

# A lower bound on computational complexity given by revelation mechanisms<sup>★</sup>

Kenneth R. Mount<sup>1</sup> and Stanley Reiter<sup>2</sup>

<sup>1</sup> Department of Mathematics, Northwestern University, Evanston, IL 60208-2014, USA

<sup>2</sup> Department of Economics and Kellogg Graduate School of Management, Northwestern University, Evanston, IL 60208-2014, USA

Received: June 3, 1993; revised version August 2, 1994

**Summary.** This paper establishes a lower bound on the computational complexity of smooth functions between smooth manifolds. It generalizes one for finite (Boolean) functions obtained (by Arbib and Spira [2]) by counting variables. Instead of a counting procedure, which cannot be used in the infinite case, the dimension of the message space of a certain type of revelation mechanism provides the bound. It also provides an intrinsic measure of the number of variables on which the function depends. This measure also gives a lower bound on computational costs associated with realizing or implementing the function by a decentralized mechanism, or by a game form.

## 1. Introduction

This paper establishes an elementary lower bound on the computational complexity of smooth functions between Euclidean spaces (actually, smooth manifolds). The main motivation for this comes from mechanism design theory. The complexity of computations required by a mechanism determines an element of the costs associated with that mechanism. The lower bound presented in this paper is useful in part because it does not require specification in detail of the computations to be performed by the mechanism, but depends only on the goal function that the mechanism is to realize or implement.

Our lower bound generalizes a bound due to Arbib and Spira [2] for the complexity of functions between finite sets. The Arbib-Spira bound is based on the concept of *separator sets* for a function. This concept corresponds to the number of (Boolean) variables that the function actually depends on. In the finite case the number of variables can be easily counted. But a counting procedure is too crude to 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 applies to functions with infinite domains and ranges. The counting procedure is replaced by

---

\* This research was supported by National Science Foundation Grant No. IRI-9020270.

Correspondence to: S. Reiter

construction of a *universal object in a category*, namely the category of *encoded revelation mechanisms* ( $\text{ERM}(F)$ ) that realize the function  $F$ , whose complexity is under analysis. The universal object is a minimal encoded revelation mechanism called an *essential revelation mechanism*. The dimension (when it exists) of the message space of the universal object is the number of variables on which  $F$  really depends.<sup>1</sup>

In addition to this abstract characterization of the number of variables that must be used in order to compute the function  $F$ , we give an algebraic characterization in terms of conditions on the ranks of certain bordered Hessian matrices of  $F$ .

The formal presentation of this material is organized as follows. Section 1 contains the set theoretic constructions used subsequently. Definitions of  $F$ -equivalence, of encoded 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,  $F$ , is the smallest encoded revelation mechanism that serves as a universal object in the category  $\text{ERM}(F)$  of encoded revelation mechanisms for  $F$ . Section 2 deals with the case where the domain of  $F$  is a product of smooth manifolds, and  $F$  is smooth. Simple conditions are given that ensure that the quotient sets (under  $F$ -equivalence) are topological manifolds and therefore have dimensions.

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

In Section 3 we discuss the relationships between our construction and certain theorems of Hurwicz, Chen and Abelson, which arise in connection with analysis of dimension of message spaces.

Appendix A contains three propositions and their proofs, namely Lemma A.1, Theorem A.2 and Theorem A.3. These propositions present a slightly altered version of a theorem of Leontief that is used to obtain the results on encoded revelation mechanisms in Section 2. This result is related to a result announced in [1]. Appendix A also contains an example of the constructions required.

The remainder of this Introduction contains an informal presentation of background and concepts useful for understanding the formal presentation that follows, and for relating our results to the literature on mechanism design. We begin with a brief informal discussion of computational complexity of functions.

## Computational complexity of functions

The computational complexity of a function depends on the model of computing used. We use the model of computing presented in [14], (an elementary exposition is in [16]). In that model there is a network consisting of a set of elementary processors connected by a directed graph, which computes as follows.

---

<sup>1</sup> While we use a concept from category theory, our analysis is self-contained and does not require knowledge of category theory other than the concept of a universal object in a category, which is explained in the paper. This concept is not new to economic theory; Sonnenschein [28] and Jordan [8] have used it in analyzing economic mechanisms.

Each processor  $p$  receives the values of its inputs, say,  $x^1, \dots, x^s$ , from outside the network, or from immediately preceding processors, and computes in one unit of time the value of a function  $y = f_p(x^1, \dots, x^s)$ . Here  $s \leq r$ , where  $r$  is a given integer 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. The class  $\mathcal{F}$  is a primitive of the model. Each processor sends the result of its computation to every successor, i.e., to every processor to which it is directly connected, or to outside the network if it has no successor.

A network of this kind, called an  $(r, d)$ -network in [14] and [16], is said to compute a function

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

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

In the finite case, when  $\mathcal{F}$  consists of Boolean functions, every  $(r, d)$ -network is equivalent to a finite state machine, and conversely every finite state machine can be represented as an  $(r, d)$ -network. (See [14].) The complexity of  $F$  relative to the class of networks characterized by  $r, d$  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 that class.)

An  $(r, d)$ -network,  $Q$ , that computes  $F$  in time  $t$  may contain loops. It is shown in [14, Lemma 3.2] that an  $(r, d)$ -network,  $T$ , can be constructed that is free of loops, that uses the same elementary functions (modules) that  $Q$  uses (perhaps with the Identity function added to the functions used by  $Q$ ), and computes  $F$  in time  $t$ . The network  $T$  is a tree with inputs entering at the leaves and value of  $F$  emerging at the root. The length of  $T$  is the time needed to compute  $F$ . Therefore, for a fixed  $r$ , the number of variables entering at the leaves determines a lower bound on the length of a tree that computes  $F$ , since each node of  $T$  can have at most  $r$  predecessors. Thus the minimum number of variables on which  $F$  depends provides a lower bound on the time needed to compute  $F$  by  $(r, d)$ -networks with elementary functions  $\mathcal{F}$ .

To arrive at this lower bound it is helpful to view the process of computing  $F$  as follows. Each factor  $E^i$  in the domain of  $F$  is regarded as the parameter space of an agent  $i$ , and is equipped with coordinates. To compute  $F$  at the point  $(e^1, \dots, e^N)$ , for each  $i$ , agent  $i$  sends the coordinates of the point  $e^i$  to the  $(r, d)$ -network that computes  $F$ . Thus agent  $i$ 's message is the same as that used by a direct revelation mechanism. But it may well be the case that some coordinates of  $e^i$  are not needed to compute  $F$  at  $e$ . In that case only partial revelation of  $e^i$  would be required. Therefore we extend the concept of a revelation mechanism to include partial revelation.

When the domain of  $F$  is a smooth manifold, the number of variables on which  $F$  depends is not obvious. Suppose that  $F$  is a real valued function with partial derivatives defined on the Euclidean space  $E^1 = R^2$ , 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  $F$  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  $x$ .

