Discussion Paper No. 1047

ESSENTIAL REVELATION MECHANISMS AND COMPUTATIONAL COMPLEXITY

by

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

May 1993

---

[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 Grants No. SES-7715793, IST-8314504, and IST-8509678.

Suppose a function F of n real variables is given. Is it possible to write F as a function of fewer than n variables? More particularly, what is the smallest number of variables on which the value of F "really" depends? We mention two contexts in which this question arises.

First, Mount and Reiter [8, 9] have proposed a model of computation in which a network of processors, consisting of a set of processors connected by a directed graph, 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 $s \le r$, 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 $F: E^1 \chi E^2 \chi \ldots \chi E^N \to Z$ 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 for the first time as output of the network at time t.

The question is, 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.

In the case where the sets E^i are finite Arbib and Spira [2] have given a general (i.e., no special assumptions about F are made) lower bound on the number of variables on which F really depends, using the number of elements in certain subsets of the sets E^i, called separator sets. We seek an analogous lower bound for the case in which the sets E^i are infinite, more specifically when they are differentiable manifolds. When these sets are infinite the counting arguments of Arbib and Spira are not applicable. Instead we formulate the concept of separator set in terms of an equivalence relation induced on each of the sets E^i by the function F and obtain an analogous lower bound for the complexity of F in terms of the dimensions of certain quotient spaces discussed below.

Our exploration of this problem makes formal use of the equilibrium form of privacy preserving message exchange processes, sometimes referred to as privacy preserving mechanisms. (See Hurwicz [4] and references cited there.) In order to make this exposition self-contained we digress to provide a brief account of the basic elements of a privacy preserving mechanism. Following that we present briefly the concept of communication complexity of a function in a distributed computation.

Privacy Preserving Mechanisms

There is a finite number N of economic agents each of whom has a space of characteristics. Let E^i denote the space of agent i's characteristics (such as her preference relations). It is assumed that the information about the joint environment $e = (e^1,.....e^N)$ is distributed among the agents so that agent i knows only her characteristic e^i.

There is given a function $F: E^1\chi...\chi E^N \to Z$, called the goal function that expresses the goal of economic activity. For example, for each $e = (e^1,.....e^N)$ in $E^1\chi...\chi E^N$, F(e) is the Walrasian allocation (or trade) when e is the vector of characteristics. Agents communicate by exchanging messages drawn from a message space denoted M. The final or consensus message, also called the equilibrium message, in the environment e is given by a correspondence

$$\mu : E^1\chi \ ...\chi \ E^N \to M.$$

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

A mechanism $\pi = (M, \mu, h)$ is said to realize the goal function F (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

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

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, which 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 Hurwicz [4] and 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 [5] or Hurwicz [4]). 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.

Communication Complexity

The dimension of the message space of a privacy preserving mechanism that realizes F is closely related to the number of variables that must be communicated between processors in a distributed computation of F. The latter problem has been studied under the name communication complexity of F. Abelson[1] first studied this question in the following setting.

We state the problem for two processors. A function

$F:R^{n(1)}{}_{\chi}R^{n(2)} \rightarrow Z$ is to be computed by two processors, where processor 1 (P_1) has the value $x = (x^1.....x^{n(1)})$ in its memory and P_2 knows $y = (y^1.....y^{n(2)})$. The processors are in two-way communication. Each processor computes something on the basis of the variables whose values it knows and communicates the result to the other. This process continues iteratively until one of the processors has the value of F at the point (x,y).

The communication complexity of F is the minimum number of values of variables, (real numbers), that must be communicated in total between the two processors in order to compute the value of F. This number depends on the number of variables x^i, and y^j on which F "really" depends.

The relation between the size of the message space of a privacy preserving mechanism that realizes F and the communication complexity of F is given by the equation dimension M = K + 1, where K is the communication complexity of F. (Mount and Reiter [9]). (Of course, processor P_i is identified with agent i and the sets E^i and $R^{n(i)}$ are identified.)

Separator Sets and Quotients

We return now to the main line of exposition and 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. Specifically, for a function $F: E^1 \times \ldots \times E^N \to Z$ we establish the existence of a collection of sets E^i/F, $1 \le i \le N$,

functions

$$q^i : E^i \to E^i/F,$$

and a function

$$F^* : (E^1/F) \times \ldots \times (E^N/F) \to Z$$

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

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

and

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

for which

$H \circ (p^1 \times \ldots \times p^N) = F$, then there are (one can construct) unique functions

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

such that

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

and

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

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 any object of the category to be specified by identifying a mapping to (or from) the universal object [7]).

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, say, 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.

In any case conditions are imposed that ensures that the quotient object, $(E^1/F)_\chi\ldots_\chi(E^N/F)$, is a topological manifold. In that case, the dimension of the quotient manifold counts the number of variables required.

