Because m is privacy preserving

$$m=\cap_a(L_a \times X_{C(a)})$$

where

$$L_a=m_{a \times M}.$$

As before, $m_{a \times M}$ is the projection of m into the set $X_a \times M$. If $t \in M$, then

$$m^{-1}(t)=\prod_{a \in A} L_a^{-1}(t).$$

Indeed, if $t \in M$ and if x is an element of $m^{-1}(t)$, then

$$t \in m(x)=\cap_a L_a(x_a).$$

Therefore

$$t \in L_a(x_a)$$

and thus

$$x_a \in L_a^{-1}(t).$$

We have shown that x is an element of $\prod_{a \in A} L_a^{-1}(t)$. More interesting is the assertion that the rectangle

$\prod_{a \in A} L_a^{-1}(t)$, is contained in $m^{-1}(t)$.

Suppose that

$$x \in \prod_{a \in A} L_a^{-1}(t).$$

The element

$$(x_a,t) \in L_a$$

for each a. Thus

$$t \in \cap_a L_a(t)$$

and therefore t is in the set $m^{-1}(t)$. We have shown that for each $t \in M$, $m^{-1}(t)$ is a rectangle.

Conversely, suppose that for each $t \in M$, the set $m^{-1}(t)$ is a rectangle. For each $t \in M$ and each $a \in A$

there is a set $U_a(t)$ in X_a such that

$$m^{-1}(t)=\prod_{a \in A} U_a(t).$$

Set

$$K_a=\cup_{t \in M} (U_a(t),t) < X_a \times M.$$

The relation K_a is a correspondence from X_a to M; that is, for each x_a in X_a, $K_a(x_a)$ is nonempty. Because m is a correspondence, if

$$(y,x_a) \in X \text{ for } x_a \in X_a,$$

then there is a t in M, such that

$$((y,x_a),t) \in m$$

and hence $x_a \in U_a(t)$.

If $x \in X$, and if $t \in m(x)$,

then

$$m^{-1}(t)=\prod_{a \in A} U_a(t),$$

therefore

$$(x_a,t) \in U_a(t)$$

or, what is the same thing,

$t \in \cap_a K_a(x_a)$. Thus

$$m(x) \subseteq \cap_a K_a(x_a).$$

If $t \in \cap_a K_a(x_a)$, then $t \in K_a(x_a)$. Therefore

$$x_a \in K_a^{-1}(t)=U_a(t).$$

But then

$$x \in \prod_{a \in A} U_a(t)=m^{-1}(t)$$

so that $t \in m(x)$. This shows that

$$m(x)=\cap_a K_a(x_a)$$

for each x in X. It follows that m is a privacy

preserving correspondence.

In the next section we will attempt an elementary classification of privacy preserving correspondences.

As motivation for the discussion, let us look at an example. Suppose that

$X_1=\{0,1\}$,

$X_2=\{0,1\}$,

$Y_1=\{a,b\}$,

$Y_2=\{a,b\}$,

$M=\{r,s,t\}$

and

$N=\{u,v,w\}$.

Define a correspondence $m:X_1 \times X_2 \rightarrow M$ by setting

m(0,0)=r,

m(1,1)=t,

m(0,1)=r

m(1,0)=s.

Similarly, define

n:Y_1 x Y_2--->N by setting

n(a,a)=u,

n(b,b)=w,

n(a,b)=u

n(b,a)=v.

The correspondences m and n are different because they are defined on different spaces. They are both privacy preserving since it is easy to see that each satisfies the criterion given in Lemma A1.2. It is also clear that the two correspondences differ only in the way the points in the various spaces are labelled. In fact, the correspondence m can be transformed into the correspondence n if 0 is renamed a, 1 is renamed b while we rename r, s, t, u, v, w, respectively. In order to treat these correspondences as equivalent we introduce a concept of isomorphism. The next section is devoted to building such a concept. The approach taken is directly analogous to classical definition of the equivalence of functions. We start by defining the concept of map between privacy preserving

correspondences. This mapping theory is not necessary in order to define the concept of isomorphism, but the slight increase in generality is useful.

Section A2. Mappings.

A function f:X-->Y is equivalent to a function g:Z->W if there are one-to-one onto maps h:X-->Z and k:Y-->W so that the diagram in Figure A2.0 commutes(c.f. [10, p.72]). More generally, a map from a function f to a function g is a pair of functions h and k that make the diagram in Figure A2.0 commute. The same definition is to be used to define a map between correspondences f and g, however one must be careful in defining the commutativity of a diagram when correspondences are used. Because the concept of map is to be used in the discussion of privacy preserving correspondences we give the definition only for that case.

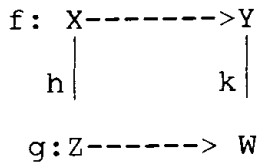

Figure A2.0

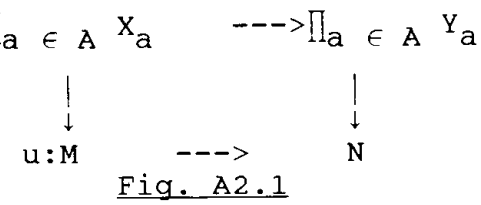

Fig. A2.1

Condition (iii) of Definition A2.1 is the commutativity condition we use. In the case that correspondences are isomorphic, a stronger commutativity condition applies. For this reason Definition A2.1 includes the definition of strict mapping.

Definition A2.1. Suppose that $\{X_a\}$ and $\{Y_a\}$ are two collections of nonempty sets indexed by a set A. Assume that

$$m:\prod_{a \in A} X_a \dashrightarrow M$$

and

$$n:\prod_{a \in A} Y_a \longrightarrow N$$

are privacy preserving correspondences. By a mapping from m to n we shall mean a pair of functions

$$(\prod_{a \in A} u_a, v)$$

such that:

(i) $u_a:X_a \dashrightarrow Y_a$ is a function for each a,

(ii) $v:M \dashrightarrow N$ is a function,

iii) for each $x \in \prod_{a \in A} X_a$,

$$m(\underline{x}) \subseteq v^{-1}[n(\prod_{a \in A} u_a(x_a))].$$

The mapping $(\prod_{a \in A} u_a, v)$ will be called a strict

mapping if

(iv) for each $x \in \prod_{a \in A} X_a$,

$$m(\underline{x}) = v^{-1}(n(\prod_{a \in A} u_a(x_a))).$$

Lemma A1.2 characterizes privacy preserving correspondences in terms of the inverse correspondence; i.e. $m:\prod_{a \in A} X_a \dashrightarrow M$ is privacy preserving if and only if the inverse correspondence carries points to rectangles. Because of that characterization it is useful to describe mappings by what they do to inverse correspondences. This the content of the next lemma. The representation applies equally well to arbitrary relations, and the more general statement significantly lightens the notation.

Lemma A2.1. Suppose that $m:X \dashrightarrow M$ and $n:Y \dashrightarrow N$ are relations and assume that $u:X \dashrightarrow Y$ and $v:M \dashrightarrow N$ are functions. Then

(i) $m(x) \subseteq v^{-1}[n(u(x))]$ for each x in X if and only if $u(m^{-1}(z)) \subseteq n^{-1}(v(z))$ for each z in M,

(ii) $m(x) = v^{-1}[n(u(x))]$ for each x in X if and only if $m^{-1}(z) = u^{-1}[n^{-1}(v(z))]$ for each z in M.

Proof. We first prove (i). If

$$v(\, m(\, x\,)\,)\subseteq n(\, u(\, x\,)\,)$$

and if

$$w\in u(m^{-1}(\, z\,)\,),$$

then $w=u(\, x\,)$ for some $x\in m^{-1}(\, z\,)$. But $z\in m(\, x\,)$ and, because

$$v(\, m(\, x\,)\,)\subseteq n(\, u(\, x\,)\,),$$

it follows that $v(\, z\,)\in n(\, u(\, x\,)\,)$. Hence $w=u(\, x\,)$ is an element of the set $n^{-1}(\, v(\, z\,)\,)$. Then

$$u(\, m^{-1}(\, z\,)\,)\subseteq n^{-1}(\, v(\, z\,)\,).$$

On the other hand, the proof of the "if" part of (i) is the same as the argument already given if one replaces m by m^{-1}, n by n^{-1}, X by M, Y by N, v by u and u by v.

We turn to the proof of (ii). If we assume that

$$m(\, x\,)=v^{-1}[\, n(\, u(\, x\,)\,)\,]$$

for all $x\in X$ it follows from (i) that

$$u(\, m^{-1}(\, z\,)\,)\subseteq n^{-1}(\, v(\, z\,)\,)$$

for each z in M. We need only show that

$$m^{-1}(\, z\,)\supseteq u^{-1}(\, n^{-1}(\, v(\, z\,)\,)\,)$$

for all z in M. Suppose that

$$w\in u^{-1}(\, n^{-1}(\, v(\, z\,)\,)\,).$$

Then

$$u(\, w\,)\in n^{-1}(\, v(\, z\,)\,)$$

and therefore

$$v(\, z\,)\in n(\, u(\, w\,)\,).$$

But if

$$m(w)=v^{-1}[n(u(w))],$$

then $z \in m(w)$ and hence $w \in m^{-1}(z)$. Now replace u by v, m by m^{-1}, n by n^{-1}, X by M, and Y by N in the proof of (i). The equality

$$m^{-1}(w)=u^{-1}[n^{-1}(v(w))]$$

for all $w \in M$ implies that

$$m(x)=v^{-1}[n(u(x))]$$

for all $x \in X$. ▒

Lemma A2.1 has the following simple consequence.