Beyond that, when  $F$  is defined on a product space, there is a natural restriction on coordinate changes allowed in the product  $E^1 \times \dots \times E^N$ . The restriction is to allow only coordinate changes that are the product of individual coordinate changes in the separate spaces  $E^i$ . This is especially clear when the space  $E^i$  is the parameter space of an agent  $i$ . While there may be nothing intrinsic about the coordinate system used in  $E^i$ , since agent  $i$ 's parameters are private to  $i$ , coordinate transformations that depend on parameters in  $E^j$  with  $j \neq i$  should certainly be ruled out. Moreover, even when the spaces  $E^i$  are not parameter spaces of agents, such transformations should be ruled out, because computations helpful in evaluating  $F$  could be carried out via such transformations, but in a form concealed from the analysis. With this restriction one can ask for a lower bound on the number of parameters from coordinate systems in  $E^i$  needed 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 of 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  $G(a; y) = G(b; y)$  independent of the point  $y$  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  $Y$ .

With these considerations in mind, we extend the concept of a revelation mechanism to allow for partial revelation of parameters in any allowable coordinate system in the space  $E$ . We refer to a mechanism of this type as an *encoded revelation mechanism*. Note that while these mechanisms form a larger class than do revelation mechanisms, that class does not include all privacy preserving mechanisms, or game forms, with the given structure of private information.

In order to make this point clear and to help make this paper self-contained, we include below a brief summary of the formal structure of privacy preserving mechanisms, and relate encoded revelation mechanisms to them. This is done in the

part of the Introduction headed **Privacy Preserving Mechanisms, Universal Objects and Encoded Revelation Mechanisms.**

### Separator sets and quotients

Our formulation of the concept of separator sets for the function  $F$  is in terms of an equivalence relation induced on each of the sets  $E^i$  by  $F$ . To begin with, this is stated set theoretically without topological or smoothness conditions on the set  $E^i$ . The quotient constructions are quite elementary. 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 procedure used to construct the quotients that describe the number of variables on which the function  $F$  depends is a natural generalization of the argument used in the discussion of the function  $G(x_1, x_2, y_1, y_2) = x_1 y_1 + x_2 y_2$ . The quotient object so constructed has the natural set theoretic structure of a universal object. The remaining task is to show that in the case of differentiable functions, a set of rank conditions on certain matrices associated with the function under analysis ensure that the quotient object has the structure of a differentiable manifold. The manifold structure on the quotient object allows us to conclude that the dimension of the quotient exists as a topological concept and that the dimension of the quotient is the number of variables required to compute the function. The universality condition guarantees that the quotient object is a space with the least number of variables sufficient to compute the function.

Specifically, for a function  $F: E^1 \times \dots \times E^N \rightarrow Z$  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  $F^*: (E^1/F) \times \dots \times (E^N/F) \rightarrow Z$  that together satisfy the following conditions. First, the composition

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

and second, if there are functions

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

and

$$H: X^1 \times \dots \times X^N \rightarrow Z$$

for which

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

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

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

These conditions state that the quotient object  $(E^1/F) \times \dots \times (E^N/F)$  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 [12]).

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 set. 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  $(x_1, \dots, x_t)$  around a point, in (say)  $E^1$ , it were possible to ignore the coordinate  $x_t$  and still to evaluate  $F$ , then knowledge of the coordinates  $(x_1, \dots, x_{t-1})$  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 " $(x_1, \dots, x_{t-1}, x_t) \approx (x_1, \dots, x_{t-1}, x'_t)$ " if and only if  $F(x_1, \dots, x_{t-1}, x_t) = F(x_1, \dots, x_{t-1}, x'_t)$ . 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  $(E^1/F) \times \dots \times (E^N/F)$ , the quotient object, is a topological manifold. In that case, the dimension of the quotient manifold counts the number of variables required.

When we assume the existence of certain local threads, 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  $E^1 \times \dots \times E^N$ . Possibly Gode-ment's Theorem ([27], 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].<sup>2</sup>

The conditions we use for the construction of a "good" quotient of  $E^1$  where  $F: E^1 \times \dots \times E^N \rightarrow R$ , 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

<sup>2</sup> Abelson used this result to construct a lower bound on the communication complexity of  $F$  in a distributed system. In Abelson's paper, communication complexity is the number of real variables that must be transmitted among the processors in order to compute  $F$ . This is essentially the same as the size of the message space in the analyses carried out by Hurwicz [5] and Chen [3]. The relationship of our results to theorems about communication complexity or size of the message space is discussed below in Section 3.

$F$  and by the coordinates  $y_j$  from  $E^2 \times \dots \times E^N$  with the  $(x_i, F)$  entry being  $(\partial F/\partial x_i)$  and the  $(x_i, y_i)$  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  $F$ .

The Full Bordered Hessian,  $FBH(F)$  is the Bordered Hessian with a row added indexed by  $F$ . The entry in position  $(F, F)$  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  $(E^1/F)$ . 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  $E^2 \times \dots \times E^N$ , then the quotient of  $E^1$  under the equivalence relation “ $\approx$ ” is a manifold of dimension  $r$ .

As an example, consider the function  $K(x, x', y, y') =$

$$xy + x'^2y + 2xy'^2 + 2x'^2y'^2 = (y + 2y'^2)(x + x'^2)$$

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  $H^{\#}(K)$ , of  $K$ , with rows and columns indexed by all variables  $x, x', y, y'$ , has rank 4.

However, the (nonlinear) change of coordinates given by

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

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

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

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

**Privacy preserving mechanisms, universal objects and encoded revelation mechanisms**

The basic setup is as follows. 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  $e = (e^1, \dots, e^N)$  is distributed among the agents so that agent  $i$  knows only her characteristic  $e^i$ . Given is a function  $F: E^1 \times \dots \times E^N \rightarrow Z$ , called the *goal function* that expresses the goal of economic activity. For example, for each  $e = (e^1, \dots, e^N)$  in  $E^1 \times \dots \times E^N$ ,  $F(e)$  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

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

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  $F$  (on  $E$ )<sup>3</sup> if for all  $e$  in  $E$ ,

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

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

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

This condition states that the set of equilibrium messages 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].) A revelation mechanism is, of course, one in which each agent transmits his/her parameter value to the message space. (If the mechanism realizes  $F$  then the outcome function  $h$  is  $F$  itself). Formally this can be represented as a mechanism in which the message space  $M$  is a product  $M = M^1 \times \dots \times M^N$ . If  $M^i = E^i$ , and if the individual message correspondence of agent  $i$  maps the parameter vector  $e^i$  in  $E^i$  to

$$\mu^i(e^i) = M^1 \times \dots \times M^{i-1} \times \{e^i\} \times M^{i+1} \times \dots \times M^N,$$

then the mechanism is a *direct revelation mechanism*.

When  $\mu^i$  is given by equilibrium equations, we may write it as  $m^i - e^i = 0$ , and define  $g^i: E^i \rightarrow M^i$  by

$$g^i(e^i) = m^i \text{ if and only if } m^i - e^i = 0.$$

The mechanism realizes  $F$  if the outcome function  $h$  satisfies the condition that

$$F(e^1, e^2, \dots, e^N) = h(g^1(e^1), g^2(e^2), \dots, g^N(e^N)).$$

If we permit  $M^i$  to be any space obtained from  $E^i$  by allowable coordinate transformations, then the mechanism

$$(M^1, \dots, M^N, g^1, \dots, g^N, h)$$

is an encoded revelation mechanism.