When the smoothness conditions imposed include 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 is as smooth as the original product $E^1{}_\chi\ldots_\chi E^N$. Possibly Godement's Theorem ([10], 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.

An algebraic characterization of the number of variables required to compute a given function F is obtained from a theorem of Leontief [6], also used by Abelson [1] 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 $F:E^1{}_\chi...{}_\chi E^N \to R$, are rank conditions on the bordered Hessian BH. The matrix BH has rows indexed by coordinates x_i from E^1, and columns indexed by F and by the coordinates y_j from $E^2{}_\chi...{}_\chi E^N$ 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, is the sub-matrix of the bordered Hessian that consists of the columns other than column F.

If at each point x of E^1 the matrix $BH|_x$ has rank r and $H|_{x,y}$ also has rank r at each point x of E^1 and each point y of $E^2{}_\chi...{}_\chi E^N$, then the quotient of E^1 under the equivalence relation "$\approx$" is a manifold of dimension r.

For example, consider the function $K(x,x',y,y') = xy + x'^2 y + 2 x y'^2 + 2 x'^2 y'^2 = (y + 2 y'^2)(x + x'^2)$ 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 H, of K has rank 4.

However, the (nonlinear) change of coordinates given by

$$\varsigma = (x + x'^2),$$

$$\eta = (y + 2y'^2),$$

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

$$K(x, x'; y, y') = \varsigma\eta.$$

The matrices $H|_{x,y}$ and $BH|_x$ both have rank equal to 1.

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

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

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.

It is not possible to eliminate any of the 2N variables X,Y in the computation of Φ. But, no matter what the value of N, ($N \geq 3$), only three real numbers need to be communicated between the two processors to permit Φ to be computed. 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.

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.

Universal Objects and Revelation Mechanisms

We have noted that the quotient manifold serves as a universal object. The concept of universal object comes from category theory. However 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 use an elementary form of mechanism in which each agent uses the space of his parameters as his message 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 such a mechanism is called the essential revelation mechanism, and it is uniquely determined to within isomorphism. This universal object (mechanism) exists when the Hessian conditions (and some smoothness assumptions) are satisfied, and it is the differentiable manifold version of the product $(E^1/F)\chi...\chi(E^N/F)$. 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.

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, 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.

The result on adequate revelation mechanisms in Section 2 require a slightly altered version of Leontief's theorem. This is related to a result announced by Abelson[1]. The four propositions Lemma A1 and Theorems A2, A3, and A4 present the material. They and their proofs are given in Appendix A. Appendix A includes an example of the constructions required.

Section 1. Initial set theoretic constructions

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

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

F-Equivalence

Definition 1.1: Suppose that X_i, $1 \le i \le n$, and Y are sets, suppose that $F: \Pi_1^n X_i \to Y$ is a function, and suppose that $1 \le j \le n$. 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 $(X_1/F) \chi \ldots \chi (X_n/F)$ 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 $F: X_1 \chi \ldots \chi X_n \to Y$ is a function. There is a unique function $F^*: (X_1/F) \chi \ldots \chi (X_n/F) \to Y$ that makes the Diagram 1.1 commute.

[Display Diagram 1.1]

Furthermore, if $Z_1, \ldots, Z_n$ are sets, and if there are functions $g_i: X_i \to Z_i$, $1 \le i \le n$, and a function $G: Z_1 \chi \ldots \chi Z_n \to Y$ 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.

[Display Diagram 1.2]

[Display Diagram 1.3]

Proof of Lemma 1.1.

We first show that if $g_i:X_i \to Z_i$ and $G:\Pi_1^n Z_i \to Y$ are functions that make Diagram 1.2 commute, then we can factor the map $\Pi_1^n g_i$ through the product $\Pi_1^n (X_i/F)$. 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 $F(x \int_i w) = G(g_i(x) \int_i g(w)) = G(g_i(x') \int_i g(w)) = F(x' \int_i w)$. 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 $h^*_i:Z_i \to (X_i/F)$, $1 \le i \le n$, 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 $g^*_i(z) = g^*_i(g_i(x)) = q_i(x) = h^*_i(g_i(x)) = h^*_i(z)$.

Adequate and Essential Revelation Mechanisms

Definition 1.2. Suppose that X_i, $1 \le i \le n$, 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 $g_i:X_i \to M_i$, $1 \le i \le n$,

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

$(y_1, \ldots, y_n) \in X_1 \times \ldots \times X_n$, $F(y_1, \ldots, y_n) = h(g_1(y_1), \ldots, g_n(y_n))$.

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 a 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, $1 \le i \le n$, and Z are nonempty sets and suppose that $F: X_1 \times \ldots \times X_n \to Z$ is a function.