Theorem A2.1. Suppose that $\{X_a\}$ and $\{Y_a\}$ are two collections of nonempty sets indexed by a set A. If

$$m:\prod_{a \in A} X_a \rightarrow M$$

and

$$n:\prod_{a \in A} Y_a \rightarrow N$$

are privacy preserving correspondences, then a pair of functions

$$(\prod_{a \in A} u_a, v)$$

such that

$$\prod u_a : X_a \rightarrow Y$$

and

$$v: M \rightarrow N$$

is a mapping from m to n if and only if for each

$$z \in M,$$

$$m^{-1}(z)=(\prod_{a \in A} u_a)^{-1}[n^{-1}(v(z))].$$

The pair $(\prod_{a\in A} u_a, v)$ is a strict mapping if and only if

$$m^{-1}(\ z\ ) = (\prod_{a\in A} u_a)^{-1}[\ n^{-1}(\ v(\ z\ )\ )\ ]$$

for each $z\in M$.

In general, two mathematical structures M and N are considered to be equivalent or isomorphic, relative to the mappings defined between them. Once the mappings have been defined, then two objects M and N are isomorphic if there are mappings $u:M\text{--->}N$ and $v:N\text{--->}M$ so that the compositions $u\cdot v$ and $v\cdot u$ are identity maps on M and N, respectively. We use the same definition for the concept of isomorphism between privacy preserving correspondences. For such a definition to make sense one must define the composition of mappings between privacy preserving correspondences, check that such compositions are again mappings, and define the mapping that is to play the role of the identity mapping. The following definition and lemma are devoted to these housekeeping tasks. The proof of the lemma is routine and not included.

Definition A2.2. Suppose that $\{X_a\}$ is a collection of nonempty sets indexed by A, and suppose that $m:\prod_{a\in A} X_a\text{--->}M$ is a privacy preserving correspondence from $\prod_{a\in A} X_a$ to a set M. The identity

mapping from m to itself is the pair $(\prod_{a\in A} Id_a, Id_M)$ where Id_a is the identity function on X_a and Id_M is the identity function on the set M.

Lemma A2.2. Suppose that m:X--->M, n:Y--->N, and p:Z--->P are correspondences and suppose that

s:X--->Y,

u:M--->N,

t:Y--->Z

v:N--->P

are functions such that

(i) $m(x) \subseteq u^{-1}[n(s(x))]$

for all x in X;

(ii) $n(y) \subseteq v^{-1}[p(t(y))]$

for all y in Y.

Then,

(iii) $m(x) \subseteq (u\cdot v)^{-1}[p(t\cdot s(x))]$

for all $x \in X$.

Further if

(iv) $m(x) = u^{-1}[n(s(x))]$;

and

(v) $n(y) = v^{-1}[p(t(y))]$

for all $x\in X$ and all $y\in Y$;

then,

(vi) $m(x) = (u\cdot v)^{-1}[p(t\cdot s(x))]$

for all $x\in X$.

We can now give the definition of isomorphism between privacy preserving correspondences.

Definition A2.3. Suppose that $\{X_a\}$ and $\{Y_a\}$ are two collections of nonempty sets indexed by A. Suppose M and N are nonempty sets and assume that $m:\prod_{a\in A} X_a \text{--->} M$ and $n:\prod_{a \in A} Y_a \text{--->} N$ are privacy preserving correspondences. A mapping

$$(u,v)=(\prod_{a \in A} u_a,v):m\text{--->}n$$

is an isomorphism, and m and n are isomorphic, if there is a mapping

$$(s,t)=(\prod_{a \in A} s_a,t):n\text{--->}m$$

such that

$$(u,v)\cdot(s,t)=Id_n$$

and

$$(s,t).(u,v)=Id_m,$$

where Id_m and Id_n are the identity mappings on m and n, respectively.

Occasionally the following lemma simplifies the problem of verifying that two privacy preserving correspondences are isomorphic. The proof is straight forward and not included.

Lemma A2.3. Suppose that $\{X_a\}$ and $\{Y_a\}$ are two collections of nonempty sets indexed by A, and suppose

that M and N are sets. Suppose that

$$m:\prod_{a \in A} X_a \text{---}>M$$

and

$$n:\prod_{a \in A} Y_a \text{---}>N$$

are privacy preserving correspondences. The correspondences m and n are isomorphic if and only if for each $a \in A$ there is a one-to-one onto function

$$u_a:X_a \text{---}>Y,$$

and a one-to-one onto function

$$v:M \text{---}>N$$

such that the pair

$$(\prod_{a \in A} u_a, v)$$

form strict mapping from m to n.

The following example shows that the strictness condition given in the statement of Lemma A2.3 cannot be dropped.

Suppose that A consists of one element X and assume $X=\{P,Q\}$. Set

$$M=N=\{R,S,T\}.$$

Define a correspondence $m:X \text{---}>M$ by setting

$$m(\ P\ )=R$$

and

$$m(\ Q\ )=\{S,T\}.$$

Define a second correspondence $n:X \text{--}>N$ by the equations

$n(\ P\ )=\{R,S\}$

and

$n(\ Q\ )=\{S,T\}$.

Then, $I=(Id_X,Id_M)$ is a mapping from m to n, however I is not an isomorphism because the pair of functions (Id_X,Id_M) do not form a mapping from n to m.

It is an easy exercise to check that the relation of isomorphism is an equivalence relation on the class of privacy preserving correspondences. In the next section we investigate the equivalence classes of this equivalence relation.

Section A3. Isomorphisms

Lemma A1.2 shows that if a correspondence $m:\prod_{a\ \in\ A} X_a \dashrightarrow M$ is privacy preserving that for each $t\in M$ the set $m^{-1}(\ t\ )$ is a rectangle. If one treats these rectangles as the points of a set R then associated to m is a correspondence m* from $\prod_{a\in A} X_a$ to R given by setting

$m^*(\ x\ )=\{m^{-1}(\ t\ ):x\in m^{-1}(\ t\ )\}$.

The correspondence m* is privacy preserving since the inverse of each point in R is exactly that rectangle. For example, suppose that $X_1=X_2=\{0,1\}$ and suppose $M=\{a,b,c\}$. Define $m:X_1\ x\ X_2\dashrightarrow M$ by the equations

$m(\ 0,0\ )=\{a,b\}$,

$m(\ 1,1\ )=\{a,c\}$,

$m(\ 1,0\ )=m(\ 0,1\ )=\{a\}$.

Then

$m^{-1}(\ a\ )=\{(0,0),(1,1),(0,1),(1,0)\}=R(1)$,

$m^{-1}(\ b\ )=\{(0,0)\}=R(2)$,

and

$m^{-1}(\ c\ )=\{(1,1)\}=R(3)$.

The correspondence m* is given by

$m^*(\ 0,0\ )=\{R(1),R(2)\}$,

$m^*(\ 1,1\ )=\{R(3),R(1)\}$,

$m^*(\ 1,0\ )=m^*(\ 0,1\ )=\{R(1)\}$.

Note that in the example we can reconstruct m from m*.

Set

$v(\ a\ )=R(1)$,

$v(\ b\ )=R(2)$

and

$v(\ c\ )=R(3)$.

Then for each t in M,

$m^{-1}(\ t\ )=v^{-1}(\ m^{*-1}(\ t\ )\ )$.

Since v is one-to-one and onto it follows from Lemma A2.3 that m and m* are isomorphic. There is a clear advantage to working with the correspondence m* over working with the correspondence m, because the points of R are subsets the product space $X_1 \times X_2$. The representation of a privacy preserving correspondence by the rectangles associated to it is the powerful constructive technique used in [11]. The search for

message spaces which have minimal cardinality and realize a function is reduced to the consideration of spaces of rectangles.

It is not true that every privacy preserving correspondence is (to within isomorphism) a correspondence with message space formed of rectangles in a product $\prod_{a \in A} X_a$. Consider, for example, the following correspondence. Use

$X_1=X_2=\{0,1\}$,

set

M=I(the nonnegative integers)

and define

m(0,0)={4.j:j a nonnegative integer},

m(0,1) = {1+4.j:j a nonnegative integer},

m(1,0) = {2 + 4.j: j a nonnegative integer}

m(1,1) = {3+4.j:j a nonnegative integer}.

The correspondence m has as message space an infinite set and therefore is certainly not isomorphic to a correspondence formed of subsets of the product $X_1 \times X_2$. It is also clear, however, that m can be reconstructed from the correspondence m* from $X_1 \times X_2$ to {0,1,2,3} given by

m*(0,0)=0,

m*(0,1)=1,

m*(1,0)=2,

m*(1,1)=3.

In this section we make precise the relation between a correspondence $m:\prod_{a \in A} X_a \dashrightarrow M$ and the associated "internal" correspondence with message space consisting of rectangles in $\prod_{a \in A} X_a$.

Definition A3.1. Suppose that $\{X_a\}$ is a collection of nonempty sets indexed by A. Set $X=\prod_a X_a$. Denote by R(X) (or R when there is no fear of confusion) the set of all rectangles in X. Let $r_X:X \dashrightarrow R$ denote the correspondence defined by the equation

$$r_X(x)=\{r \in R: x \in r\}$$

for each $x \in X$. The correspondence r_X is the rectangle correspondence for the collection $\{X_a\}$.

Lemma A3.1. Suppose that $\{X_a\}$ is a collection of nonempty sets indexed by A. The rectangle correspondence for the collection is privacy preserving.

Proof. If R is the set of rectangles in $X=\prod_{a \in A} X_a$, then for each r in R the set $\{x:x \in r\}$ is a rectangle. The conclusion of the lemma now follows from Lemma A1.2.▒

The construction of the introductory paragraph of this section can be restated in terms of the rectangle correspondence.

Theorem A3.1. Suppose that $\{X_a\}$ is a collection of nonempty sets indexed by A and suppose $X=\prod_{a\in A} X_a$. Let $r_X:\prod_{a \in A} X_a$--->R(X) be the rectangle correspondence. Denote by Id the identity function X to itself. If m:X--->M is a privacy preserving correspondence, then there is a unique function v:M--->R(X) so that the pair (Id,v) is a strict mapping from m to r_X.

Proof. If m:X--->M is privacy preserving, define v:M--->R(X) by the equation

$$v(\ t\ )=m^{-1}(\ t\ ),$$

for each t in the set M. The correspondence v is clearly a function. If $x\in X$, then for each $t\in M$,

$$r_X^{-1}(\ v(\ t\ )\ )=(m^{-1}(\ t\ )\ )=m^{-1}(\ t\ ).$$

It follows from Lemma A2.3 that v is a strict mapping from m to r_X.