Let  $ERM(F)$  denote the class of encoded revelation mechanisms that realize  $F$ . If the mechanisms in  $ERM(F)$  have a universal object, then we call it the essential revelation mechanism for  $F$ . It is unique to within isomorphism. The universal object exists when certain conditions on Hessian matrices of  $F$ , and when certain smoothness assumptions, are satisfied. The universal object is the product

<sup>3</sup> More generally,  $F$  can be a correspondence, in which case the definition of realizing  $F$  must be modified, as in [5].

$(E^1/F) \times \dots \times (E^n/F)$ , with a differentiable manifold structure on each of the factors  $(E^i/F)$ . The dimension of  $(E^i/F)$  is a lower bound on the number of variables agent  $i$  must reveal to the computing network for  $F$  to be computed; the sum of these numbers over the agents is a lower bound on the number of variables on which  $F$  really depends, and therefore determines a lower bound on the computational complexity of  $F$ . The computational complexity of  $F$  is an indicator of the costs of computation that are incurred by any mechanism that realizes  $F$ . It also indicates the computational costs of implementing  $F$  by game forms, because to each equilibrium of a game form that implements  $F$  there corresponds a privacy preserving mechanism that realizes  $F$ . (See [20].)

Let  $PPM(F)$  denote the class of all privacy preserving mechanisms that realize  $F$ . The construction of  $ERM(F)$  shows that it is a subset of the class  $PPM(F)$ . While the dimension of the manifolds of the universal object is a lower bound on the dimensions of message spaces of encoded revelation mechanisms, it is not a lower bound on the dimension of message spaces of mechanisms in  $PPM(F)$ . Examples are given in Section 3 that show this. Theorems due to Hurwicz, Chen and Abelson, already mentioned, do establish lower bounds on the dimension of message spaces of mechanisms in  $PPM(F)$ . While those theorems use rank conditions on certain Hessian matrices of  $F$ , they do not yield the same bounds as those given by the universal object. In general the bounds on the dimension of message spaces are lower than the bound on computational complexity. The relationships among these results are explored in Section 3.

**Section 1. Initial set theoretic constructions**

*Notation.* If  $x_j, 1 \leq j \leq n$ , are sets, then  $X_{\langle -j \rangle}$  denotes the set

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

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

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

**F-Equivalence**

**Definition 1.1.** Suppose that  $X_i, 1 \leq i \leq n$ , and  $Y$  are sets, suppose that  $F: \prod_{i=1}^n X_i \rightarrow Y$  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  $z \in X_{\langle -j \rangle}$ ,  $F(x \int_j z) = F(x' \int_j z)$ .

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  $(X_1/F) \times \dots \times (X_n/F)$  is the smallest product set through which  $F$  factors.

**Lemma 1.1.** *Suppose that  $X_1, \dots, X_n$ , and  $Y$  are sets and suppose that  $F: X_1 \times \dots \times X_n \rightarrow Y$  is a function. There is a unique function  $F^*: (X_1/F) \times \dots \times (X_n/F) \rightarrow Y$  that makes the Diagram 1.1 commute. Furthermore, if  $Z_1, \dots, Z_n$  are sets, and if there are functions  $g_i: X_i \rightarrow Z_i, 1 \leq i \leq n$ , and a function  $G: Z_1 \times \dots \times Z_n \rightarrow Y$*

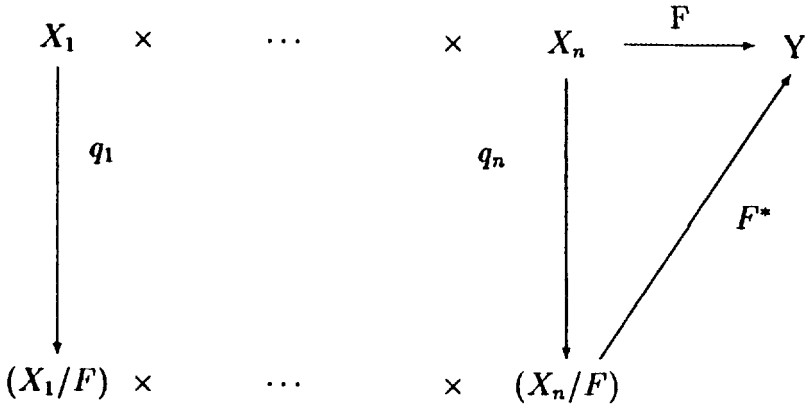


Diagram 1.1.

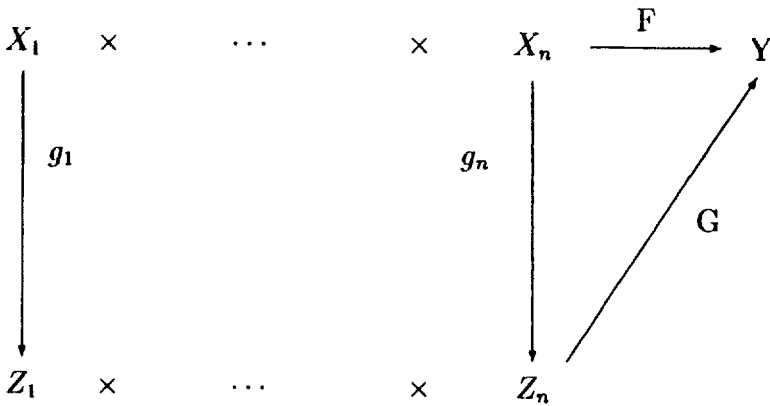


Diagram 1.2.

that makes Diagram 1.2 commute, then there are uniquely determined maps  $g_1^*, \dots, g_n^*, g_i^*: Z_i \rightarrow (X_i/F)$ , that make Diagram 1.3 commute.

Proof of Lemma 1.1.

We first show that if  $g_i: X_i \rightarrow Z_i$  and  $G: \prod_1^n Z_i \rightarrow Y$  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  $w \in X_{\langle -i \rangle}$ , set

$$g(w) = (g_1(w_1), \dots, g_{i-1}(w_{i-1}), g_{i+1}(w_{i+1}), \dots, g_n(w_n)) \in Z_{\langle -i \rangle}.$$

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.

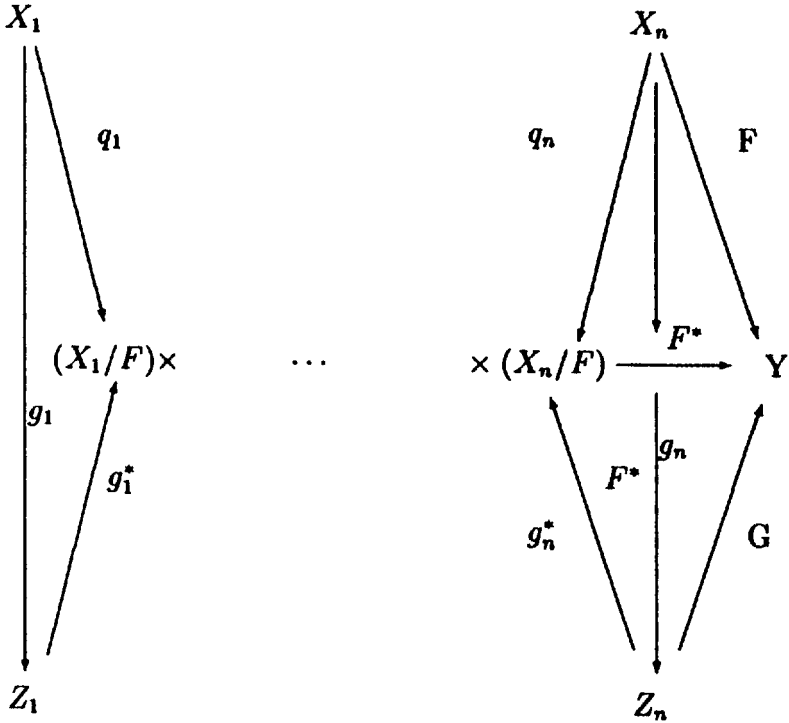


Diagram 1.3.

