DISCUSSION PAPER NO. 168

# ON THE INFORMATIONAL SIZE OF MESSAGE SPACES

by

Mark Walker

August 1975

# ON THE INFORMATIONAL SIZE OF MESSAGE SPACES

by

Mark Walker

State University of New York
Stony Brook

In several recent papers, [1-4], K.Mount and S.Reiter have studied procedures for allocating resources, and they have made the informational properties of the procedures a central part of their investigation. They have described how, in order for a comparison of the informational properties of alternative procedures to be meaningful, some sort of restriction must be placed on the procedures' communication rules -- a restriction which will reflect the practical impossibility of conveying an "arbitrarily large amount" of information in an "arbitrarily small" message. We want to disallow, for example, such rules as a continuous parametrization of a cube -- a "space-filling curve" -- which would allow one to "use the unit interval to describe a cube." Mount and Reiter have proposed that we regard as "admissible" only those procedures which satisfy a certain regularity condition -- a formal version of the idea expressed in the preceding sentence -- and which are "privacy-preserving" (i.e., which do not require too much direct knowledge on the part of the individuals involved). They have restricted their consideration to just the admissible procedures, and have investigated several important implications of that restriction.

In [1], a definition of informational size was developed for topoligical spaces, and it was shown that, over a reasonably broad class of economic environments, any admissible procedure which can duplicate the performance of the competitive procedure must have a space of equilibrium messages which is at least as large as the competitive one. In other words, the competitive procedure is, in a certain sense, the most efficient of all the admissible procedures. This "optimality" of the competitive procedure was demonstrated in both a global context and a local context. It will be shown in this note that the global result in [1] is untenable, but that the local result there is actually equivalent to an interesting alternative global result.

Let us begin with some notation. Let $n$ and $\ell$ be positive integers ($n$ is interpreted as the number of economic agents, and $\ell$ as the number of goods). The theory is trivial and uninteresting if $n = 1$, but the results are also quite different in that case than when $n \neq 1$, so we let $n \geq 2$. Let $S$ be the "open" unit simplex in $R^{\ell}$. Let $E$ be the set of all pairs $e = (\alpha,\omega)$, where $\alpha, \omega \in R^{\ell}$, and where $\alpha_j > 0$ and $\omega_j \geq 0$ $(j = 1, \ldots, \ell)$ ($\alpha$ is interpreted as the representation of a Cobb-Douglas utility function $u(x) = \Pi_{i=1}^{\ell} x_i^{\alpha_i}$; $\omega$ is interpreted as an initial endowment; and $e = (\alpha,\omega)$ is interpreted as the description of a (Cobb-Douglas) economic agent). An n-tuple $e = (e^1, \ldots, e^n) \in E^n$ is called a Cobb-Doublas exchange environment. Both $S$ and $E$ are endowed with their usual (Euclidean) topologies. It is easy to show that we may take $E$ to be $S \times R_+^{\ell}$ without loss of generality.

A pair $(p,y) \in S \times \mathbb{R}^{n\ell}$ is a competitive equilibrium for the environment $e \in E^n$ if (a) for each $i(i = 1,\dots,n)$, $y^i \in \mathbb{R}^{\ell}$ is the net demand generated (in the competitive procedure) by $e^i$ and prices $p \in S$; and (b) $\Sigma_{i=1}^n y^i = 0 \in \mathbb{R}^{\ell}$. We denote the competitive equilibrium correspondence by $\bar{\mu}:E^n \twoheadrightarrow S \times \mathbb{R}^{n\ell}$, and its coordinates by $\sigma:E^n \twoheadrightarrow S$ and $\rho:E^n \twoheadrightarrow \mathbb{R}^{n\ell}$; i.e., for each $e \in E$: [1]

$$\bar{\mu}(e) = \{(p,y) \mid (p,y) \text{ is a competitive equilibrium for } e\},$$

$$\sigma(e) = \{p \in S \mid \exists y \in \mathbb{R}^{n\ell} : (p,y) \in \bar{\mu}(e)\},$$

$$\rho(e) = \{y \in \mathbb{R}^{n\ell} \mid \exists p \in S: (p,y) \in \bar{\mu}(e)\}.$$

Finally, let $\bar{M}$ denote the (equilibrium) message space of the competitive procedure: $\bar{M} = \mu(E^n)$.