(i) The triple $(q_1 \chi \ldots \chi q_n, (X_1/F) \chi \ldots \chi (X_n/F), F^*)$ is an adequate revelation mechanism that realizes F:

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

(iii) The set $(X_1/F) \chi \ldots \chi (X_n/F)$ 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 indicates 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.[3]).

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 ≥ 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. [3,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 $x_1,\ldots,x_n$ at p 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 [6].

Suppose that $E^1,\ldots,E^n$, are Euclidean spaces of dimensions d(1),..... d(n), such that the space E^i, $1 \le i \le n$ has coordinates $x_i = (x_{i\ 1},\ldots,x_{i\ d(i)})$. Assume that $(p_1,\ldots,p_n)$ is a point of $E^1 \chi \ldots \chi E^n$, and assume that U_i is an open neighborhood of the point p_i, $1 \le i \le n$. We assume that F is a real valued C^2-function defined on $U_1 \chi \ldots \chi U_n$.

We require four matrices.

(I): The matrix

$BH(F: x_{1\ 1}, \ldots, x_{1\ d(1)}; x_{2\ 1}, \ldots, x_{2\ d(2)}; \ldots; x_{n\ 1}, \ldots, x_{n\ d(n)}) =$

$BH(F:x_i:x_{<-i>})$ is a matrix that has rows indexed by $x_{i\ 1},\ldots,x_{i\ d(i)}$ and columns indexed by $F, x_{1\ 1},\ldots,x_{i-1\ d(i-1)},x_{i+1\ 1},\ldots,x_{n\ d(n)}$. The entry in the $x_{(i\ u)}{}^{th}$ row and in the F column is $\partial F/\partial x_{i\ u}$. The entry in row $x_{i\ u}$ and in column $x_{j\ w}$ is $\partial^2 F/\partial x_{i\ u}\ \partial x_{j\ w}$.

The matrix $BH(F:x_i:x_{<-i>})$ is a type of bordered Hessian because it consists of a matrix of second derivatives bordered by a collection of columns of first derivatives.

(II): The matrix $H(F:x_i:x_{<-i>})$ is the submatrix of $BH(F:x_i:x_{<-i>})$ that consists of the columns indexed by $x_{u\ v}$, $u\in\{1,\ldots,i-1,i+1,\ldots,n\}$ and $1\le v\le d(u)$. 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 $F:E^1\chi E^2\to R$, we use a slightly less cumbersome notation. Suppose that E^1 has coordinates $(x_1,\ldots,x_p)$ and E^2 has coordinates $(y_1,\ldots,y_q)$, then 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 $BH(F:x_i:x_{<-i>})$ and $H(F:x_i:x_{<-i>})$ are matrices of functions in the coordinates $x_1,\ldots,x_n$ of $E^1\chi\ldots\chi E^n$. 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 $BH^*(F: x_i: x_{<-i>})[x_i, p_{<-i>}]$

is the matrix that results from evaluating the variables $x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n$ of the entries of $BH(F:x_i:x_{<-i>})$ at the point $p_{<-i>} = (p_1,\ldots,p_{i-1},p_{i+1},\ldots,p_n)$. The matrix $BH^*(F:x_i:x_{<-i>})[x_i,p_{<-i>}]$ is a function of the variables $x_{i\,1},\ldots,x_{i\,d(i)}$ alone.

Similarly, the matrix $H^*(F:x_i:x_{<-i>})[x_i,p_{<-i>}]$ is the submatrix of $BH^*(F:x_i:x_{<-i>})[x_i,p_{<-i>}]$derived by deleting the column indexed by F.

Differential Separability

Definition 2.2. Suppose that $X_1,\ldots,X_n$ are differentiable manifolds, where for each $1 \le i \le n$, X_i has dimension d(i). Suppose that $p_i \in X_i$, $1 \le i \le n$, and suppose that for each i, $\phi_{i\,1},\ldots,\phi_{i\,d(i)}$ is a coordinate system in an open neighborhood U_i of p_i. Suppose that $F:\Pi_1^n X_i \to R$ is a C^2-function. Assume that for $1\le i\le n$, $\phi_i = \Pi\phi_{i\,j}$ 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 $x_{i\,1},\ldots,x_{i\,d(i)}$. 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 $\phi_{1\,1},\ldots,\phi_{n\,d(n)}$ if for each $1\le i\le n$, the matrices

$BH(F\cdot(\Pi\phi_t)^{-1}: x_{i\,1},\ldots,x_{i\,d(i)}; x_{<-i>})$ and

$H^*(F\cdot(\Pi\phi_t)^{-1}:x_{i\,1},\ldots,x_{i\,d(i)}:x_{<-i>})[x_i,0_{<-i>}]$ have rank r_i in a neighborhood

of $(0_1,....0_n)$. If F is differentiably separable of rank $(r_1,....r_n)$ at $(p_1,....p_n)$, and if $r_i=\dim(X_i)$ for each $1\le i\le n$, then we will say that F is differentiably separable at $(p_1,....p_n)$.