To see the uniqueness of the maps  $g_i^*$ , note that if  $h_i^*: Z_i \rightarrow (X_i/F)$ ,  $1 \leq i \leq n$ , 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

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

**Encoded and essential revelation mechanisms**

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

- (i) a product of sets  $M_1 \times \dots \times M_n$ ,
- (ii) a collection of functions  $g_i: X_i \rightarrow M_i, 1 \leq i \leq n$ ,
- (iii) a function  $h: M_1 \times \dots \times M_n \rightarrow Z$ , such that for each

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

Using the notation of Lemma 1.1, the triple

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

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

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

### Universality of the essential revelation mechanism

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

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

(i) *The triple*

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

*is an encoded revelation mechanism that realizes  $F$ ;*

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

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

(iv) *Finally, the essential revelation mechanism is the unique encoded revelation mechanism (to within isomorphism) through which all encoded 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  $\Phi: X \rightarrow Y$  be a differentiable mapping. If at a point  $p \in X$  the mapping  $\Phi$  has maximum rank, and if  $\dim X \geq \dim Y$ , then  $\Phi$  is said to be a *submersion* at  $p$ . If  $\Phi$  is a submersion at each point of  $X$ , then  $\Phi$  is a submersion. If a map  $g: X \rightarrow Y$  is a submersion, then it is known (cf. [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  $x_1, \dots, x_n$  at  $p$  in a neighborhood  $U$  of  $p$ , and coordinates  $y_1, \dots, y_m$ , in a neighborhood of  $g(p)$  so that for each  $q \in U$ ,  $g(q) = (x_1(q), \dots, x_m(q))$ .

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

Suppose  $E^1, \dots, E^n$ , are Euclidean spaces of dimensions  $d_1, \dots, d_n$ , such that the space  $E^i$ ,  $1 \leq i \leq n$  has coordinates  $x_i = (x_{i,1}, \dots, x_{i,d_i})$ . Assume that  $(p_1, \dots, p_n)$  is a point of  $E^1 \times \dots \times E^n$ , and assume that  $U_i$  is an open neighborhood of the point  $p_i$ ,  $1 \leq i \leq n$ . We assume that  $F$  is a real valued  $C^2$ -function defined on  $U_1 \times \dots \times U_n$ . We require four matrices.

(I): The matrix

$$BH(F; x_{i,1}, \dots, x_{i,d(i)}; x_{1,1}, \dots, x_{i-1,d_{i-1}}, x_{i+1,1}, \dots, x_{n,d_n}) \\ = BH(F; x_{\bar{i}}; x_{\langle -i \rangle})$$

is a matrix that has rows indexed by  $x_{i,1}, \dots, x_{i,d_i}$  and columns indexed by  $F, x_{1,1}, \dots, x_{(i-1),d_{i-1}}, x_{(i+1),1}, \dots, x_{n,d_n}$ . The entry in the  $x_{i,u}$  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  $\partial^2 F / \partial x_{i,u} \partial x_{j,w}$ .

(II): The matrix  $H(F; x_{\bar{i}}; x_{\langle -i \rangle})$  is the submatrix of  $BH(F; x_{\bar{i}}; x_{\langle -i \rangle})$  that consists of the columns indexed by  $x_{u,v}$ ,  $u \in \{1, \dots, i-1, i+1, \dots, n\}$  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  $F: E^1 \times E^2 \rightarrow R$ , we use a slightly less cumbersome notation. Suppose that  $E^1$  has coordinates  $(x_1, \dots, x_p)$  and  $E^2$  has coordinates  $(y_1, \dots, y_q)$ . We use as row indices for  $BH(F; x_1, \dots, x_p; y_1, \dots, y_q)$  the variables  $x_1, \dots, x_p$  and as column indices  $F, y_1, \dots, y_q$ . The  $(x_i, F)$  entry in  $BH(F; x_1, \dots, x_p; y_1, \dots, y_q)$  is  $\partial F / \partial x_i$  and the  $(x_i, y_j)$  entry is  $\partial^2 F / \partial x_i \partial y_j$ .

The matrices  $H(F; x_{\bar{i}}; x_{\langle -i \rangle})$  and  $BH(F; x_{\bar{i}}; x_{\langle -i \rangle})$  are matrices of functions in the coordinates  $x_1, \dots, x_n$  of  $E^1 \times \dots \times E^n$ . The conditions we place on the matrices  $BH$  and  $H$  require ahtat 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  $BH^*(F; x_{\bar{i}}; x_{\langle -i \rangle})[x_{\bar{i}}, p_{\langle -i \rangle}]$  is the matrix that results from evaluating the variables  $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n$  of the entries of  $BH(F; x_{\bar{i}}; x_{\langle -i \rangle})$  at the point  $p_{\langle -i \rangle} = (p_1, \dots, p_{i-1}, p_{i+1}, \dots, p_n)$ . The matrix  $BH^*(F; x_{\bar{i}}; x_{\langle -i \rangle})[x_{\bar{i}}, p_{\langle -i \rangle}]$  is a function of the variables  $x_{i,1}, \dots, x_{i,d_i}$  alone.

Similarly, the matrix

$$H^*(F; x_{\bar{i}}; x_{\langle -i \rangle})[x_{\bar{i}}, p_{\langle -i \rangle}]$$

is the submatrix of

$$BH^*(F; x_{\bar{i}}; x_{\langle -i \rangle})[x_{\bar{i}}, p_{\langle -i \rangle}]$$

derived by deleting the column indexed by  $F$ .

**Differential separability**

**Definition 2.2.** Suppose  $X_1, \dots, X_n$  are differentiable manifolds, where for each  $1 \leq i \leq n$ ,  $X_i$  has dimension  $d_i$ . Suppose that  $p_i \in X_i$ ,  $1 \leq i \leq n$ , and suppose for each  $i$ ,  $\phi_{i,1}, \dots, \phi_{i,d_i}$  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  $1 \leq i \leq n$ ,  $\phi_i = \prod_j \phi_{i,j}$  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  $\phi_i$  carries  $p_i$  to  $0_i$ . We assume that  $E^i$  has coordinates  $x_{i,1}, \dots, x_{i,d_i}$ . The function  $F$  is said to be *differentially separable of rank  $(r_1, \dots, r_n)$  at the point  $(p_1, \dots, p_n)$  in the coordinate system  $\phi_{1,1}, \dots, \phi_{n,d_n}$*  if for each  $1 \leq i \leq n$ , the matrices

$$BH(F \circ (\prod \phi_i)^{-1}; x_{i,1}, \dots, x_{i,d_i}; x_{\langle -i \rangle})$$

and

$$H^*(F \circ (\prod \phi_i)^{-1}; x_{i,1}, \dots, x_{i,d_i}; x_{\langle -i \rangle}) [x_i, 0_{\langle -i \rangle}]$$

have rank  $r_i$  in a neighborhood of  $(0_1, \dots, 0_n)$ . If  $F$  is differentially separable of rank  $(r_1, \dots, r_n)$  at  $(p_1, \dots, p_n)$ , and if  $r_i = \dim(X_i)$  for each  $1 \leq i \leq n$ , then we will say that  $F$  is *differentially separable at  $(p_1, \dots, p_n)$* .

