha(1)})(x, q), \ldots, A_r = D(y_{\beta(r)}; F_{\alpha(r)})(x, q)$$

are C^k–functions of $(x_1, \ldots, x_m)$ in a neighborhood of p. Set

$$z_1 = A_1(x_1, \ldots, x_m), \ldots,\ z_r = A_r(x_1, \ldots, x_m).$$

Because

$$D(x_j; A_i)(p) = D(x_j y_{\beta(j)}; F_{\alpha(i)})(p, q),$$

the matrix with $(i, j)^{th}$ entry $D(x_j; A_i)(p, q)$ has rank r. Therefore, the Implicit Function Theorem [4] shows that there is a neighborhood U^* of p, and C^k–functions

$$h_1(z_1, \ldots, z_r, x_{r+1}, \ldots, x_m), \ldots, h_r(z_1, \ldots, z_r, x_{r+1}, \ldots, x_m)$$

that are defined on U^* such that

$$z_i = A_i(h_1, \ldots, h_r, x_{r+1}, \ldots, x_m), \qquad \text{E.1}$$

$1 \leq i \leq r$, in the set U^*. Then

$$h_i(A_1(x_1, \ldots, x_m), \ldots, A_r(x_1, \ldots, x_m), x_{r+1}, \ldots, x_m) = x_i,$$

$1 \leq i \leq r$, for $(x_1, \ldots, x_p) \in U^*$. Set

$$G_i(w_1, \ldots, w_r, x_{r+1}, \ldots, x_m, y_1, \ldots, y_n) =$$

$$F_i(h_1(w_1, \ldots, w_r, x_{r+1}, \ldots, x_m), \ldots, h_r(w_1, \ldots, w_r, x_{r+1}, \ldots, x_m), y_1, \ldots, y_q),$$

$1 \leq i \leq N$. Because

$$G_i(A_1, \ldots, A_r, x_{r+1}, \ldots, x_m, y_1, \ldots, y_n) =$$

$$F_i(h_1(A_1, \ldots, A_r, x_{r+1}, \ldots, x_m), \ldots, h_r(A_1, \ldots, A_r, x_{r+1}, \ldots, x_m), x_{r+1},$$
$$\ldots, x_m, y_1, \ldots, y_n) = F_i(x_1, \ldots, x_m, y_1, \ldots, y_n),$$

in order to complete the proof of the assertion it will suffice to show that each of the functions G^i is independent of the variables $x_{r+1}, \ldots, x_m$. The hypothesis of (ii) asserts that the column vector $(D(x_1; F_i), \ldots, D(x_m; F_i))^T$ is a linear combination of the columns of the matrix

$$H^*(F_1, \ldots, F_n : x_1, \ldots, x_m; y_1, \ldots, y_n)[x, q]$$

in the neighborhood $U^* \times V$, because BH has rank at most r in $U \times V$, and H^* has rank r in U^*. Therefore, the column $(D(x_1; F_i), \ldots, D(x_m; F_i)^T$ is a linear combination of columns indexed by $(F_{\alpha(1)}, y_{\beta(1)}), \ldots, (F_{\alpha(r)}, y_{\beta(r)})$ in the neighborhood $U^* \times V$. It follows, that for each $1 \leq i \leq N$, and $1 \leq t \leq m$,

$$D(x_t; F_i) = \Sigma_{s=1}^r C_{is} D(x_t; A_s),$$

where the C_{is} are functions on $U^* \times V$. Furthermore, if one differentiates Eq (E.1) by x_j, for $r+1 \leq j \leq m$, it follows that

$$0 = \Sigma_{t=1}^r D(x_t; A_i) D(x_j; h_t) + D(x_j; A_i).$$

Therefore, if $r+1 \leq j \leq m$,

$$D(x_j; G_i) = \Sigma_{t=1}^r D(x_t; F_i) D(x_j; h_t) + D(x_j; F_i) =$$

$$\Sigma_{t=1}^r [\Sigma_{s=1}^r C_{is} D(x_t; A_s)] D(x_j; h_t) + \Sigma s = 1^r C_{is} D(x_j; A_s) =$$

$$\Sigma_{s=1}^r [\Sigma_{t=1}^r D(x_t; A_s) D(x_j; h_t) + D(x_j; A_s)] C_{is} = 0. \square$$

BIBLIOGRAPHY

1. Abelson, H. (1980), "Lower bounds on Information Transfer in Distributed Computations;" JACM, 27, 384-392.

2. Arbib, M.A. (1969), Theories of Abstract Automata; Prentice Hall, Inc. Englewood Cliff, New Jersey.

3. Chen, P. (1992), "A lower bound for the dimension of the message space of the decentralized mechanisms realizing a given goal;" Journal of Mathematical Economics, 21, 249-270.