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 $1\le i\le n$, X_i and Y_i are C^2-manifolds and suppose that $h_i:Y_i\to X_i$ is a C^2-diffeomorphism. Assume that $g:\Pi_1{}^n Y_i\to R$ and $F:\Pi_1{}^n X_i\to R$ are C^2 -functions such that $g=\Pi\, h_i\cdot F$. Suppose that $(q_1,....q_n)\in\Pi\, Y_i$ and let $h_i(q_i) = (p_i)$. If F is differentiably separable of rank $(r_1,....r_n)$ at $(p_1,....p_n)$, then g is differentiably separable of rank $(r_1, \dots, r_n)$ at $(q_1, \dots, q_n)$.

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

Definition 2.3. If X_i, $1\le i\le n$, are C^2-manifolds, the function $F:X_1\chi \dots\chi\, X_n\to R$ is differentiably separable of rank $(r_1, \dots, r_n)$ at the point $(p_1,....p_n)$ if there is a coordinate system $\{\phi_{i\,j}\}$ at the point $(p_1,....p_n)$ such that F is differentiably separable of rank $(r_1,....r_n)$ at the point $(p_1,....p_n)$ in the coordinate system $\phi_{1\ 1}, \dots, \phi_{n\ d(n)}$.

The Number of Variables On Which F Really Depends

If $F:X_1\,\chi \dots \chi\, X_n\to R$ is differentiably separable of rank $(r(1),....r(n))$ at a point $(p_1,....p_n)$, then it is possible to write F as a function

of variables $\{y_{1\ 1},\ldots,y_{1\ r(1)},\ldots,y_{n\ 1},\ldots,y_{n\ r(n)}\}$. This assertion, Lemma 2.2, is a restatement of Theorem A.4. The proof of Theorem A.4 can be found in Appendix A together with an example of the construction.

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

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

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

A necessary condition that F can be written in the form

$G(y_{1\ 1},\ldots,y_{1\ r(1)},\ldots,y_{n\ 1},\ldots,y_{n\ r(n)})$, where $(y_{i\ 1},\ldots,y_{i\ d(i)})$ is a coordinate system on X_i, is that F is differentiably separable at $(p_1,\ldots,p_n)$ of rank $(s(1),\ldots,s(n))$ where for each $1 \leq j \leq n$, $s(j) \leq r(j)$. Conditions (i) and (ii) are also sufficient for F to be written in the form

$G(y_{1\ 1},\ldots,y_{1\ r(1)},\ldots,y_{n\ 1},\ldots,y_{n\ r(n)})$, for a C^k-function G in a neighborhood of a point $(p_1, \ldots, p_n)$, if 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 $F: X_1 \chi \ldots \chi X_n \rightarrow Z$ is a differentiable function. The triple $(g_1, \ldots, g_n, M_1 \chi \ldots \chi M_n, h)$ that consists of spaces $M_1 \chi \ldots \chi M_n$, maps $g_1, \ldots, g_n$, $g_i: X_i \rightarrow M_i$, $1 \leq i \leq n$, and function $h: M_1 \chi \ldots \chi M_n \rightarrow Z$ 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.

Definition 2.5. Suppose that $F: X_1 \chi \ldots \chi X_n \rightarrow Z$ 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 $Z_1 \chi \ldots \chi Z_n$ if there are submersions $g_i: X_i \rightarrow Z_i$, and a differentiable mapping $h: Z_1 \chi \ldots \chi Z_n \rightarrow Y$ such that the diagram in Diagram 2.1 commutes [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 the matrix $BH(F: x_i; x_{<-i>})$ 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 the generalization of a theorem of Leontief and Abelson given in 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 $x_{i\,1},\ldots,x_{i\,d(i)}$ and a function G such that the subset that consists of the coordinates $F(x_{1\,1},\ldots,x_{n\,d(n)}) = G((x_{i\,1},\ldots,x_{i\,r}) \int_i x_{<-i>})$. We can use the remaining set of coordinates in X_i to determine a subspace S of X_i by setting $x_{i\,r+1} = 0,\ldots, x_{i\,d(i)} = 0$. The set S is a submanifold of X_i and the restriction of F to the space $S \chi X_{<-i>}$ has the property that $BH(\text{restriction}(F):x_{i\,1},\ldots,x_{i\,r}:X_{<-i>})$ 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 discussion is devoted to adding enough restrictions to ensure that the local argument can be carried out globally on $X_1 \chi \ldots \chi X_n$.