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  $(q_1, \dots, q_n) \in \prod_{i=1}^n Y_i$  and let  $h_i(q_i) = (p_i)$ . If  $F$  is differentially separable of rank  $(r_1, \dots, r_n)$  at  $(p_1, \dots, p_n)$ , then  $g$  is differentially separable of rank  $(r_1, \dots, r_n)$  at  $(q_1, \dots, q_n)$ .*

We can now define the term differentially 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  $F: X_1 \times \dots \times X_n \rightarrow R$  is differentially separable of rank  $(r_1, \dots, r_n)$  at the point  $(p_1, \dots, p_n)$  if there is a coordinate system  $\{\phi_{i,j}\}$  at the point  $(p_1, \dots, p_n)$  such that  $F$  is differentially separable of rank  $(r_1, \dots, r_n)$  at the point  $(p_1, \dots, p_n)$  in the coordinate system  $\phi_{1,1}, \dots, \phi_{n,d_n}$ .

**The number of variables on which  $F$  really depends**

If  $F: X_1 \times \dots \times X_n \rightarrow R$  is differentially separable of rank  $(r_1, \dots, r_n)$  at a point  $(p_1, \dots, p_n)$ , then it is possible to write  $F$  as a function of variables  $\{y_{1,1}, \dots, y_{1,r_1}, \dots, y_{n,1}, \dots, y_{n,r_n}\}$ . 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)  $F: X_1 \times \dots \times X_n \rightarrow R$  is a  $C^{k+1}$ -function,
- (ii)  $(p_1, \dots, p_n)$  is a point on  $X_1 \times \dots \times X_n$ ,
- (iii)  $X_i$  has coordinates  $x_i$ .

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

$$G(y_{1,1}, \dots, y_{1,r(1)}, \dots, y_{n,1}, \dots, y_{n,r(n)}),$$

where  $(y_{i,1}, \dots, y_{i,d_i})$  is a coordinate system on  $X_i$ , is that the matrix

$$BH(G; \mathfrak{X}_i; \mathfrak{X}_{\langle -i \rangle})$$

has rank at most  $r_i$  for each  $i$ . Furthermore, a sufficient condition for  $F$  to be written in the form  $G(y_{1,1}, \dots, y_{1,r(1)}, \dots, y_{n,1}, \dots, y_{n,r(n)})$ , for a  $C^k$ -function  $G$  in a neighborhood of a point  $(p_1, \dots, p_n)$ , is that  $F$  is differentially separable of rank exactly  $(r_1, \dots, r_n)$  at  $(p_1, \dots, p_n)$ .

**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  $F: X_1 \times \dots \times X_n \rightarrow Z$  is a differentiable function. The triple  $(g_1, \dots, g_n, M_1 \times \dots \times M_n, h)$  that consists of spaces  $M_1 \times \dots \times M_n$ , maps  $g_1, \dots, g_n, g_i: X_i \rightarrow M_i, 1 \leq i \leq n$ , and function  $h: M_1 \times \dots \times M_n \rightarrow Z$  is an encoded  $C^k$ -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  $F: X_1 \times \dots \times X_n \rightarrow Z$  is a differentiable map from a product of differentiable manifolds  $X_1, \dots, X_n$  to a differentiable manifold  $Y$ . The function  $F$  factors through a product of manifolds  $Z_1 \times \dots \times Z_n$  if there are submersions  $g_i: X_i \rightarrow Z_i$ , and a differentiable mapping  $h: Z_1 \times \dots \times Z_n \rightarrow Y$  such that the diagram in Diagram 2.1 commutes.

It has not been established that the essential revelation mechanism is an encoded  $C^k$ -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  $BH(F; \mathfrak{X}_i; \mathfrak{X}_{\langle -i \rangle})$  is the same as the dimension of  $X_i$ , then for each two points  $x$  and  $x'$  in  $X_i$ , there is an element  $y \in \mathfrak{X}_{\langle -i \rangle}$  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  $BH(F; \mathfrak{X}_i; \mathfrak{X}_{\langle -i \rangle})$  at a point is  $r_i$ , then in a neighborhood of the point there is a coordinate system  $\{x_{i,1}, \dots, x_{i,d_i}\}$  and a function  $G$  such that  $F(x_{1,1}, \dots, x_{n,d_n}) = G((x_{i,1}, \dots, x_{i,r_i}) \int_i \mathfrak{X}_{\langle -i \rangle})$ . We can use the remaining set of

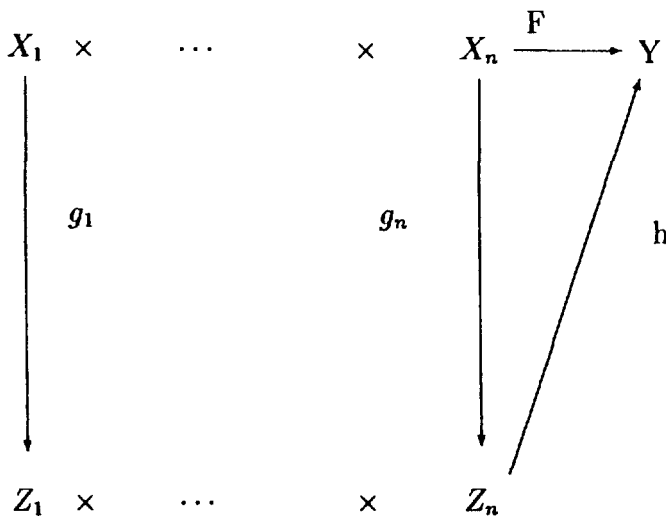


Diagram 2.1.

coordinates in  $X_i$  to determine a subspace  $S$  of  $X_i$  by setting  $x_{i,(r+1)} = 0, \dots, x_{i,d_i} = 0$ . The set  $S$  is a submanifold of  $X_i$  and the restriction of  $F$  to the space  $S \times X_{\langle -i \rangle}$  has the property that  $BH(\text{restrict}(F): x_{i,1}, \dots, x_{i,r}; X_{\langle -i \rangle})$  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  $X_1 \times \dots \times X_n$ .

**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 differentially separable at each point  $(p_1, \dots, p_n) \in U_1 \times \dots \times U_n$ . 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  $w \in U_{\langle -i \rangle}$  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  $X_{\langle -i \rangle} = Y$ , set  $\dim(X_{\langle -i \rangle}) = N$ , 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  $F(z_1, \dots, z_m, w_1, \dots, w_N)$  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  $(z_1, \dots, z_m, w_1, \dots, w_N)$  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  $w \in V'$ ,  $|F(z, w) - F(z', w)| = |u \circ (z - z') + w \circ (z - z') + z^T Q z' + P(z^*, w^*)[z', w] - P(z^*, w^*)[z, w]|$ .