To prove the assertion on the uniqueness of v, suppose that v':M--->R is a second function so that (Id,v') is a strict mapping from m to r_X. For each $t \in M$, set $S=v(\ t\ )$ and $S'=v'(\ t\ )$. Both S and S' are elements of the set R. But

$$S=r_X^{-1}(\ v(\ t\ )\ )=m^{-1}(\ t\ )$$

and

$$S'=r^{-1}(\ v'(\ t\ )\ )=m^{-1}(\ t\ ),$$

because both (id,v) and (Id,v') are assumed to be

strict mappings. Therefore v(t)=S=S'=v'(t).▒

For a given collection $\{X_a\}$ of nonempty sets X_a indexed by a set A, Theorem A3.1 shows that all privacy preserving correspondences defined on a set $X=\prod_{a \in A} X_a$ are in one-to-one correspondence to functions that map to special subsets of R(X). The special sets in R are those sets of rectangles that cover X. To build a privacy preserving correspondence on X, choose a collection of rectangles in R(X) and call the set of those rectangles M*. The correspondence has as domain all of X, therefore the set of rectangles chosen must cover X. Define a correspondence m*:X---->M* by setting

$$m^*(x)=\{r:r \in M \text{ and } x \in r\}.$$

If M is a set and if v:M——>M* is a function from M onto M*, set

$$m(x)=v^{-1}(m^*(x))$$

for each x in X. The correspondence m is then a privacy preserving correspondence from X to M. Theorem A3.1 guarantees that as M* varies through all the classes of subsets of R that cover X, the procedure outlined above constructs all possible privacy preserving correspondences defined on the set X. This procedure leaves open the question of which privacy preserving correspondences (constructed by the choice

of M* and the function v) are isomorphic. Some information which is readily available.

Lemma A3.2. Suppose that $\{X_a\}$ is a collection of nonempty sets indexed by A, set $X=\prod_{a\in A} X_a$, and suppose that M and M′ are subsets of the set of rectangles R(X). Let i and i′ denote the inclusion maps of M and M′ into R, respectively. Set

$$m=i^{-1}\, r_X$$

and set

$$m'=i'^{-1}\, r_X$$

where r_X is the rectangle correspondence. The correspondences m and m′ are isomorphic if and only if for each $a\in A$ there is a one-to-one onto function

$$u_a:X_a\text{--->}X_a$$

such that

$$(\prod_{a\in A} u_a)[M]=M'.$$

Proof. Suppose that m and m′ are isomorphic. There is a mapping

$$(\prod_{a\in A} u_a, v):m\text{--->}m'$$

where each u_a is a one-to-one onto mapping from X_a to X_a, and v is a one-to-one onto mapping from M to M′. Further, because $(\prod_{a\in A} u_a, v)$ must be a strict mapping, it follows that for each $r\in M$,

$$m^{-1}(\, r\,)=(\prod_{a\in A} u_a)^{-1}[m'^{-1}(\, v(\, r\,)\,)\,].$$

That is,

$$r=(\prod_{a\in A} u_a)^{-1}[\ v(\ r\ )\ ],$$

or

$(\prod_{a\in A} u_a)(\ r\ )=v(\ r\ )$. But v must be a one-to-one and onto function. Therefore, $\prod_{a\in A} u_a$ carries each rectangle in M onto one and only one rectangle in M'.▒

We can describe the isomorphisms between privacy preserving correspondences, at least in the case in which both correspondences use the same collection of sets $\{X_a\}$ indexed by a set A. Suppose that $\prod_{a\in A} X_a=X$ and that m:X--->M is a privacy preserving correspondence. Denote by v(m) the function from M to R(X) that is uniquely determined by m (c.f. Theorem A3.1). Let M* denote the image of v(m) in R, denote by i the inclusion map from M* into R, and denote by m* the correspondence $i^{-1}r_X$, where r_X denotes the rectangle correspondence of the collection $\{X_a\}$. If n:X--->N is a second privacy preserving correspondence, and if $(\prod_{a\in A} u_a,v)$:m--->n is an isomorphism, then $\prod_{a\in A} u_a$ carries rectangles to rectangles and determines a one-to-one onto function u* from R onto R. Extend the v(.) notation used for m, and denote by v(n) the uniquely determined map from N to R(X) determined by n. Let N* denote the image of v(n). The function u*

must carry the set M* onto the set N*. Indeed, if $S \in M^*$ (so S is a rectangle) and if $S = m^{-1}(t)$, then,

(i) $(\prod_{a \in A} u_a)(S) = (\text{pr } u_a) m^{-1}(t) = n^{-1}(u(t))$.

Further the pair

$$(\prod_{a \in A} u_a, u^*)$$

(with u* restricted to M*) is an isomorphism from m* to n*. The equation (i) shows that the pair $(\prod_{a \in A} u_a, u^*)$ defines a strict mapping from m* to n*. Because $(\prod_{a \in A} u_a, u)$ is an isomorphism, each of the functions u_a and the function u must have an inverse. Suppose v_a is the inverse of u_a and suppose v is the inverse of u. Denote by v* the restriction of v to the image of v(n). Then $(\prod_{a \in A} v_a, v^*)$ is a strict mapping from n* to m* that is the inverse for $(\prod_{a \in A} u_a, u^*)$.

These relations are illustrated in the diagram of Figure A3.1.

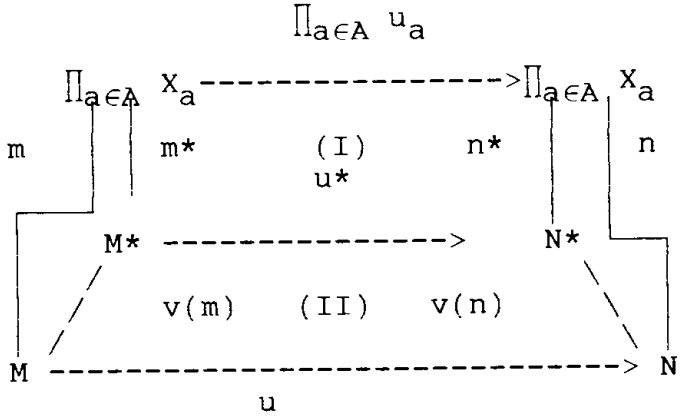

Fig. A3.1

If $t\in M$, then

$$u^*[\, v(\, m\,)(\, t\,)\,]=$$

$$(\prod_{a\in A} u_a)[\, m^{-1}(\, t\,)\,]=$$

$$n^{-1}[\, u(\, t\,)\,]=v(\, n\,)[u(\, t\,)].$$

Thus the diagram in Figure A3.1 commutes. Because the square labelled (II) commutes, it follows that the isomorphisms u* and u induce an isomorphism from the function v(m) to the function v(n). Thus isomorphisms between the privacy preserving correspondences m and n are constructed of an isomorphism between the associated correspondences m* and n* and an isomorphism between the functions v(m):M--->M* and v(n):N--->N*.

The construction of privacy preserving correspondences was for the purpose of realizing performance functions (c.f. [11] or [21]). In the next

section we shall apply the concepts introduced in this section to the study of realizations.

Section 4. Realizations.

In [20] privacy preserving correspondences were used to realize a performance standard. A performance standard is a function defined on a product, but when one need not contend with topological questions it is easy to extend the discussion to realizations of correspondences. We begin with the following definition.

Definition A4.1. Suppose that $\{X_a\}$ is a collection of nonempty sets indexed by A, assume Z is a set and suppose that $F:\prod_{a\in A} X_a \dashrightarrow Z$ is a relation. A realization of F consists of:

(i) a set M called the message space,

(ii) a privacy preserving correspondence

$m:\prod_{a\in A} X_a \dashrightarrow M$, called the

message correspondence,

and

(iii) a function $h:M\dashrightarrow Z$, called the outcome function,

such that,

(iv) for each $x\in\prod_{a\in A} X_a$,

$$h(m(x))\subseteq F(x).$$

Condition (iv) is the nonwasteful condition of [12]. In case F is a function, condition (iv) guarantees that h is constant on m(x) and that for each $x \in \prod_{a \in A} X_a$,

$F(x) \subseteq h(m(x))$.

Definition A4.1 coincides with the definition in [20] of an allocation mechanism that realizes a function F.

Lemma A2.3 is applicable also to the situation presented by a discussion of realizations. For the purposes of this section we would like to restate it.

Lemma A4.1. Suppose that $\{X_a\}$ is a collection of nonempty sets indexed by A, assume that M and are sets, and suppose that

$F: \prod_{a \in A} X_a \dashrightarrow Z$ is a correspondence. If

$m: \prod_{a \in A} X_a \dashrightarrow M$

is a privacy preserving correspondence and if

$g: M \dashrightarrow Z$

is a function, then the pair (m,g) realizes F if and only if for each $t \in M$,

$m^{-1}(t) \subseteq F^{-1}(g(t))$.

The condition

$m^{-1}(t) \subseteq F^{-1}(g(t))$

has some elementary consequences.

Suppose that the correspondence F has domain $X=\prod_{a\in A} X_a$. Suppose further that m:X--->M has image M and assume that F has image Z. If $t\in M$, then $t\in m(x)$ for some x. Similarly if $z\in Z$, then $z\in F(y)$ for some $y\in X$. In the case that m, g, and F are functions the condition

$$g(m(x))\subseteq F(x)$$

implies that

$$g(m(x))=F(x),$$

because F(x) is a point. Because m has image M it follows that g is uniquely determined by m. Indeed if t is an element of M, then t=m(x) so g(t)=F(x). Otherwise stated,

$$g(m(x))=F(x)$$

implies (by Lemma A2.1) that

$$m^{-1}(t)\subseteq F^{-1}(g(t))$$

for each t, so

$$g=F\cdot m^{-1}.$$

Lemma A4.1 summarizes the set theory used in [HRS] to construct minimal message spaces for performance standards that are differentiable functions. Suppose that $\{X_a\}$ is a collection of nonempty sets indexed by A, that $\prod_{a\in A} X_a=X$ and that F:X--->Z is a performance standard. In order to realize by a mechanism that uses a privacy preserving correspondence m, the correspondence m* :X--->R(X) must cover each level set

$F^{-1}(\ z\ )$ by disjoint rectangles. The privacy preserving correspondence required to realize F associates to each $x \in X$ the rectangles that contain x. The outcome function from the set of rectangles to the set is uniquely determined by the function F and the function m. In order to build a message space of minimum cardinality, it suffices to cover each level set of F by a collection of disjoint rectangles of minimum cardinality.