Theorem 2.2. Suppose that X_i, $1 \le i \le n$, is a Euclidean space of dimension $d(i) \ge 1$. Suppose that for each $1 \le i \le N$, 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 $(p_1,\ldots,p_n) \in U_1 \chi \ldots \chi U_n$. 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 $z_j \chi w_j$ position, $1 \le j \le m$, 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 $F(z, w) =$ $F(0, 0) + u \cdot z + v' \cdot w + w \cdot z + z^T Q z + w^T Q' w + P(z^*, w^*)[z, w]$ where Q and Q' are square matrices, u and v' are vectors in R^m and R^N respectively, $v' \cdot w$ 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 $U \chi V$ evaluated at some point $z^* \epsilon U$ and $w^* \epsilon V$. These coefficients of P are bounded on a ball that is a compact neighborhood of $(0, 0) \epsilon U' \chi V'$, $U' \subseteq U$ and $V' \subseteq V$. Then for $z, z' \epsilon U'$ and $w \epsilon V'$, $|F(z,w)-F(z',w)| =$ $|u \cdot (z-z') + w \cdot (z-z') + z^T Q z' + P(z'^*, w'^*)[z', w] - P(z^*, w^*)[z, w]|$. 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 $u \cdot v = L$, and set $(z-z') = v$. To complete the proof, it will suffice to show that the function

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

is not constant on the ball V'. For this it will suffice to show that the function $Q = w \cdot v + P(z'^*, w'^*)[z', w] - P(z^*, w^*)[z, w]$ is not constant on the ball V'. The function $P(z'^*, w'^*)[z', w]\, P(z^*, w^*)[z, w]$ is a homogeneous

cubic $\sum a_{\alpha\ \beta}\ z^{\alpha}\ w^{\beta}$ in the variables $w_1,\ldots,w_N$ with coefficients $\{a_{\alpha\ \beta}(z,z',w,w')\}$ that are functions bounded on $U'\chi V'$. Set $w = tv$. The powers of the constants $z_1,\ldots,z_m$ can be combined with the coefficients $a_{\alpha\ \beta}$ and therefore $Q = t|v|^2 + a(t)\ t^3$, 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 $|v|^2 + a(t)t^2 = c$ (a constant), then $a(t) = (c - |v|^2)/t^2$, 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 $F:X_1\chi\ldots\chi X_n\rightarrow R$ induces strong equivalence on X_i, if the following condition is satisfied for each $x, x' \in X_i$, such that $x \neq x'$:

if there is an open neighborhood U of a point $q\in X_{<-i>}$, such that $F(x\ \int_i u) = F(x'\ \int_i u)$ for each $u\in U$, then $F(x\ \int_i z) = F(x'\ \int_i z)$ 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 $x_{i\ j}$.

$1 \le i \le n$, $1 \le j \le d(i)$. If for each $1 \le i \le n$, $\beta(i) = (\beta(i\ 1).....\beta(i\ d(i)))$ is a sequence of nonnegative integers, denote by $x_i^{\beta(i)}$ the monomial $x_{i\ 1}^{\beta(i\ 1)} ... x_{i\ d(i)}^{\beta(i\ d(i))}$, and denote by $x_1^{\beta(1)}...x_n^{\beta(n)}$ the product of the monomials $x_i^{\beta(i)}$. Write $F(x_1,.....,x_n) = \sum_{\beta(1),\ ...\ ,\beta(n)} A_{\beta(1)...\beta(n)}(x_1)\ x_2^{\beta(2)}...x_n^{\beta(n)}$, where the $A_\beta(x_1)$ 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

$\sum [A_\beta(x_1) - A_\beta(x'_1)]\ x_2^{\beta(2)}...x_n^{\beta(n)} = 0$ for the $x_2,.....x_n$ chosen arbitrarily in an open set in $X_2 \chi ... \chi X_n$. 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, $1 \le i \le n$ are C^4 manifolds of dimensions $d(1).....d(n)$, respectively. Suppose that $F: X_1 \chi ... \chi X_n \to R$ is a C^4 function that is differentiably separable on $X_1 \chi ... \chi X_n$ of rank $(r(1).....r(n))$ where each $r_i \ge 1$. 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 $1 \le i \le n$,

then, for each $1 \le i \le n$, 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 $p_i^* \in (X_i/F)$, $1 \le i \le n$. Choose a point $p_i \in X_i$, $1 \le i \le n$, such that $q_i(p_i) = p_i^*$. Because the function F is differentiably separable of rank $(r(1),\ldots,r(n))$ at the point $(p_1,\ldots,p_n)$, it follows from Lemma A.3 that for $1 \le i \le n$, 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 $x_i = (x_{i\ 1},\ldots,x_{i\ d(i)})$ 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 $F(x_1,\ldots,x_n) = G((x_{i\ 1},\ldots,x_{i\ r(i)})\ \int_i\ z)$ for each $z \in U_{<-i>}$. Denote by S^*_i the set of elements $(x_{i\ 1},\ldots,x_{i\ r(i)},0,\ldots,0)$ that lie in U_i. Choose in S^*_i a compact neighborhood S_i of $(0,\ldots,0)$ (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