4. Golubitsky, M. and V. Guillemin (1973), Stable Mappings and Their Singularities; Graduate Texts in Mathematics No.14, Springer Verlag, New York.

5. Hurwicz, L. (1986), "On Informational Decentralization and Efficiency in Resource Allocation Mechanisms;" S. Reiter, ed., Studies in Mathematical Economics Vol. 25, The Mathematical Association of America.

6. _____, (1972), "On Informationally Decentralized Systems;" Decision and Organization, ed. B. McGuire and R. Radner, Amsterdam: North Holland.

7. _____, S. Reiter, and D. Saari (1980), "On Constructing an Informationally Decentralized Process Implementing a Given Performance Function;" Mimeo, Presented and distributed at the Econometric Society World Congress, Aix- en-Province.

8. Jordan, J.S., _____, (1982), "The Competitive Allocation Process Is Informationally Efficient Uniquely;" J. Econ. Theory, 28, 1-18.

9. _____, (1987), "The Informational Requirements of Local Stability in Decentralized Allocation Mechanisms;" Information, Incentives and Economic Mechanisms, ed. by T. Groves, R. Radner and S. Reiter. Minneapolis: University of Minnesota Press.

10. Kalai, E. and W. Stanford (1988), "Finite Rationality and Interpersonal Complexity in Repeated Games;" Econometrica, 56, 397-410.

11. Leontief, W. (1947), "A Note on the Interrelation of Subsets of Independent variables of a Continuous Function with Continuous First Derivatives;" Bull. AMS, 53, 343-350.

12. Mac Lane, S. (1971), Categories for the Working Mathematician; Graduate Texts in Mathematics 5, Springer Verlag; New York.

13. Mount, K. R. and S. Reiter (1974), "The informational size of message spaces;" Journal of Mathematical Economics, 8, 161-192.

14. _____, (1982), "Computation, Communication, and Performance in Resource Allocation;" Presented at the CEME-NBER Decentralization Seminar, University of Minnesota, May 21-23; Mimeo, Northwestern University, 1983.

15. _____, (1983), "On The Existence of a Locally Stable Dynamic Process with a Statically Minimal Message Space;" Information, Incentives and Economic Mechanisms, ed. by T. Groves, R. Radner and S. Reiter. Minneapolis: University of Minnesota Press.

16. _____, (1990), "A Model of Computing With Human Agents;" Discussion Paper No. 890; The Center for Mathematical Studies in Economics and Managerial Science, Northwestern University.

17. Neyman, A. (1985), "Bounded Complexity Justifies Cooperation in the Finitely Repeated Prisoners Dilemma;" Economic Letters, 19, 227-229.

18. Reichelstein, S. (1982), "On the informational requirements for the implementation of social choice rules;" Handout for the Decentralization Conference, Minneapolis, May 1982.

19. _____, (1984), "Incentive Compatibility and Informational Requirements;" J. Econ. Theory, 32, 384-390.

20. _____, and S. Reiter (1988), "Game Forms with Minimal Message Spaces;" Econometrica, 56, 1988, 661-692.

21. Reiter, S. (1977), "Information Incentive and Performance in the New^2 Welfare Economics;" Papers and Proceedings of the Eighty-Ninth Annual Meeting of the American Economic Association, The American Economic Review, 67, 219-237. Reprinted in Studies in Mathematical Economics, Mathematical Association of America, 1987.

22. _____, (1979), "There is no adjustment process with two-dimensional message spaces for counter examples;" summarized in [5]

23. _____, (1994), "A Decentralized Process for Finding Equilibria Given by Linear Equations;" Mimeo, Northwestern University.

24. _____, and C.P. Simon (1992), "Decentralized Dynamic Processes for Finding Equilibrium;" J. Econ. Theory, 56, 400-425.

25. Rubinstein, A. (1986), "Finite Automata Play the Repeated Prisoner's Dilemma;" J. Econ. Theory, 39, 83-96.

26. Saari, D. and C. P. Simon (1978); "Effective price mechanisms;" Econometrica, 46, 1097-1125.

27. Serre, J.P. (1965), Lie Algebras and Lie Groups; W.A. Benjamin, Inc., New York.

28. Sonnenschein, H. (1974), "An Axiomatic Characterization of the Price Mechanism;" Econometrica, 42, 425-460.

29. Widder, D.V. (1963), Advanced Calculus; Prentice Hall; New York.

30. Williams, S. (1988), "Necessary and sufficient conditions for the existence of a locally stable message process;" J. Econ. Theory, 35, 127-154.