We complete this section by considering a few examples. First suppose that $X_1=X_2=\{0,1,2\}$. Define a function $F: X_1 \times X_2 \rightarrow \{0,1\}$ by setting

$$F(\ i,j\ )=a(\ i,j\ )$$

where $(a(\ i,j\ ))$ is the 3 x 3 matrix

$$\begin{matrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{matrix} .$$

Thus

$$F(\ 0,0\ )=1$$

while

$$F(\ 2,0\ )=0.$$

The set $F^{-1}(\ 0\ )$ consists of the points $\{0,2\}$ and $\{2,0\}$. The set $F^{-1}(\ 0\ )$ can be covered only by the two rectangles $S_0=\{0,2\}$ and $S_1=\{0,2\}$.

The set $F^{-1}(\ 1\ )$ has several different coverings by rectangles. We give three such covers.

Case 1. The first cover consists of the three rectangles

$R_1=\{(0,0),(0,1)\}$,

$R_2=\{(1,0,(1,1),(1,2)\}$

$R_3=\{(2,1),(2,2)\}$.

In this case a message space for a realization for the function F is the set of five points

$\{S_0,S_1,R_1,R_2,R_3\}=M$.

The message correspondence is given by

$m(\ x\ )=\{r:r\in M \text{ and } x\in r\}$.

Thus

$m(\ 0,0\ )=R_1$

while

$m(\ 1,1\ )=R_2$.

The function g:M-->{0,1} carries the "S" labelled rectangles to 0 and the "R" labelled rectangles to 1.

Case 2. The second covering of $F^{-1}(\ 1\ )$ consists of the three rectangles

R_1,

$R_2^* =\{(1,1),(1,2),(2,1),(2,2)\}$,

$R^*=\{(1,0)\}$.

Again the message space correspondence m* assigns to each point the rectangles that contain it. The outcome function, g, again assigns 0 to S labelled points and 1 to R labelled points. Note that the two correspondences m and m* are not isomorphic since no

one-to-one and onto function from $X_1 \times X_2$ to itself can change the number of points in a rectangle. Furthermore, it is relatively easy to see that any covering of the level set $F^{-1}(1)$ must contain at least three rectangles if the rectangles are to be disjoint. (A proof of this will be given in the next section). It follows that m and m* are both privacy preserving correspondences for realizations of F with a message space of minimum cardinality. Thus realizations with message spaces of minimum cardinality are not necessarily isomorphic.

Case 3. In this case cover $F^{-1}(1)$ by the two rectangles

$T_1=\{(0,0),(0,1),(1,0),(1,1)\}$

$T_2=\{(1,1),(1,2),(2,1),(2,2)\}$.

The message space for F consists of the four points S_0, S_1, T_1, and T_2. The message correspondence is not a function since the point (1,1) is in both rectangles T_1 and T_2. Thus it may be possible to lower the cardinality of a minimal message space by dropping the condition that the message correspondence be a function.

One might also hope that if $\{X_a\}$ is a collection of nonempty sets indexed by A, then a message space of minimum cardinality for $F:\prod_{a\in A} X_a \dashrightarrow$ occurs also as the minimum message space for the realization of a

thread of F. This is not true. In Case 3 above, the correspondence m* is privacy preserving and can be used to realize itself. The message space for the correspondence m* is the set

$$M^*=\{S_0,S_1,R_1^*,R_2^*\}.$$

It will be convenient to represent m* by the matrix

R_1^*	R_2^*	S_0
R_1^*	$\{R_1^*, R_2^*\}$	R_2^*
S_1	R_2^*	R_2^*

where

$$m^*(1,1)=\{R_1^*, R_2^*\}.$$

The outcome function from M* to itself must be the identity. The correspondence m* has an image that consists of four distinct points. Each of these points is actually a value of the function m* restricted to the complement of the point (1,1). Therefore the message space of any privacy preserving correspondence used to realize m* must have at least four points. The realization of m* by itself is then a realization with a message space of minimum possible cardinality. To examine the threads of the correspondence m* represent the subsets of the product space $X_1 \times X_2$ by the standard device of associating to a set its characteristic function. The characteristic function of a set takes the value 1 on points of the set and is otherwise 0. A subset of the product $X_1 \times X_2$ is

identified with a 3 x 3 matrix of 0's and 1's. There are only two distinct threads of the correspondence m*. Each of the threads coincides with the correspondence m* on the complement of the point (1,1). The first thread, s_1, takes the value R_1* on the point (1,1), while the second thread s_2 takes the value R_2* at the point (1,1). The thread s_1 has as level sets the following matrices;

$$s_1^{-1}(R_1^*)= \begin{matrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{matrix}$$

$$s_1^{-1}(R^*_2)= \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{matrix}$$

$$s_1^{-1}(S_1)= \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{matrix}$$

$$s_1^{-1}(S_0)= \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix} .$$

It is easy to see that five rectangles are required to cover these level sets. It follows that the minimum cardinality for the message space of a realization of s_1 is five. The thread s_2 is

constructed from s_1 by interchanging the rows and columns of the matrix for s_1, interchanging the subscripts of the R*'s and then, interchanging the subscripts on the S's. The thread s_2 also requires a message space cardinality at least five. It would appear, therefore, that restricting realizations to threads of correspondences inflates the size of the message space. We do not know this to be true in the topological case.

Section A5. Rank Conditions

In Section A4 the characteristic function of the level set of a function defined on a product X x Y was described as a matrix of zeros and ones. It is possible to give a bound on the number of disjoint rectangles required to cover a level set in terms of the rank of the matrix which describes the characteristic function of the level set. In particular this will give necessary and sufficient conditions to ensure that a function has a realization with a message space of finite cardinality. We shall explore only the case in which the function is defined on a product X x Y. We shall be very lax in specifying the set in from which the elements 0 and 1 are chosen. The elements 0 and 1 are to be taken from a field, but any field will do. The two fields of most interest are

the field of real numbers and the field Z/2Z that has only two elements 0 and 1.

Definition A5.1. Suppose that T is a subset of the product X x Y. We denote by M(T) the matrix that represents the characteristic function of T. We call M(T) the matrix of T.

Thus M(T) has rows indexed by elements of X, columns indexed by elements of Y and an entry in the (x,y) position that is a 1 if (x,y) is in T and a 0 if (x,y) is not in T. If T is a subset of X x Y, it is convenient to think of M(T) as a function on the entries of X x Y. Thus we will write M(T)(x,y) for the (x,y) entry of M(T).

The following lemma characterizes a set T as a rectangle by a condition on M(T).

Lemma A5.1. Suppose that T is a nonempty subset of a product X x Y. Then T is a rectangle in X x Y if and only if the matrix of T, M(T), has rank one.

Proof. Suppose that T is a rectangle. Then there are sets $U \subseteq X$ and $V \subseteq Y$ so that for each $z \in X \times Y$, $M(T)(z) = 1$ if and only if $z \in U \times V$. If a row of M(T) is indexed by an element u which is not in U, then the row must consist entirely of 0's. Suppose that u

and v are elements of U. Then for each y in X,

M(T)(u,y) = M(T)(v,y) = 1

if y is in V

and

M(T)(u,y) = M(T)(v,y) = 0

if y is not in V.

Thus the nonzero rows of M(T) are identical. It follows that M(T) has rank one.

Conversely, suppose that M(T) has rank one. Let U denote the set of elements of X which index a nonzero row. Similarly let V denote the set of elements in Y which index a nonzero column. Clearly if

M(T)(x,y) = 1 ,

then x is in U and y is in V.

Thus suppose that $x \in U$ and $y \in V$. Then

M(T)(x,z) = 1

and

M(T)(w,y) = 1

for some z and w.

But the row indexed by x is nonzero and,since M(T) has rank one, each nonzero row of M(T) must be a nonzero multiple of row x. In particular the row indexed by w must be a multiple of the row indexed by x. But since the only nonzero entries in either row are 1's it follows that row w is 1 times row x. Note that this is true no matter which field is used for the

elements 0 and 1. That is, the rows are identical. Thus if

$$M(T)(w,y) = 1,$$

then

$$M(x,y) = 1.$$

It follows that M(T) is nonzero on U x V. Thus M(T) is the characteristic function of the rectangle U x V.▒

As an immediate consequence of Lemma A5.1, we prove the following assertion.

Theorem A5.1. Suppose that T is a nonempty subset of the product X x Y with matrix M(T). Then T can be covered by a finite number of rectangles if and only if M(T) has finite rank.

Proof. First suppose that T can be covered by a finite number of rectangles, $R_1, \ldots, R_t$. Each R consists of the repetition of one single nonzero row vector v since Lemma A5.1 shows that the characteristic matrix of a rectangle has rank one. It follows that the nonzero rows of T all occur among the finite collection of row vector $v_1, \ldots, v_t$. Therefore T has finite rank.