$F(x_{i\ 1},\ldots,x_{i\ r(i)},b_1,\ldots,b_{d(i)-r(i)}\ \int_i\ z_{<-i>}) =$

$F((x_{i\ 1},\ldots,x_{i\ r(i)},0,\ldots,0)\ \int_i\ z_{<-i>})$ implies that $q_i(x_{i\ 1},\ldots,x_{i\ d(i)}) =$

$q_i(x_{i\ 1},\ldots,x_{i\ r(i)})$ for each $(x_{i\ 1},\ldots,x_{i\ d(i)})$ 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 in 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, $1 \le i \le n$ are C^4-manifolds and that X_i has dimension d(i). Assume that $F:X_1 \chi \ldots \chi X_n \to R$ is a real valued function on F that satisfies the following conditions:

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

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

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

Then the triple $(q_1 \chi \ldots \chi q_n, (X_1/F) \chi \ldots \chi (X_n/F), F^*)$ where:

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

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

(3) $F^*:(X_1/F) \chi \ldots \chi (X_n/F) \to R$ is the function such that

$F^*(q_1(x_1), \ldots, q_n(x_n)) = F(x_1,\ldots,x_n)$ for each $(x_1,\ldots,x_n) \in X_1 \chi \ldots \chi X_n$,

is an adequate C^0-revelation mechanism that realizes F. The space (X_i/F) has dimension r(i). Furthermore, if a triple $(g_1 \chi \ldots \chi g_n, Z_1 \chi \ldots \chi Z_n, G)$ is such that $g_i:X_i \to Z_i$, $G:Z_1 \chi \ldots \chi Z_n \to R$, and the triple is an adequate revelation mechanism that realizes F, then there are continuous maps $g^*_i:Z_i \to (X_i/F)$ such that the diagram in Diagram 1.3 commutes, with Y = R.

Proof. We have already shown in Theorem 2.3 that the triple $(q_1\chi...\chi q_n,(X_1/F)\chi...\chi(X_n/F),F^*)$, is an adequate revelation mechanism that realizes F. Suppose that $z^*_i \in Z_i$. Denote $(g_1(w),....,g_{i-1}(w),g_{i+1}(w),....,g_n(w))$ 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 $w \in X_{<-i>}$, $F(x^*_i \int_i w) = G(g_i(x^*_i) \int_i g_{<-i>}(w)) = G(g_i(x'_i) \int_i g_{<-i>}(w)) = F(x'_i \int_i w)$. Therefore $q_i(x^*_i) = q_i(x'_i)$. Set $g^*_i(z^*_i) = q_i(x^*_i)$. Because the map $g_i: X_i \to Z_i$ has a thread in the neighborhood of each point, there is a neighborhood N of the point z^*_i and a thread $s_i: N \to X_i$ such that $g_i(s_i(z^*)) = g_i(z^*)$ for each $z^* \in N$. 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.

Appendix A.

Leontief and Abelson Theorem

Suppose that $F(x_1,....x_N)$ is a function of N variables which has continuous partial derivatives to order d. For each sequence $\alpha = (\alpha(1),....\alpha(N))$ of nonnegative integers, denote by $|\alpha|$ the sum $\alpha(1)+...+\alpha(N)$. We denote by $D(x_1^{\alpha(1)}...x_N^{\alpha(N)};F)$ the derivative $\partial^{|\alpha|}F/\partial x_1^{\alpha(1)}...\partial x_N^{\alpha(N)}$, $d>|\alpha|$. 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 $(F \cdot G)(x)$ 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.[11].

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

(i) $$\begin{vmatrix} D(x_1; F) & ...D(x_m; F) \\ D(x_1; G) & ... D(x_m; G) \end{vmatrix}$$

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 $w - G(x_1,....x_m) = 0$

has a unique solution in a neighborhood U' of (p,q). That is, 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 $1 \le j \le m$. 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 $C(G(x_1,\ldots,x_m),y) = F(c(G(x_1,\ldots,x_m), x_2,\ldots, x_m),x_2,\ldots,x_m,y) = F(x_1,\ldots,x_m,y)$.