Now let us briefly review the relevant results from [1]. Mount and Reiter first establish that the equilibrium (or one-iteration) representation of the competitive procedure is itself an admissible procedure.

THEOREM 1: [2] Let $\bar{\bar{g}}: S \times \mathbb{R}^{n\ell} \to \mathbb{R}^{n\ell}$ be the projection of $S \times \mathbb{R}^{n\ell}$ onto $\mathbb{R}^{n\ell}$, and let $\bar{g}: \bar{M} \to \mathbb{R}^{n\ell}$ be the restriction of $\bar{\bar{g}}$ to $\bar{M}$. Then $(\bar{\mu},\bar{g})$ is a privacy-preserving procedure [3] which realizes $\rho$, and which uses the message space $\bar{M}$.

[1] Notice that $\bar{\mu}, \sigma$, and $\rho$ are each single-valued on all of $E^n$, and that they are thus functions on $E^n$.

[2] This is a conjunction of several statements in [1].

[3] See the Appendix for definitions of terms given in [1].

The major results in [1] have to do with the sizes of the message spaces of procedures which could be used to realize the same performance as the competitive procedure. The notion that one space is larger, or can convey more information, than another, is given formal expression by Mount and Reiter in the following definition. Examples and discussion, which may help to illuminate the definition, will be provided shortly (see also [5], and pages 173-180 of [1]).

<u>Definition 1:</u>[4] A space $X$ has as much information as a space $Y$, which we denote by $X \trianglerighteq Y$,[5] if there is a continuous, locally sectioned[6] (c.l.s.) surjection from $X$ to $Y$.

It is easy to verify that $\trianglerighteq$ is both a quasi-ordering (reflexive and transitive)of the class of all topological spaces, and a topological invariant (homeomorphic spaces are the same size), as we would expect a notion of "size" to be.

Using Definition 1, Mount and Reiter obtain the following statements about the informational efficiency of the competitive procedure, when applied only to Cobb-Douglas exchange economies.

[4] This is Definition 9 in [1].

[5] For any quasi-ordering $\geq$, we will, as is customary, denote "$X \geq Y$ and $Y \ngeq X$" by $X > Y$, and "$X \geq Y$ and $Y \geq X$" by $X \equiv Y$.

[6] See Definition A2 in the Appendix.

THEOREM 2:[7] If $(\mu, g)$ is a privacy-preserving procedure which uses the message space $M$ to realize $\rho$, and if $\mu^{-1}$ is upper-semicontinuous,[8] then $M \geqq \bar{M}$.

THEOREM 3:[9] If $(\mu, g)$ is a privacy-preserving procedure which uses a Hausdorff message space $M$ to realize $\rho$, then a subset of $M$ is locally homeomorphic to $\bar{M}$.

Theorems 2 and 3 refer only to Cobb-Douglas environments, and consequently they are not, by themselves, very interesting. The following "Inheritance Lemma", however, enables us to extend the results to a very broad class of environments, and in this larger context the results (Theorems $2^*$ and $3^*$ below) are quite impressive.

Definition 2: A property $\mathcal{P}$ of procedures is an inherited property if, whenever $(\mu, g)$ is a procedure defined on a space $X$, and $(\mu, g)$ has property $\mathcal{P}$, then the restriction $(\mu', g)$ of $(\mu, g)$ to a subspace $X'$ of $X$ is also a procedure which has property $\mathcal{P}$.

The following properties, for example, are clearly inherited: "$(\mu, g)$ is privacy-preserving," "$\mu$ is single-valued," and "$\mu$ is upper-semicontinuous." Notice that these are all properties which the procedure $(\bar{\mu}, \bar{g})$ possesses.

[7] This is Theorem 31 in [1].

[8] This is Theorem 35 in [1].

[9] In [1] this condition was "$\mu$ is u.s.c.," but it was changed in [6] to "$\mu^{-1}$ is u.s.c." For more on this, see below.