Conversely, suppose the matrix of T has finite rank, say t. Choose elements $x_1, \ldots, x_t$ in X and elements $y_1, \ldots, y_t$ in Y so that the submatrix M of

the matrix of T which has rows and columns indexed by $x_1,\ldots,x_t$ and $y_1,\ldots,y_t$, respectively, has rank t. Suppose that the row vectors of M are $v'_1,\ldots,v'_t$. There are only 2^t-1 possible nonzero rows of zeros and ones with t entries. Denote by R the set of all possible nonzero rows of zeros and ones with t entries which are linear combinations of the row vectors $v'_1,\ldots,v'_t$. For v in R, if $v=x_1(v)v'_1+\ldots+x_t(v)v'_t$, then the $x_i(v)$ are uniquely determined because the matrix M is nonsingular. If u is a nonzero row of the matrix of T, then the vector u' with entries in the columns $y_1,\ldots,y_t$ equal those of u is an element of the set R. It follows that

$$u'=x_1(u')v'_1+\ldots+x_t(u')v'_t,$$

and because u is a linear combination of the linearly independent vectors v, then

$$u = x_1(u')v_1+\ldots+x_t(u')v_t.$$

Therefore, there are only a finite number of distinct nonzero rows among the rows of the matrix of T. It follows that we may cover T by a finite number of rectangles, since we may choose for each distinct row vector v of T the rectangle which consists of all the rows of T which are identical to v.

Theorem A5.1 establishes an upper bound on the number of rectangles required to cover a set T in X x Y

in terms of the rank of the matrix of T. In particular, if the matrix of T has rank t, then no more than 2^t+t-1 disjoint rectangles are required to cover T.

A more interesting problem is to establish a lower bound on the number of elements in a rectangular covering of a set in X x Y in terms of the rank of the matrix of the set.

Theorem A5.2. Suppose that X and Y are finite sets and suppose that S is a subset of the product X x Y. Suppose that S has matrix M of rank t. Then each covering of S by disjoint nonempty rectangles requires at least t distinct rectangles.

Proof. Assume that $X = \{1,...,n\}$ and $Y = \{1,...,m\}$. Suppose that S can be covered by s distinct disjoint rectangles $R_1,....,R_s$. Each rectangle R_i has a matrix M which can be described as a repeated row vector v, because M must have rank one. Suppose that the r^{th} row is nonzero in the matrix of S. The r^{th} row must be covered by intersections with the rectangles R_i, by which we mean that if the j^{th} column of the row r is nonzero, then the j^{th} column of row r in one of the matrices M_i must also be nonzero. Because the rectangles R_i were assumed to be disjoint, each nonzero entry in the rth row can be covered (in

the sense just described) by at most one rectangle. It follows that the r^{th} row is a sum of the vectors v_i for those i's for which the rectangle R_i intersects the set of points $\{(r,j):1\leq j\leq m\}$. This shows that the rank of the matrix of T is at most s, the number of rectangles in the covering. Thus if the rank of T is t, then there are at least t rectangles in a covering of T by disjoint rectangles.▒

Finally, note that Theorem A5.2 can be used to establish that in the examples which are at the end of section A4, a covering by disjoint rectangles of the set described by the matrix

$$\begin{matrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{matrix}$$

requires at least three rectangles. This follows from the fact that the given matrix has rank three no matter what field is used for the elements 0 and 1.

Appendix B.

Leontief and Abelson Theorem

Suppose that $F(x_1,\ldots,x_N)$ is a function of N variables which has continuous partial derivatives to order D. If $\alpha =(\alpha(1),\ldots,\alpha(N))$ is a sequence of nonnegative integers, denote by $|\alpha|$ the sum $\alpha(1)+\ldots+\alpha(N)$. we denote by

$$D(x_1^{\alpha(1)}\ldots x_N^{\alpha(N)};F)$$

the derivative $\partial^{|\alpha|}F/\partial x_1^{\alpha(1)}\ldots\partial x_N^{\alpha(N)}, D>|\underline{\alpha}|$. Set

$$Z^0F/Zx_j^0 = F.$$

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.[29].

Theorem B.1. Suppose that $x=(x_1,\ldots,x_m)$ and $y=(y_1,\ldots,y_n)$ 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 $(p,q)=(p_1,\ldots,p_m,q_1,\ldots,q_n)$ that satisfy the following

conditions.

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

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 $w-G(x_1,\ldots,x_m)=0$ 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

$$D(x_j;C)=D(x_1;F)D(x_j;c)+D(x_j;F)$$

for $j>1$. Because

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

it follows that

$$0=D(x_1;G)D(x_j;c)+D(x_j;G) \text{ for } j>1.$$

Further, by condition (i), there is an Ω so that $D(x_j;F)=\Omega D(x_j;G)$ for $1\leq j\leq m$. Therefore

$D(x_j;C)=\Omega[D(x_1;G)D(x_j;c)+D(x_j;G)]=0$. Hence the function C is independent of the variables $x_2,\ldots,x_m$ and we can write

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

Then

$$C(\ G(\ x_1,\ldots,x_m\ ),y\ )=$$

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

$$F(\ x_1,\ldots,x_m,y\ ).$$ ▒

Leontief proved the following result in [11].

Theorem B.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 $1\le k\le n$

$$\partial/\partial y_k[F_i/F_j]=0,$$

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

Proof. Form the matrix

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

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 $F(\ x,y\ )=C(\ G(\ x\ ),y\ )$.▒

The conditions discussed in this appendix are rank conditions on matrices that are bordered Hessians for functions defined on products. The notation for these matrices extends the notation $H(F:x_i;x_{<-i>})$ and $BH(F:x_i;x_{<-i>})$ already introduced in Chapter VI to the case of m-tuples of functions. Because the notation is cumbersome, at best, we give the extended notation in detail.

Suppose that $E^1,\ldots,E^n$, are Euclidean spaces of dimensions $d(1),\ldots,d(n)$, respectively. We suppose that the space E^i, $1\leq i\leq n$ has coordinates $(x_{i1},\ldots,x_{id(i)})$. Assume that $(p_1,\ldots,p_n)$ is a point of $E^1x\ldots E^n$, and assume that U_i is an open neighborhood

of the point p_i for $1 \leq i \leq n$. Suppose that F_j, $1 \leq j \leq m$, is a real valued C^2-function defined on $U_1 x \ldots x U_n$.

(I):

$BH(F_1,\ldots,F_m:x_{i\ 1},\ldots,x_{i\ d(i)};x_{1\ 1},\ldots,x_{i-1\ d(i-1)},$
$\ldots,x_{i+1\ 1},\ldots,x_{n\ d(n)})=$
$BH(F_1,\ldots,F_m:x_i;x_{<-i>})$

is a matrix that has rows indexed by $x_{i\ 1},\ldots,x_{i\ d(i)}$ and columns indexed by $F_1,\ldots,F_m,(F_1,x_{1\ 1}),\ldots,$ $(F_1,x_{i-1\ d(i-1)}),(F_1,x_{i+1\ 1}),\ldots,(F_1,x_{n\ d(n)}),\ldots,$ $(F_m,x_{1\ 1}),\ldots,(F_m,x_{i-1\ d(i-1)}),(F_m,x_{i+1\ 1},\cdot\cdot,$ $(F_m,x_{n\ d(n)})$. The entry in the $x_{iu}{}^{th}$ row and in the $F_v{}^{th}$ column is $D(x_{i\ u};F)=\partial F_v/\partial x_{i\ u}$. The entry in the $x_{i\ u}{}^{th}$ row and in the $(F_v,x_{j\ w})^{th}$ column is $D(x_{i\ u}\ x_{j\ w};F_v)=\partial^2 F_v/\partial x_{i\ u}\ \partial x_{j\ w}$.

As we noted in Chapter VI, the matrix $BH(F_1,\ldots,F_m:x_i;x_{<-i>})$ is a type of bordered Hessian because it consists of a matrix of second derivatives bordered by collection of columns of first derivatives.

(II):

$H(F_1,\ldots,F_m:x_i;x_{<-i>})$ is the submatrix of $BH(F_1,\ldots,F_m:x_i;x_{<-i>})$ that consists of the columns indexed by $(F_i,x_{u\ v})$ for $1\leq i\leq m$, $u\in\{1,\ldots,i-1,i+1,\ldots,n\}$ and $1\leq v\leq d(u)$. In other words, we derive H from BH by eliminating the columns indexed by the functions $F_1,\ldots,F_m$.

Leontief and Abelson used the matrice BH and H in the special case of one function F defined on a product

E^1xE^2. As already noted in Chapter VI, if E^1 has coordinates $(x_1,...,x_p)$ and E^2 has coordinates $(y_1,...,y_q)$ then we use as row indices for $BH(F:x_1,...,x_p;y_1,...,y_q)$ the variables $x_1,...,x_p$ and as columns indices F, $y_1,...,y_q$. The $(x_i,F)^{th}$ entry in $BH(F:x_1,..,x_p;y_1,...,y_q)$ is $\partial F/\partial x_i=D(x_i;F)$ and the $(x_i,y_j)^{th}$ entry is

$$D(x_i\ y_j;F)=\partial^2/\partial x_i\ \partial y_j.$$

We follow the same convention established in Chapter VI that when a partial evaluation of the matrices $BH(F_1,...,F_m:x_i;x_{<-i>})$ and $H(F_1,...,F_m:x_i;x_{<-i>})$ occurs we indicate this by adding an asterisk to the H or BH. Specifically,

(III):

$BH^*(F_1,...,F_m:x_i;x_{<-i>})[\ x_i,p_{<-i>}\ ]$ is the matrix that results from evaluating the variables

$$x_1,...x_{i-1},x_{i+1},...x_n$$

in the entries of

$$BH(F_1,...,F_m:x_i;x_{<-i>})$$

at the point $p_{<-i>}=(p_1,...,p_{i-1},p_{i+1},...,p_n)$.

The matrix $BH^*(F_1,...,F_m;X_i,x_{<-i>})[\ x_i,p_{<-i>}\ ]$ is a function of the variables $x_{i\ 1},...,x_{i\ d(i)}$ alone. Similarly, the matrix

$$H^*(F_1,...,F_m;X_i,x_{<-i>})[\ x_i,p_{<-i>}\ ]$$

is the submatrix of $BH^*(F_1,...,F_m;X_i,x_{<-i>})[\ x_i,p_{<-i>}\ ]$ derives by deleting the columns indexed by $F_1,...,F_m$.