Leontief's Theorem

Leontief proved the following result in [6].

Theorem A.2. Suppose that F is a function of the variables $x_1,\ldots,x_m,\ldots,y_1, \ldots, y_n$. Set $F_i = D(x_i; F)$, $1 \le i \le m$. 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 $1 \le i, j \le m$ and each $1 < k \le n$, $(\partial/\partial y_k)[F_i/F_j] = 0$,

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

Proof. Form the matrix

$$M = \begin{vmatrix} F_1 & \cdots & F_m \\ F^*_1 & \cdots & F^*_m \end{vmatrix}$$

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 $F(x, y) = C(G(x), y)$.

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 neighborhood 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 in order 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, $\omega(F_1,....,F_m)^t = (D(x_1y_k; F),....,D(x_my_k; F))^t$ (M^t denotes the transpose of M). Thus $\omega D(x_i;F) = D(x_iy_k;F) = D(y_k;F_i)$ for each i and k. Therefore $D(y_k;F_i/F_j) = 0$ for all k.

Corollary A.2.2. Suppose that F(x; y) is a C^2-function in the variables $x = (x_1,....,x_m)$ and $(y_1,....,y_n)$. A necessary condition that there exist functions C(u,v), A(x), and B(y) such that F(x;y) = C(A(x),B(y)) is that the

matrices BH(F:x:y) and BH(F:y:x) each have rank at most one. Further, assume that for some $1 \le j \le m$ and some $1 \le k \le n$, $D(x_j:F)(p,q) \neq 0$ and $D(y_k:F)(p,q) \neq 0$, then the matrix rank conditions are also sufficient for the existence of C, A, and B such that F = C(A, B).

Proof. Because BH(F:x: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 $D(wy_j:C) = D(x_1y_j:F)\ D(w:h)$. By hypothesis there is a Θ such that $D(x_1y_j:F) = \Theta\ D(y_j:F)$ 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 $w^{(0)} = F(p:q)$, $D(y_j:C(w,y))(p:q) \neq 0$. 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 $h(F(x_1,\ldots,x_m:q),x_2,\ldots,x_m) = x_1$. If $w^{(0)} = F(p:q)$, because C(w,y) is independent of the variables $x_2,\ldots,x_m$, it follows that $C(w^{(0)},y) = F(h(F(p:q),p_2,\ldots,p_m:y) = F(p:y)$. Therefore $D(y_j:C) = D(y_j:F(p:y)) \neq 0$ for some j.

Corollary A.2.3. Suppose that $x_{i,\,j}$, $1 \le i \le r$, $1 \le j \le d(i)$ are r ordered sets of variables. Denote by x_i the set of variables $(x_{i,\,1},\ldots,x_{i,\,d(i)})$. Assume that $p = (p_1,\ldots,p_p) = (p_{1,\,1},\ldots,p_{r,\,d(r)})$ is a point. Necessary conditions that

in some neighborhood of the point p there exist functions G, A_j, $1 \le j \le r$ such that $F(x_{1,\,1},\ldots,x_{r,\,d(r)}) = G(A_1(x_1),\ldots,A_r(x_r))$ is that each matrix $BH(F{:}x_j{:}x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_r)$ has rank at most one. The condition is also sufficient if for each j, there exists a k(j) such that the derivative $D(x_{j,\,k(j)};\, F(p_1,\ldots,p_{j-1},x_j,p_{j+1},\ldots,p_r)) \neq 0$.

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 $(x_1,\ldots,x_m)$ and Y has coordinates $(y_1,\ldots,y_n)$. Assume that $F_1,\ldots,F_N$ are functions from $X\chi Y$ to R that are defined on a neighborhood $U\chi V$ of a point (a,b), $a\epsilon X$ and $b\epsilon Y$. A necessary condition that there are functions $A_1(x_1,\ldots,x_m),\ldots,A_r(x_1,\ldots,x_m)$, functions $G_i(W_1,\ldots,W_r,y_1,\ldots,y_n)$, $1\le i\le N$, 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 $(x_1,\ldots,x_m)\epsilon U$ and $(y_1,\ldots,y_n)\epsilon V$ 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 $U\chi V$.

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 $D(x_j;\, F_i) = \sum_{s=1}^{r} D(A_s;\, G_i)\, D(x_j;\, A_s)$ and $D(x_j\, y_k;\, F_i) = \sum D(y_k\, A_s;G_i)\, D(x_j;A_s)$. Each of the columns is a linear combination of the r columns $(D(x_1;A_i),\ldots,D(x_m;A_i))^t$, $1\le i\le r$, where the superscript t denotes the transpose. 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 $W \chi V$ of a point $(p',q)\in R^r \chi V$, 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 $U \chi V$ 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 $1 \le i \le N$, 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 $U \chi V$.