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  $u \circ v = L$ , 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  $\sum_{\alpha, \beta} a_{\alpha, \beta} z^\alpha w^\beta$  in the variables  $w_1, \dots, w_N$  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  $z_1, \dots, z_m$  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.  $\square$

We now give conditions on a function  $F$  that is differentially separable of rank  $(r_1, \dots, r_n)$ , 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  $F: X_1 \times \dots \times X_n \rightarrow R$  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  $q \in X_{\langle -i \rangle}$ , 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  $z \in X_{\langle -i \rangle}$ .

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

$$F(x_1, \dots, x_n) = \sum_{\beta(1), \dots, \beta(n)} A_{\beta(1) \dots \beta(n)} x_1^{\beta(1)} \dots x_n^{\beta(n)},$$

where  $A_\beta(x_1)$  are polynomials in  $x_1$ . Then for  $x_1, x'_1 \in X_1, F(x_1, x_{\langle -1 \rangle}) = F(x'_1, x_{\langle -1 \rangle})$  for  $x_{\langle -1 \rangle}$  in an open set in  $X_{\langle -1 \rangle}$ , if and only if  $[A_\beta(x_1) - A_\beta(x'_1)] x_2^{\beta(2)} \dots x_n^{\beta(n)} = 0$  for the  $x_2, \dots, x_n$  chosen arbitrarily in an open set in  $X_2 \times \dots \times X_n$ . However, a polynomial vanishes in an open set if and only if each of its coefficients is zero. Therefore if  $F(x_1, x_{\langle -1 \rangle}) = F(x'_1, x_{\langle -1 \rangle})$  for the  $x_{\langle -1 \rangle}$  chosen in some open set, it follows that for each  $\beta, A_\beta(x_1) - A_\beta(x'_1) = 0$ . That is,  $F$  induces a strong equivalence relation on  $X_1$ .  $\square$

**Theorem 2.3.** Suppose that  $X_i, 1 \leq i \leq n$  are  $C^4$ -manifolds of dimensions  $d_1, \dots, d_n$ , respectively. Suppose  $F: X_1 \times \dots \times X_n \rightarrow R$  is a  $C^4$ -function that is differentially

separable on  $X_1 \times \dots \times X_n$  of rank  $(r_1, \dots, r_n)$  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  $q_i: X_i \rightarrow (X_i/F)$  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  $q_i: X_i \rightarrow (X_i/F)$  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 differentially separable of rank  $(r_1, \dots, r_n)$  at the point  $(p_1, \dots, p_n)$ , 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  $x_i = (x_{i,1}, \dots, x_{i,d_i})$  in  $X_i$  such that  $x_i(p_i) = (0, \dots, 0)$  and a  $C^3$ -function  $G$  defined in a neighborhood of the origin, such that

$$F(x_1, \dots, x_n) = G\left( (x_{i,1}, \dots, x_{i,r_i}) \int_i z \right)$$

for each  $z \in U_{<i>}$ . Denote by  $S_i^*$  the set of elements  $\{x_{i,1}, \dots, x_{i,r_i}, 0, \dots, 0\}$  that lie in  $U_i$ . Choose in  $S_i^*$  a compact neighborhood  $S_i$  of  $(0, \dots, 0)$  (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

$$F\left( x_{i,1}, \dots, x_{i,r_i}, b_1, \dots, b_{d_i-r_i}, \int_i z_{<i>} \right) = F\left( (x_{i,1}, \dots, x_{i,r_i}, 0, \dots, 0) \int_i z_{<i>} \right)$$

implies that  $q_i(x_{i,1}, \dots, x_{i,d_i}) = q_i(x_{i,1}, \dots, x_{i,r_i})$  for each  $(x_{i,1}, \dots, x_{i,d_i})$  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  $q_i$  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  $R^n$ . Furthermore, the function  $s_i$  is a thread of  $q_i$  on the set  $N_i$ .  $\square$

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  $C^0$ -encoded 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  $F: X_1 \times \dots \times X_n \rightarrow R$  is a real valued function on  $F$  that satisfies the following conditions:

- (i) there are integers  $(r_1, \dots, r_n)$ ,  $1 \leq r_i \leq d_i$ , such that at each point  $(p_1, \dots, p_n) \in X_1 \times \dots \times X_n$ ,  $F$  is differentially separable of rank  $(r_1, \dots, r_n)$ ,
- (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

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

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

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

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

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

is such that  $g_i: X_i \rightarrow Z_i$ ,  $G: Z_1 \times \dots \times Z_n \rightarrow R$ , and the triple is an encoded 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

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

is an encoded revelation mechanism that realizes  $F$ . Suppose that  $z_i^* \in Z_i$ . Denote  $(g_1(w), \dots, g_{i-1}(w), g_{i+1}(w), \dots, g_n(w))$  by  $g_{\langle -i \rangle}(w)$ , for each  $w \in X_{\langle -i \rangle}$ . 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

$$w \in X_{\langle -i \rangle}, \quad F\left(x_i^* \int_i w\right) = G\left(g_i(x_i^*) \int_i g_{\langle -i \rangle}(w)\right) = G\left(g_i(x'_i) \int_i g_{\langle -i \rangle}(w)\right) = F\left(x'_i \int_i w\right).$$

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  $z^* \in N$ . 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.  $\square$

### Section 3. The results of Abelson, Chen and Hurwicz

In [5] (p. 291), Hurwicz addressed the question of realizing a function 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  $M$  of dimension 2 with coordinates  $m^1$ , and  $m^2$ , if the realization uses messages correspondences  $g^i(a_1, a_2, m^1, m^2)$  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 Fully 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  $\Theta$ . Then there exist smooth functions  $G^1$  and  $G^2$  such that  $F$  is realized by  $(g^1, g^2, h, M)$  with*

$$\begin{aligned} g^1(m, a) &\equiv m_2 - G^1(m_1, a), & a \in \Theta^1, \\ g^2(m, b) &\equiv m_2 - G^2(m_1, b), & b \in \Theta^2, \end{aligned}$$

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  $R^{k_1} \times R^{k_2} \rightarrow \mathcal{R}$ . Chen uses the notation  $BH(P)$  for the Full Bordered Hessian of  $P$ . Chen’s theorem states:

**Theorem (Chen).** *Let  $P: R^{k_1} \times R^{k_2} \rightarrow R$  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<sup>4</sup> with privacy-preserving mechanism with a message space of dimension  $n$ , then  $\text{rank } BH(P) \leq n$  in  $U$  (where  $BH(P)$  is Chen’s notation for the Full Bordered Hessian).*

This condition on the Full Bordered Hessian can be restated as the condition that all  $(n + 1) \times (n + 1)$  submatrices of  $FBH(F)$  have determinant zero. Chen further showed if one uses the differential ideal constructions of [7], and if one replaces the formation of determinants by wedge products, then one can generalize the Hurwicz necessary condition to find necessary conditions that a goal function  $F: R^{k_1} \times \dots \times R^{k_l} \rightarrow R^m$ , can be realized by a privacy preserving mechanism that uses a message space of dimension  $n$ .