Corollary B.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 in Chapter VI, Lemma 6.1. Set $F_j=D(x_j;F)$. Theorem B.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,

$$\Omega(F_1,\ldots,F_m)^t =$$

$$(D(x_1y_k;F),\ldots,D(x_my_k;F))^t$$

(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 B.2.2. Suppose that $F(x;y)$ is a C^2-function in the variables $x=(x_1,\ldots,x_m)$ and $(y_1,\ldots,y_n)$. A necessary 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 Corollary B.3.2 that F(x;y)=C(A(x),y) for some A and C. To complete the proof, it will suffice the prove that C(w,y) satisfies the conditions of Corollary B.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

$$D(y_j;C) =$$

$$D(y_j;F(h(w,x_2,\ldots,x_m),x_2,\ldots,x_m);y)) \text{ and}$$

$$D(wy_j;C)=D(x_1y_j;F)\ D(w;h).$$

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 Lemma B.2.1

$$C(w,y)=G(w,B(y))$$

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 B.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 B.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 $(x_{i,1},\ldots,x_{i,d(i)})$. 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, $1\leq j\leq r$ 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

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

Proof. The necessity of the conditions was proved in Chapter VI, Lemma 6.1. The sufficiency is a straight forward induction.▒

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 B.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 x Y to R that are defined on a neighborhood U x V of a point (a,b), a $\in$ X and b $\in$ Y.

A necessary condition that there are functions

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

functions

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

such that

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

$$G_i(A_1,\ldots,A_r,y_1,\ldots,y_n),\ 1\leq i\leq N,$$

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

$BH(F_1,\ldots,F_N:x_1,\ldots,x_m;y_1,\ldots,y_n)$ has rank less than or equal to r at each point of U x V.

Proof. Because

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

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

it follows that

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

and

$$D(x_j\ y_k;F_i) =$$

$$\Sigma\ D(y_k\ A_s;G_i)\ D(x_j;A_s).$$

Each of the columns is a linear combination of the r columns

$$(D(x_1;A_i),\ldots,D(x_m;A_i))^T,\ 1\leq i\leq r,$$

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 B.4. 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

Fi, $1 \leq i \leq N$, is a C^{k+1}-function, $k \geq 2$, from U x V to R.

Then

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

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

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

defined on W x V , and C^k-functions

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

defined on U x V such that

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

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

$y_1,\ldots,y_n),$

for $1 \leq i \leq N$, is that the matrix

$BH(F_1,\ldots,F_n:x_1,\ldots,x_p;y_1,\ldots,y_q)$

has rank less that or equal to r at each point of U x 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 x 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 x Y, a neighborhood W x V' of (p',q), a neighborhood U'x V' of (p,q),

C^k-functions $G_1,\ldots,G_N$,

defined on W x 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' x 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. 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)=

$y_1+y_3+y_1y_4$	$1+y_4$	0	1	y_1
$y_2+y_3-y_1y_4+$	$-y_4+2x_2(1+y_4)$	1	$1+2x_2$	$-y_1+2x_2y_1$
$2x_2(y_1+y_3+y_1y_4)$				
$2x_3[y_2+y_3-y_1y_4]$	$-2x_3y_4$	$2x_3$	$2x_3$	$-2x_3y_1$

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]=

3	2	0	1	1
$1+6x_2$	$-1+4x_2$	1	$1+2\ x_2$	$-1+2\ x_2$
$2\ x_3$	$-2\ x_3$	$2x_3$	$2\ x_3$	$-2x_3$

It is an easy exercise to check that BH* has rank 2 in R^3. Furthermore,

the matrix H*(F:x;y)[p,q]=

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

has rank 2. Theorem B.4 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

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

$$D(y_2;F)=x_2+x_3^2$$

$$D(y_3;F)=x_1+x_2+x_2^2+x_3^2 \quad \text{and}$$

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

At the point q these derivatives are

$$D(y_1;F)=2x_1-x_2+2x_2^2-x_3^2$$

$$D(y_2;F)=x_2+x_3^2$$

$$D(y_3;F)=x_1+x_2+x_2^2+x_3^2 \quad \text{and}$$

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

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 [7:p.7], because we have already observed that the necessary rank condition is satisfied using the first two rows and first two columns of $B^*(F:x;y)[\ p,q\ ]$. In this case, of course, the solutions are easily written down. That is,

$$x_2=w_2-x_3^2$$

and

$$x_1=(1/2)(w_1+w_2-2\ w_2^2+4w_2x_3^2-2x_3^4).$$

The final computation in the proof of Theorem B.4 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 $G(\ A_1,A_2;y_1,\ldots,y_4\ )=F$.

We now turn to the formal proof of Theorem B.4.

Proof. Condition (i) has already been established in Lemma B.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 [7] shows that there is a neighborhood U* of p, and C^k-functions

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

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

that are defined on U* such that

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

$1\le i\le r$, 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

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

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

$$h_r(\ w_1,\ldots.,w_r,x_{r+1},\ldots,x_m),y_1,\ldots,y_q\ ),\ 1\le i\le N.$$

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* x V, because BH has rank at most r in U x 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* x V. It follows, that for each $1\le i\le N$, and $1\le t\le m$,

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

where the C_{is} are functions on U* x V. Furthermore, if one differentiates Eq 4.1 by x_j, for $r+1\le j\le m$, it follows that

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

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

$$D(x_j;G_i)=$$

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

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

$$\Sigma_{s=1} C_{is}\, D(x_j;A_s) =$$

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

$$0.\blacksquare$$

Computational Complexity of Mechanisms

Appendix C

Graphs and Networks

In this appendix we present a formal version of the McCulloch and Pitts model for computing that allows described informally in Chapter III. It is convenient to use the terminology of graphs and directed graphs. Definitions and terminology can be found in [5].

Definition C.1. A general abstract mixed graph G is an ordered tuple (V,X,α) where

(i) V is a finite set of elements called points or vertices,

(ii) X is a finite set whose elements are called edges,

(iii) α is a function assigning to each element of X an element of the set $V \times V \cup B$, where B consists of the subsets of X of cardinality one or two.

If α assigns to an element x an ordered pair, then x is a directed edge. If $\alpha(x)$ is a two element set, then x is an undirected edge. If $\alpha(x)$ is a single element, then x is a self loop. If α assigns to each x a subset of V of cardinality two, then the general

abstract mixed graph is a graph. In that case, each edge is called an arc. If α assigns an ordered pair to each element of X, then the general abstract mixed graph is called a digraph and the edges will also be called arcs or directed edges. If x is a directed edge in an abstract mixed graph with $\alpha(x)=(u,v)$, then u is the initial point of x and v is the end point of x. We will use the notation $\beta(x)$ for the initial point of x and
$\varphi(x)$ for the end point of x.

We will make one change in the discussion of graphs and digraphs found in [4]. We extend the definition of a walk to the case of abstract mixed graphs; that is, we allow self loops.

Definition C.2. If (V,X,α) is an abstract mixed graph, then for each $u,v \in V$, a walk from u to v is an alternating sequence of points and edges

$$(u=v_0, e_1, v_1, e_2,\ldots,v_{n-1},e_n, v_n=v)$$

such that for each e_i in the sequence

$\alpha(e_i) = (v_{i-1}, v_i)$ (ordered pair),

or $\alpha(e_i)=\{v_{i-1},v_i\}$ (the set).

The number n in the definition of the walk is called the length of the walk. The vertex v_0 is the initial vertex of the walk and e_1 is the initial arc of

the walk. If the edges of a walk are distinct, the walk is a trail. The number of edges in a trail is called the length of the trail. If the vertices of a trail are distinct, then the trail is called a path. The path is a directed path if each edge in the path is a directed edge. A trail is a closed trail if it is a path from v to v. A cycle is a closed trail of distinct points except for the first and last points.

Definition C.3. If (V,X,α) is a digraph, then the underlying abstract mixed graph of (V,X,α) is (V,X,α^*) where $\alpha^*(x)=\{u,v\}$ when $\alpha(x)=(u,v)$.

In other words, the underlying abstract mixed graph of a digraph is the abstract mixed graph produced by ignoring the orientation of arcs. The underlying mixed graph of a digraph is not, necessarily, a graph.

Definition C.4. A general abstract mixed digraph is connected if each pair of points can be connected by a walk. A digraph is connected if it is connected as a general abstract mixed digraph.

Definition C.5. A tree is a connected graph without cycles.

Definition C.6. An out-tree is a digraph such that the underlying abstract mixed graph is a tree (i.e. a directed tree) that has a distinguished point called a root with the property that all other points are reachable by directed paths from the root. An in-tree is a directed tree with a distinguished point(the root) so that each point can be connected to the root by a directed path.

Definition C.7. If v is the vertex of a digraph, then type(v)=(a,b) if a is the number of arcs with end point v and b is the number of arcs with initial point v. Sometimes a is called the in-degree and b is called the out-degree.

Definition C.8. If (V,X,α) is a digraph, then a vertex of type (0,.) is called a leaf(See Figure C.1). A vertex v of type (1,a) such that (v,v) is an edge is called an elementary loop vertex or an elementary vertex. (See Figure C.2)

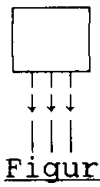

Figure C.1

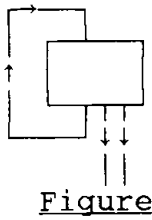

Figure C.2

Definition C.9. Suppose that G is a digraph and

suppose that d is a positive integer. Functions with values in R^d will be called $\underline{R^d}$ valued functions. A function with values in R^d defined on the vertices of G is an $\underline{R^d}$ state of G. The set of all R^d states of G we denote by $\underline{S(G;R^d)}$. In case the value d is clear we will mean by a state of G, an R^d state G.

In the case that V=R, one may also think of the collection of states of G as a vector space of n-tuples where n is the number of vertices in G and where each element of the n-tuple is indexed by a unique vertex of G.