(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 $U\chi V$, 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 $R^r \chi Y$, a neighborhood $W\chi V'$ of (p',q), a neighborhood $U'\chi V'$ of (p,q), C^k-functions $G_1,\ldots,G_N$, defined on $W\chi V'$, 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 $U'\chi V'$, $F_i(x_1,\ldots,x_m,y_1,\ldots,y_n) = G_i(A_1(x_1,\ldots,x_m),\ldots,A_r(x_1,\ldots,x_m), y_1,\ldots,y_n)$, $1 \le i \le N$, 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).

$BH(F:x;y) =$

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

the matrix BH(F:x;y) has rank at most 2, and for the point $(x_1,x_2,x_3;y_1,y_2,y_3,y_4) = (0, 0, 0; 1, 1, 1, 1) = (p, q)$, $BH^*(F: x; y)[x, q] =$

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

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

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

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 $D(y_i;F)$, $1 \le i \le 4$. The derivatives are $D(y_1;F) = x_1 + x_2^2 + x_1y_4 - x_2y_4 + x_2^2y_4 - x_3^2y_4$, $D(y_2;F) = x_2 + x_3^2$, $D(y_3; F) = x_1 + x_2 + x_2^2 + x_3^2$, 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 $D(y_1;F) = 2x_1 - x_2 + 2x_2^2 - x_3^2$, $D(y_2; F) = x_2 + x_3^2$, $D(y_3; F) = x_1 + x_2 + x_2^2 + x_3^2$, and $D(y_4; F) = x_1 - x_2 + x_2^2 - x_3^2$. The 2 x 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 [3,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 $G(A_1, A_2; y_1, \ldots, y_4) = F$.

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 neighborhood U' of p and an (r x 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 [3] 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

(Eq.4.1) $z_i = A_i(h_1,\ldots,h_r, x_{r+1},\ldots, x_m)$,

$1\le i\le r$, in the set U^*. Then $h_i(A_1(x_1,\ldots,x_m),\ldots,A_r(x_1,\ldots,x_m),x_{r+1},\ldots,x_m) = x_i$, $1\le i\le r$, for $(x_1,\ldots,x_p) \in U^*$. Set $G_i(w_1,\ldots,w_r,x_{r+1},\ldots,x_m,y_1,\ldots,y_n) = F_i(h_1(w_1, \ldots, w_r, x_{r+1},\ldots x_m), \ldots, h_r(w_1,\ldots, w_r, x_{r+1}, \ldots, x_m), y_1, \ldots, y_q)$, $1 \le i \le N$. 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 $U_\chi V$, 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 the columns indexed by $(F_{\alpha(1)},y_{\beta(1)}),\ldots,(F_{\alpha(r)},y_{\beta(r)})$ in the neighborhood $U *_\chi V$. It follows, that for each $1 < i < N$, and $1 \leq t < m$, $D(x_t:F_i) = \Sigma_{s=1}^{r} C_{is}\, D(x_t:A_s)$, where the C_{is} are functions on $U *_\chi V$. Furthermore, if one differentiates Eq 4.1 by x_j, for $r+1 \leq j < m$, it follows that $0 = \sum_{t=1}^{r} D(x_t:A_i)\, D(x_j:h_t) + D(x_j:A_i)$. Therefore, if $r+1 < j < m$, $D(x_j:G_i) = \Sigma_{t=1}^{r} D(x_t:F_i)\, D(x_j:h_t) + D(x_j:F_i) =$

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

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

BIBLIOGRAPHY

1. Abelson, H. (1980): Lower bounds on Information Transfer in Distributed Computations: JACM, Vol. 27, No. 2, April 1980, pp. 384-392.

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

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

4. Hurwicz, Leonid:(1986): On Informational Decentralization and Efficiency in Resource Allocation Mechanisms: Stanley Reiter, ed., Studies in Mathematical Economics Vol. 25, The Mathematical Association of America.

5. Hurwicz, L., 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.

6. Leontief, Wassily:(1947): A Note on the Interrelation of Subsets of Independent variables of a Continuous Function with Continuous First Derivatives; Bull. AMS, vol. 53; pp.343-350

7. Mac Lane, Saunders(1971): Categories for the Working Mathematician: Graduate Texts in Mathematics 5, Springer Verlag: New York.

8. Mount, K. R. and Reiter, Stanley:(1982): Computation, Communication, and Performance in Resource Allocation: Presented at the CEME-NBER Decentralization Seminar, University of Minnesota, May 21-23.

9. Mount, K. R., and Reiter, Stanley:(1990): A Model of Computing With Human Agents, Discussion Paper No. 890; The Center for Mathematical Studies in Economics and Managerial Science.

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

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