The Bordered Hessian is used by Hurwicz and Chen and 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 used are best indicated by considering examples. The first example we consider is one due to Hurwicz and 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 realize the goal function  $F(x, z, x', z') = (z - z')/(x - x')$ . The Hurwicz result, and Chen’s generalization, state 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 when  $F$  has nonvanishing first partials, then there is a mechanism that realizes  $F$  if the Full Bordered Hessian has determinant zero. Indeed, if they use a message space of dimension 2 with 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

<sup>4</sup> If a mechanism has equilibrium message given by equations  $g_i(x_i, \mathbf{m}) = 0$  for agent  $i$  then Chen defines the mechanism to be efficient if the Jacobians  $\nabla_{x_i} g_i$  are all of maximal rank

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  $x, z, x', z'$ . To compute the intersection one must have at least implicitly computed the 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

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

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

$$\begin{pmatrix} 2 & 2x_1 & \dots & kx_1^{k-1} & y_1 + \sum_{i=1}^k iy_i x_1^{i-1} \\ 2y_1 & 0 & \dots & 0 & y_1^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ ky_1^{k-1} & 0 & \dots & 0 & y_1^k \\ x_1 + \sum_{i=1}^k ix_i y_1^{i-1} & x_1^2 & \dots & x_1^k & 0 \end{pmatrix}.$$

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  $\Phi$ . Chen also offers a mechanism that realizes  $\Phi$  with a four dimensional message space. If the message space has coordinates  $m_1, \dots, m_4$ , then the messages  $m_1 = x_1$ ,  $m_2 = y_1$ ,  $m_3 = \sum_{i=1}^k x_i m_2^i$ , and  $m_4 = \sum_{i=1}^k y_i m_1^i$ , together with the outcome function  $h(m_1, \dots, m_4) = m_3 + m_4$  realizes  $\Phi$ .

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  $\Phi: X \times Y \rightarrow \mathcal{R}(\text{Reals})$  is a  $C^2$ -function, let  $p \in X \times Y$ , and let  $R$  be the rank of the matrix of second-order partials derivatives  $\Delta_{i,j} = \partial^2 \phi / \partial x_i \partial y_j$  at  $p$  [the Hessian  $H(\Phi)$  at  $p$ ]. Then any multistage distributed computation which computes  $\Phi$  in a neighborhood of  $p$  must have total information transfer at least  $R$  between  $PX$  and  $PY$  (assuming that the functions computed at each stage are all  $C^2$ .)*

In the case of the function  $\Phi$ , the Hessian used by Abelson has rank 2, thus a distributed computation of  $\Phi$  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  $\Phi$ , and send it to  $P_1$ , who has computed the second term of  $\Phi$ , knowing  $y_1$ , and then can calculate the sum.

On the other hand, it is still not possible to eliminate any of the  $2N$  variables  $X, Y$  in the computation of  $\Phi$ . 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  $H$ .

## Appendix A

### Leontief and Abelson theorem

Suppose that  $F(x_1, \dots, x_N)$  is a function of  $N$  variables which has continuous partial derivatives to order  $d$ . For each sequence  $\alpha = (\alpha(1), \dots, \alpha(N))$  of nonnegative integers, denote by  $|\alpha|$  the sum  $\alpha(1) + \dots + \alpha(N)$ . We denote by  $D(x_1^{\alpha(1)} \dots x_N^{\alpha(N)}; F)$  the derivative  $\partial^{|\alpha|} F / \partial x_1^{\alpha(1)} \dots \partial x_N^{\alpha(N)}$ . 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  $x = (x_1, \dots, x_m)$  and  $y = (y_1, \dots, y_n)$  are sets of real variables and suppose  $F(x, y)$  and  $G(x)$  are real valued  $C^1$ -functions defined on a neighborhood  $U$  of the point  $(p, q) = (p_1, \dots, p_m, q_1, \dots, q_n)$  that satisfy the following conditions.*

$$(i) \quad \begin{pmatrix} D(x_1; F) \cdots D(x_m; F) \\ D(x_1; G) \cdots D(x_m; G) \end{pmatrix}$$

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

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

Then

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

for  $j > 1$ . Because

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

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  $\Omega$  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  $x_2, \dots, x_m$  and we can write  $C(w, x_2, \dots, x_m, y) = C(w, y)$ . Then

$$C(G(x_1, \dots, x_m), y) = F(c(G(x_1, \dots, x_m), x_2, \dots, x_m), x_2, \dots, x_m, y) = F(x_1, \dots, x_m, y). \quad \square$$

**Leontief's theorem**

Leontief proved the following result in [11].

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

- (i) for each  $1 \leq i, j \leq m$  and each  $1 \leq k \leq n$ ,  $(\partial/\partial y_k)[F_i/F_j] = 0$ ,
- (ii) for some  $j$ ,  $F_j(x_1, \dots, x_m)(p, q) \neq 0$ .

**Proof.** Form the matrix

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

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

**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 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,  $\Omega(F_1, \dots, F_m)^t = (D(x_1 y_k; F), \dots, D(x_m y_k; F))^t$  ( $M^t$  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  $k$ .  $\square$

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

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

A necessary condition that there are 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, 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  $BH(F; x; y)$  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

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

Therefore

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

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

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

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,

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

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  $j$ .  $\square$

**Corollary A.2.3.** Suppose that  $x_{i,j}$ ,  $1 \leq i \leq r$ ,  $1 \leq j \leq d_i$  are  $r$  ordered sets of variables. Denote by  $x_i$  the set of variables  $(x_{i,1}, \dots, x_{i,d_i})$ . 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 encoded revelation mechanisms require a slightly altered version of Leontief's Theorem. This version is closely related to a result announced by Abelson (cf. [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

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

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

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

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

**Proof.** Because

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

it follows that

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

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

The next theorem shows that for a product of Euclidean spaces, if  $F$  is a differentially separable function of ranks  $(r_1, \dots, r^n)$ , 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

$F_1, \dots, F_N$  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  $x_1, \dots, x_m$  and that  $Y$  has coordinates  $y_1, \dots, y_n$ . Assume that  $p \in X, q \in Y$ , that  $U$  is a neighborhood of  $p, V$  is a neighborhood of  $q$ , and that  $F_i, 1 \leq i \leq N$ , is a  $C^{k+1}$ -function,  $k \geq 2$ , 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,  $k \geq 2$ ,*

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

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

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

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

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

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

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

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  $BH(F; x; y) =$

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

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

$$(x_1, x_2, x_3; y_1, y_2, y_3, y_4) = (0, 0, 0; 1, 1, 1) = (p, q), BH^*(F; x; y)[x, q] = \begin{pmatrix} 3 & 2 & 0 & 1 & 1 \\ 1 + 6x_2 & -1 + 4x_2 & 1 & 1 + 2x_2 & -1 + 2x_2 \\ 2x_3 & -2x_3 & 2x_3 & 2x_3 & -2x_3 \end{pmatrix}.$$

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  $x_1, \dots, x_3$ , and a function  $C$  of two variables such that  $F = C(A, B)$ . To construct  $A$  and  $B$ , we first compute the derivatives  $D(y_i; F)$ ,  $1 \leq i \leq 4$ . 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  $2 \times 2$  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  $G(w_1, w_2; y_1, \dots, y_4)$  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

$$G(A_1, A_2; y_1, y_2, y_3, y_4, y_4) = F.$$

**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

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

has rank  $r$  in the set  $U$ , there is neighborhood  $U''$  of  $p$  and an  $(r \times r)$ -submatrix of