Definition C.10. A function C from $S(G;R^d)$ to $S(G;R^d)$ is a transformation of states of G if C satisfies the following conditions:

(i) for each vertex v of G, if the in-degree of v is s and v is the end point of arcs $e_1,\ldots,e_s$, then there is an R^d valued function of s variables associated to v, C#(v;.), of variables $(x_1,\ldots,x_s)$, where x_i corresponds to the arc e_i,

(ii) if σ is an element of $S(G;R^d)$, and if

C(σ)(v) denotes the v^{th} component of

C(σ), then

C(σ)(v)=

C#(v;σ(ß(e_1)),...,σ(ß(e_s))),

(where ß(e) denotes the initial point of

the arc e),

(iii) if v is a vertex that is the end point of no arc, then

$C(\sigma)(v)=\sigma(v)$, for each $\sigma \in S(G;R^d)$.

The purpose of the definitions is to construct a model in which a digraph represents modules in a network and the arcs of the graph represent connections between the modules. A digraph G and a transformation of the states $S(G;R^d)$, C, can be viewed as representing one instant in a computation carried out by the functions C#(v,.) assigned to the vertices of the digraph. The analysis of the time required for a computation is simpler if the digraph is without leaves. The assumption that the digraph is without leaves is not a significant restriction because each digraph can be extended to a leaf-free digraph by replacing the leaves of G by elementary loop vertices. Indeed, for each v that is a vertex that is a leaf of G, connect v to itself by an arc. Call the new digraph G′. Note that the extension replaces leaves with vertices of in-degree 1. Let C be a transformation of states of G. Extend C to a transformation of states C′ on G′ by assigning the identity function to each vertex of G′ that was a leaf of G. The graphs G and G′ have the same set of states. Furthermore, condition (iii)

of Definition C.10 shows that the effect of C on the states of G is the same as the effect of C′ on the states of G′. Therefore, in the discussion of transformations of states we may assume, when convenient, that the graph G is without leaves. In our formalization, data is to be introduced at specific vertices and output occurs at designated vertices. We give the following definition.

Definition C.11. A digraph with a designated (ordered)array of distinct vertices $(v_1,\ldots,v_\alpha)$ that are either leaves or elementary loop vertices, called input vertices, and a designated (ordered)array of distinct vertices $(w_1,\ldots,w_\beta)$, called output vertices, will be called an input-output digraph.

An input-output digraph may have an empty array of input vertices or an empty array of output vertices.

Notation. Suppose that G is an input-output digraph with input vertices $(v_1,\ldots,v_\alpha)$. Let $a=(a_1,\ldots,a_\alpha)$ be an array of d-vectors, then $I_G(\ a\ )$ denotes the function on $S(G;R^d)$ that carries a state σ to that state σ', that assigns the value a_i to v_i, and otherwise coincides with σ. In general, the function $I_G(a)$ is not a d-valued transformation of states. The function $I_G(\ .\ )$ will also be designated by $I(\ .\ )$ when

the context makes the subscript superfluous.

In the informal discussion of the previous Chapter III, a function's complexity was indicated by the minimum time required for (r,d)-networks to compute the function. We are interested in the time required for the computation of the value of a function when the values assigned to the variables of a function are assigned to the input-vertices at the beginning of the computation, and the assignment to the input-vertices remains fixed throughout the computation.

The complexity of the function depended on the values of the integers r and d. The integer r was a restriction on the number of lines connected to a module, and d was the size of the alphabet used in the computation. This leads to the following definition.

Definition C.12. Suppose that G is an input-output digraph with input vertices $(v_1,\ldots,v_\alpha)$ and output vertices $(w_1,\ldots,w_\beta)$. Suppose that each vertex of G has in-degree at most r and suppose that C is a transformation of the states of $S(G;R^d)$ such that $C\#(\ v_i;.\ )$ is the identity function for each $1\leq i\leq\alpha$. The pair (G,C) that consists of the input-output graph G and C, the transformation of the states $S(G;R^d)$, is called an (r,d)-network. The pair that consists of a vertex v of a network and the function $C\#(\ v;.\ )$

associated to that vertex in the definition of the transformation of states C is called a module of the network.

Normally we denote an (r,d)-network by the name of the transformation of states C.

Note that if C is a transformation of the states $S(G;R^n)$ of an input-output digraph G, where G has leaves, then replacing the leaves of G by elementary loop vertices produces a new input-output digraph G' with a new transformation of the states $S(G;R^n)$. Also, for $\sigma \in S(G;R^n)$,

$$(C\cdot I(\ a\ ))(\ \sigma\ )=(C'\cdot I(\ a\ ))(\ \sigma\ ).$$

Definition C.13. Let F be a function from the space of α-tuples of vectors in R^d to the space of β-tuples of vectors in R^d and suppose that C, i.e.(G,C), is an (r,d)-network with input vertices $(v_1,\ldots,v_\alpha)$ and output vertices $(w_1,\ldots,w_\beta)$. Suppose that σ is a state in $S(G;R^d)$. Let t be a positive integer. We say that network C computes F in time t with outputs at the vertices $(w_1,\ldots,w_\beta)$ and inputs at $(v_1,\ldots,v_\alpha)$ from the initial state σ if for each sequence of real numbers

$(a_1,\ldots,a_\alpha)=a$,

$$F(\ a_1,\ldots,a_\alpha\ )=$$

$((\{C \cdot I(\ a\ )\}^t\ \sigma\ )[\ w_1\ ],\ldots,(\{C \cdot I(\ a\ )\}^t \sigma\ )[\ w_\beta\ ])$, where $\{C \cdot I(\ a\ )\}^t$ denotes the t-fold iteration of $C \cdot I(\ a\ )$.

Suppose that C is an (r,d)-network with digraph G. What computation does C make in time t? In particular, what conditions must a real valued function F satisfy in order that C can compute F in time t? It is convenient for such an analysis to replace C with an (r,d)-network C′ that has an input-output digraph that is a tree of length t such that the network C′ computes the same function F in the same time t. Of course, this requires that the tree that replaces the digraph of C has vertices with in-degree at most r. We wish also to assign to the vertices of the tree either the functions that occur as modules of C, or possibly with identity functions. The replacement procedure, which we will refer to as <u>delooping</u> C, is most easily carried out when the graph of C is leaf-free.

The next two lemmas will be used to replace a network C with digraph G that computes a function in time t by a network with digraph T that has underlying abstract graph a tree and also compute the same function in time t. The tree T depends on the time allotted for the computation. The relation between the

original digraph G and the directed tree T that replaces G can be described in terms of a map of graphs from the directed tree T to the digraph G. Lemma C.1 is used in the construction of this map.

Definition C.14. Suppose that G and G′ are digraphs. Assume that G has vertices V(G) and arcs X(G) while G′ has vertices V(G′) and arcs X(G′). A map of digraphs Θ from G to G′ is a pair of functions, Θ_V:V(G) --->V(G′) and Θ_A:X(G)--->X(G′), such that for each if $x \in X(G)$, $\beta(\Theta_A(x))=\Theta_V(\beta(x))$ and $\varphi(\Theta_A(x))=\Theta_V(\varphi(x))$.

A map of digraphs is illustrated in Figure C.3. The element x is an arc of G that has initial point $\beta(x)$ and end point $\varphi(x)$. The map Θ_A carries the arc x to the arc $\Theta_A(x)$, while the map Θ_V carries the beginning point of x to the beginning point of $\Theta_A(x)$ and the end point of x to the end point of $\Theta_A(x)$.

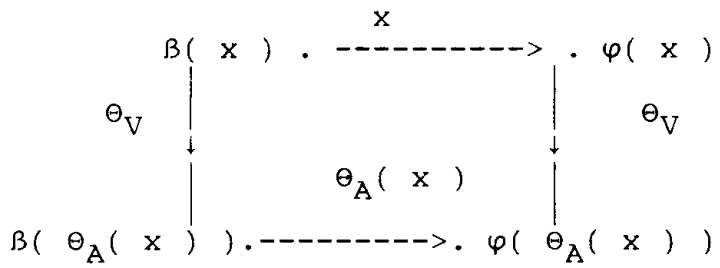

Figure C.3

If $\Theta=(\Theta_V,\Theta_A)$ is a map of digraphs, we will drop the subscripts A and V when there is no possibility of confusion.

Note that if $\Theta=(\Theta_V,\Theta_A)$ is a map of digraphs, then the map Θ carries walks in G to walks in G'.

Lemma C.1. Suppose that C and C' are (r,d)-networks with input-output digraphs G and G', respectively, and suppose that G' is leaf free. Assume that σ and σ' are R^d states of G and G', respectively, and suppose that t is a non-negative integer. Assume that the input vertices of C are $(v_1,\ldots,v_\alpha)$, the input vertices of C' are $(v'_1,\ldots,v'_\alpha)$, the output vertices of C are $(w_1,\ldots,w_\beta)$, and the output vertices of C' are $(w'_1,\ldots,w'_{\beta'})$. Suppose that $\Theta=(\Theta_V,\Theta_A)$ is a map from the graph G to the graph G' that satisfies the following conditions;

(i) $\Theta_V(v_i)=v'_i$ and $\Theta_V(w_i)=w'_i$,

(ii) $\sigma'(\Theta_V(v))=\sigma(v)$,

(iii) if $\Theta_V(\ v\ )$ is the end point of an arc that is included in a walk of length t ending at an output vertex of C', then Θ_A is an onto map from the arcs that end in v to the arcs that end in $\Theta_V(\ v\ )$,

(iv) if $\Theta_V(\ v\ )$ is the end point of arcs $e'_1,\ldots,e'_s$ and if $\Theta_V(\ v\ )$ is the end point of an arc that occurs in a walk of length t that ends in an output vertex of G', then v is the end point of arcs $e_1,\ldots,e_s$,

$$\Theta_A(\ e_i\ )=e'_i,$$

$$ß(\ e'_i\ )=\Theta_V(\ ß(\ e_i\ )\ ),$$

and

$$C'\#(\ \Theta_V(\ v\ );x_1,\ldots,x_s\ )=$$

$$C\#(\ v;x_1,\ldots,x_s\ ),$$

(v) if w' is a walk in G' of length t that ends in an output vertex of G', then there is a walk w in G of length t so that $\Theta(\ w\ )=w'$.

It follows that

$$(\ \{C\cdot I(\ a\ )\}^t\sigma\ )(\ w_i\ )=$$

$$(\ \{C'\cdot I(\ a\ )\}^t\sigma'\ )(\ w_i\ ),$$

for each $1\le i\le ß'$ and each $a=(a_1,\ldots,a_\alpha)$.

Proof. We will prove the assertion by an inductive argument on the length t of the walks.

Assume that t=1. Suppose that the output vertex w'_i in G' is the end point of the arcs e'_{ij}, $1\le j\le\tau'(i)$.

Assumption (i) states that the map Θ_V carries w_i to the vertex w'_i . Let w'_{ij} be the initial point of the arc e'_{ij}. It follows from (v) that for each $1\leq j\leq\tau(i)$ there is a walk in G of length 1 that is mapped by Θ onto the walk (w'_{ij},e'_{ij},w'_i). The vertex $w'_i=\Theta_V(\ w_i\ )$ is the end point of the arc e'_{ij}, therefore it follows from (iii) follows that Θ_A carries the arcs ending in w_i onto the arcs ending in w'_i. Suppose that the arcs ending in w_i are $\{e_{ij}\}$, $1\leq j\leq\tau(i)$ and suppose that the arcs $\{e_{ij}\}$ are indexed so that $\Theta_A(\ e_{ij}\ )=e'_{ij}$. Denote by w_{ij} the initial point of e_{ij}. Then $\Theta_V(\ w_{ij}\ )=w'_{ij}$ because Θ, as a map of graphs, carries initial points to initial points and end points to end points. Assumption (iv) allows us to conclude that $\tau(i)=\tau'(i)$ and

$$C'\#(\ w'_i;x_1,\ldots,x_{\tau(i)}\ )=C\#(\ w_i;x_1,\ldots,x_{\tau(i)}\ ).$$

Because of assumption (ii), $\sigma'(\ w'_{ij}\ )=\sigma(\ w_{ij}\ )$.

Let $a=(a_1,\ldots,a_\alpha)$. Assumption (i) asserts that the map Θ_V carries the array $(v_1,\ldots,v_\alpha)$ onto the array $(v'_1,\ldots,v'_\alpha)$. Therefore

$(I(\ a\ )\sigma\ )(\ v_i\ )=a_i$ and $(\ I(\ a\ )\sigma'\ )(\ v'_i\ )=a_i$.

Because $\sigma'(\ \Theta_V(\ v\ )\ )=\sigma(\ v\ )$, for each vertex v of G in the set of vertices $\{w_{ij},\ w_i\}$, $1\leq i\leq\alpha$, $1\leq j\leq\tau(i)$,

$(\ I(\ a\ )\sigma'\ )\Theta(\ v\ )=(\ I(\ a\ )\sigma\ )(\ v\ )$.

Because of condition (ii) of Definition C.10 the transformation of states C′ carries $I(\ a\ )\sigma'$ to the

state $C'(I(a)\sigma')$ that has value on w'_i,

$$C'\#(w'_i;(I(a)\sigma')(\beta(\Theta_A(e_{i1}))) ,\ldots,$$
$$(I(a)\sigma')(\beta(\Theta_A(e_{i\tau(i)}))))=$$
$$C\#(w_i;(I(a)\sigma)(\beta(e_{i1})),\ldots,$$
$$(I(a)\sigma)(\beta(e_{i\tau(i)}))).$$

This establishes the assertion of the lemma for walks of length t=1.

Assume that the lemma is true for all Θ, C, and C', and walks of length $t<L$. Assume that conditions (i)-(v) are satisfied for t=L. As before, the input vertices of C' are v'_i, $1\le i\le\alpha$, and the input vertices of C are v_i, $1\le i\le\alpha$. Let the output vertices of C be $\{w_j:1\le j\le\beta\}$ while the output vertices of C' are $\{w'_j;1\le j\le\beta\}$. Denote by e'_{ij}, $1\le j\le\tau(i)$, the collection of arcs of G' that have end point w'_i. Denote by w'_{ij} the initial point of the arc e'_{ij}. Then w'_i is the end point of a walk of length t. Indeed, if W is a walk that ends in w'_i, the initial vertex of the walk W is not a leaf and therefore the initial vertex of the walk W is the end point of an arc. It follows that there is a walk of length at least one larger than the length of W with end point w'_i. It follows that there are walks ending in w'_i that have as length each integer greater than zero. Because w'_i is the end point of a walk of length t and because of the assumption (iii) of the lemma, Θ_A is an onto map from the arcs that end in w_i

to the arcs that end in w'_i. Set $e'_{ij}=\Theta_A(\ e_{ij}\ )$ and set $w'_{ij}=\Theta_V(\ w_{ij}\ )$. Construct from G a new input-output digraph G*. The arcs and vertices of G* are the same as the arcs and vertices of G. The output vertices of G* are the array

$$(w_{11},\cdots,w_{1\tau(1)},\cdots,w_{\beta'1},\cdots,w_{\beta'\tau(\beta')}).$$

The input vertices of G* are the input vertices of G. Similarly, construct a new input-output digraph G" derived from G′ by designating as output vertices of G" the array

$$(w'_{11},\cdots,w'_{1\tau(1)},\cdots,w'_{\beta'1},\cdots,w'_{\beta'\tau(\beta')}).$$

The state σ of G is also a state of G*, while the state σ' of G′ is a state of G". The map Θ is also a map from G* to G" that satisfies the conditions (i)-(v) of the statement of the lemma, when L-1 is used for the value of t. Condition (v), when t=L-1, follows from the following observation. If W′ is a walk in G" of length L-1 that ends in w'_{ij}, then that walk can be extended to a walk of length L ending in w'_i by attaching to W′ the arc that connects w'_{ij} to the vertex w'_i. This new walk is the image of a walk W in G of length L, because of the hypothesis (v) is assumed true for t=L. The walk through the first L-1 arcs of W are mapped by Θ to the walk W′. Therefore, condition (v) is satisfied by the map Θ from G" to G* and for the transformations of states C and C′. By the inductive

hypothesis, for each $1 \le i \le \beta'$ and $1 \le j \le \tau(i)$,

$$(\{C \cdot I(\ a\ )\}^{L-1}\sigma)(\ w_{ij}\ ) =$$

$$(\{C' \cdot I(\ a\ )\}^{L-1}\sigma')(\ w'_{ij}\ ).$$

To find the result of applying $\{C \cdot I(\ a\ )\}^{L}$ to the state σ,

$$\{C \cdot I(\ a\ )\}^{L}\sigma = (C \cdot I(\ a\ ))\{(C \cdot I(\ a\ )\}^{L-1}\sigma,$$

with a similar assertion for $\{C' \cdot I(\ a\ )\}^{L}$. Therefore, we examine the effect that $C \cdot I(\ a\ )$ and $C' \cdot I(\ a\ )$ have on the states $\{C \cdot I(\ a\ )\}^{L-1}\sigma$ and $\{C' \cdot I(\ a\ )\}^{L-1}\sigma'$, respectively.

Condition (iv) guarantees that the function

$$C\#(\ w_i; x_{i1}, \ldots, x_{i\tau(i)}\ )$$

is the same as the function

$$C'\#(\ w'_i; x_{i1}, \ldots, x_{i\tau(i)}\ ).$$

Set

$$[C \cdot I(\ a\ )\sigma](\ w_{ij}\ ) = b_{ij}.$$

Then,

$$[C \cdot I(\ a\ )\sigma](\ w_i\ ) = C\#(\ w_i; b_{i1}, \ldots, b_{i\tau(i)}\ ) =$$

$$C'\#(\ w'_i; b_{i1}, \ldots, b_{i\tau(i)}\ ) =$$

$$[\{C' \cdot I(\ a\ )\}^{L}\sigma'](\ w'_i\ ).$$ ▒

When T is an in-tree, unless otherwise stated, we shall treat T as an input-output graph with the leaves of T as input vertices and with the root of T as output vertex.

Note that for an in-tree, the length of T is the

length of the longest path from a leaf to the root and it is also the length of the longest walk in T.

Lemma C.2. Let T be an in-tree with α leaves $(v_1,\ldots,v_\alpha)$ and let C be a (r,d)-network with input-output graph T. Let T have length L. For each state σ in S(T), each $a=(a_1,\ldots,a_\alpha)$ and each $j>L$,

$$\{C\cdot I(\ a\ )\}^j\sigma=\{C\cdot I(\ a)\}^{j+1}\sigma.$$

Proof. We proceed by induction on the length of T. If T has length 1 with root R, then each leaf v_i must be attached to the root R by an arc e_i. By the definition of a d-valued transformation of states,

$$[C\cdot I(\ a\ )\sigma](\ R\ )=C\#(\ R;a_1,\ldots,a_\alpha\ )$$

and

$$C\cdot I(\ \alpha\ )(\ v_i\ )=a_i.$$

Therefore,

$[\{C\cdot I(\ a\ )\}^2\sigma](\ R\ )=[(C\cdot I(\ a\ ))(C\cdot I(\ a\ ))\sigma](\ R\ )$. But $C\cdot I(\ a\ )\sigma=\sigma'$ is the state with in which $\sigma'(\ v_i\ )=a_i$ and in which $\sigma'(\ R\ )=C\#(\ R;a_1,\ldots,a_\alpha\ )$. Therefore

$$[\{C\cdot I(\ a\ )\}^2\sigma](\ v_i\ )=a_i=[C\cdot I(\ a\ )\sigma](\ v_i\ )$$

and

$$[C\cdot I(a)^2\sigma](\ R\ )=C\#(\ R;a_1,\ldots,a_\alpha\ )=$$
$$[C\cdot I(\ a\ )\sigma](\ R\ ).$$

Suppose the lemma is true for each in-tree of length at most L. Assume that T has length L+1. Denote by $e_1,\ldots,e_r$, the arcs that have common end