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

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

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

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

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

Because

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

the matrix with  $(i, j)$  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

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

that are defined on  $U^*$  such that

$$z_i = A_i(h_1, \dots, h_r, x_{r+1}, \dots, x_m), \quad E.1$$

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

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

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

$$\begin{aligned} G_i(w_1, \dots, w_r, x_{r+1}, \dots, x_m, y_1, \dots, y_n) \\ = F_i(h_1(w_1, \dots, w_r, x_{r+1}, \dots, x_m), \dots, h_r(w_1, \dots, w_r, x_{r+1}, \dots, x_m), y_1, \dots, y_q), \end{aligned}$$

$1 \leq i \leq N$ . Because

$$\begin{aligned} G_i(A_1, \dots, A_r, x_{r+1}, \dots, x_m, y_1, \dots, y_n) \\ = F_i(h_1(A_1, \dots, A_r, x_{r+1}, \dots, x_m), \dots, h_r(A_1, \dots, A_r, x_{r+1}, \dots, x_m), x_{r+1}, \\ \dots, x_m, y_1, \dots, y_n) = F_i(x_1, \dots, x_m, y_1, \dots, y_n), \end{aligned}$$

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  $x_{r+1}, \dots, x_m$ . The hypothesis of (ii) asserts that the column vector

$$(D(x_1; F_1), \dots, D(x_m; F_m))^T$$

is a linear combination of the columns of the matrix

$$H^*(F_1, \dots, F_m; x_1, \dots, x_m; y_1, \dots, y_n)[x, q]$$

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  $(D(x_1; F_1), \dots, D(x_m; F_m))^T$  is a linear combination of columns indexed by  $(F_{\alpha(1)}, y_{\beta(1)}), \dots, (F_{\alpha(r)}, y_{\beta(r)})$  in the neighborhood  $U^* \times V$ . It follows, that for each  $1 \leq i \leq N$ , and  $1 \leq t \leq m$ ,

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

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

$$0 = \sum_{t=1}^r D(x_i; A_t) D(x_j; h_t) + D(x_j; F_i).$$

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

$$\begin{aligned} D(x_j; G_i) &= \sum_{t=1}^r D(x_i; F_t) D(x_j; h_t) + D(x_j; F_i) \\ &= \sum_{t=1}^r \left[ \sum_{s=1}^r C_{is} D(x_i; A_s) \right] D(x_j; h_t) + \sum_{s=1}^r C_{is} D(x_j; A_s) \\ &= \sum_{s=1}^r \left[ \sum_{t=1}^r D(x_i; A_s) D(x_j; h_t) + D(x_j; A_s) \right] C_{is} = 0. \quad \square \end{aligned}$$

### References

1. Abelson, H.: Lower bounds on information transfer in distributed computations JACM 27, 384–392 (1980)
2. Arbib, M. A. Theories of abstract automata Englewood Cliff. New Jersey: Prentice Hall, Inc. 1969
3. Chen, P.: A lower bound for the dimension of the message space of the decentralized mechanisms realizing a given goal. J. Math. Econ 21, 249–270 (1992)
4. Golubitsky, M., Guillemin, V.: Stable mappings and their singularities. In: Graduate texts in mathematics No. 14. New York: Springer 1973
5. Hurwicz, L.: On informational decentralization and efficiency in resource allocation mechanisms. In: Reiter, S. (ed.) Studies in mathematical economics, Vol. 25. The Mathematical Association of America, 1986
6. Hurwicz, L.: On informationally decentralized systems. In: McGuire, B., Radner, R. (eds.) Decisions and organizations. Amsterdam: North Holland 1972
7. Hurwicz, L., Reiter, S., Saari, D.: On constructing an informationally decentralized process implementing a given performance function. Mimeo, presented and distributed at the Econometric Society World Congress, Aix-en-Provence, 1980

8. Jordan, J. S.: The competitive allocation process is informationally efficient uniquely. *J. Econ. Theory* **28**, 1–18 (1982)
9. Jordan, J. S.: The informational requirements of local stability in decentralized allocation mechanisms. In: Groves, T., Radner, R., Reiter, S. (eds.) *Information, incentives and economic mechanisms*. Minneapolis: University of Minnesota Press 1987
10. Kalai, E., Stanford, W.: Finite rationality and interpersonal complexity in repeated games. *Econometrica* **56**, 397–410 (1988)
11. Leontief, W.: A note on the interrelation of subsets of independent variables of a continuous function with continuous first derivatives. *Bull. AMS* **53**, 343–350 (1947)
12. Mac Lane, S.: *Categories for the working mathematician*. Graduate texts in mathematics No. 5. New York: Springer Verlag 1971
13. Mount, K. R., Reiter, S.: The informational size of message spaces. *J. Math. Econ.* **8**, 161–192 (1974)
14. Mount, K. R., Reiter, S.: *Computation, communication, and performance in resource allocation*. Presented at the CEME-NBER Decentralization Seminar, University of Minnesota, May 21–23, 1982. Mimeo, Northwestern University, 1983
15. Mount, K. R., Reiter, S.: On the existence of a locally stable dynamic process with a statically minimal message space. In: Groves, T., Radner, R., Reiter, S. (eds.) *Information, incentives and economic mechanisms*. Minneapolis: University of Minnesota Press 1983
16. Mount, K. R., Reiter, S.: *A model of computing with human agents*. Discussion Paper No. 890; The Center for Mathematical Studies in Economics and Managerial Science, Northwestern University, 1990
17. Neyman, A.: Bounded complexity justifies cooperation in the finitely repeated prisoners dilemma. *Econ. Lett.* **19**, 227–229 (1985)
18. Reichelstein, S.: *On the informational requirements for the implementation of social choice rules*. Handout for the Decentralization Conference, Minneapolis, May 1982
19. Reichelstein, S.: Incentive compatibility and informational requirements. *J. Econ. Theory* **32**, 384–390 (1984)
20. Reichelstein, S., Reiter, S.: Game forms with minimal message spaces. *Econometrica* **56**, 661–692 (1988)
21. Reiter, S.: *Information incentive and performance in the new welfare economics*. Papers and Proceedings of the Eighty-Ninth Annual Meeting of the American Economic Association. *Am. Econ. Rev.* **67**, 219–237 (1977). Reprinted in *Mathematical Economics*. Mathematical Association of America, 1987.
22. Reiter, S.: There is no adjustment process with two-dimensional message spaces for counter examples. Summarized in [5]
23. Reiter, S.: *A decentralized process for finding equilibria given by linear equations*. Mimeo, Northwestern University, 1994
24. Reiter, S., Simon, C. P.: Decentralized dynamic processes for finding equilibrium. *J. Econ. Theory*, **56**, 83–96 (1992)
25. Rubenstein, A.: Finite automata play the repeated prisoner's dilemma. *J. Econ. Theory* **39**, 83–96 (1986)
26. Saari, D., Simon, C. P.: *Effective price mechanisms*. *Econometrica* **46**, 1097–1125 (1978)
27. Serre, J. P.: *Lie algebras and Lie groups*. New York: W. A. Benjamin, Inc. 1965
28. Sonnenschein, H.: An axiomatic characterization of the price mechanism. *Econometrica* **42**, 425–460 (1974)
29. Widder, D. V.: *Advanced calculus*. New York: Prentice Hall 1963
30. Williams, S.: Necessary and sufficient conditions for the existence of a locally stable message process. *J. Econ. Theory* **35**, 127–154 (1988)

Copyright of Economic Theory is the property of Springer - Verlag New York, Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.