Inheritance Lemma:[10] Let $(\mu, g)$ be a procedure which has an inherited property $\mathcal{P}$, and which uses the message space $M$ to realize the function $f\colon X \to Z$. If $X$ is a subspace of $X^*$, and $f$ is the restriction of $f^*\colon X^* \to Z$ to $X$, then any procedure with property $\mathcal{P}$ which realizes $f^*$ has a message space $M$ which satisfies $M \mathrel{\cdot\!\geq} \bar{M}$.

THEOREM $2^*$:[11] Let $\mathcal{E} = \Pi_{i=1}^{n}\mathcal{E}^i$, where, for each $i$, $\mathcal{E}^i$ is a superspace of $E$, and let $\rho^*\colon \mathcal{E}^* \to \mathbb{R}^{n\ell}$ be an extension of $\rho$. If $(\mu^*, g^*)$ is a privacy-preserving procedure which uses $M^*$ to realize $\rho^*$, and if $\mu^{*-1}$ is u.s.c., then $M^* \mathrel{\cdot\!\geq} \bar{M}$.

THEOREM $3^*$: If $(\mu^*, g^*)$ is a privacy-preserving procedure which uses $M^*$ to realize $\rho^*$, and if $M^*$ is Hausdorff, then there is a subspace of $M^*$ which is locally homeomorphic to $\bar{M}$.

Let us consider the global results, Theorems 2 and $2^*$, a bit more closely. In the original formulation of these results in [1], the condition "$\mu$ is u.s.c." was used, instead of "$\mu^{-1}$ is u.s.c." The property "$\mu$ is u.s.c." is inherited, of course, so there is no difficulty in applying the Inheritance Lemma, to obtain Theorem $2^*$ from Theorem 2. However, Theorem 2 itself is not true under the condition "$\mu$ is u.s.c." (this occasioned the change in [6] to "$\mu^{-1}$ is u.s.c."), and there is consequently

[10] This is Lemma 14 of [1].

[11] This is Corollary 34 of [1].

nothing to which the Inheritance Lemma can be applied. On the other hand, Theorem 2 is true if the condition "$\mu^{-1}$ is u.s.c." is used, but in this case the Inheritance Lemma cannot be applied, because "$\mu^{-1}$ is u.s.c." is not an inherited property. This does not show that Theorem $2^*$ is untrue, of course, but it certainly rules out the use of the Inheritance Lemma as a means of proof.

Can we, then, by some other means of proof, salvage Theorem $2^*$? The following example indicates that we cannot; further, it indicates that the condition "$\mu^{-1}$ is u.s.c." is simply not a reasonable restriction to place on procedures.

Example 1: Let $n = \ell = 2$, and define two Cobb-Douglas exchange economies, $\bar{e}$ and $\hat{e}$, as follows:

$$\bar{\alpha}^1 = \bar{\alpha}^2 = 1;\ \bar{\omega}^1 = \bar{\omega}^2 = (\tfrac{1}{2},\tfrac{1}{2});\ \bar{e}^i = (\alpha^i,\bar{\omega}^i),\ i = 1,2;$$

$$\text{and } \bar{e} = (\bar{e}^1,\bar{e}^2);$$

$$\hat{\alpha}^1 = \hat{\alpha}^2 = 1;\ \hat{\omega}^1 = (1,0),\ \hat{\omega}^2 = (0,1);\ \hat{e}^i = (\hat{\alpha}^i,\hat{\omega}^i),\ i = 1,2;$$

$$\text{and } \hat{e} = (\hat{e}^1,\hat{e}^2).$$

Notice that neither $\bar{e}$ nor $\hat{e}$ is a member of $E^2$. Let $\bar{p} = (1,0)$ and $\hat{p} = (\tfrac{1}{2},\tfrac{1}{2})$.

For each real number $\beta$ which satisfies $0 < \beta < 1$, define the Cobb-Douglas exchange economy $e(\beta)$ as follows:

$$\omega(\beta) = (1-\beta)\hat{\omega} + \beta\,\overline{\omega},$$

$$p(\beta) = (1-\beta)\hat{p} + \beta\,\overline{p},$$

$$\alpha^i(\beta) = \frac{p_1(\beta)\omega_1^i(\beta)}{p_1(\beta)\omega_1^i(\beta) + p_2(\beta)\omega_2^i(\beta)}\quad, \ i = 1,2,$$

$$e^i(\beta) = (\alpha^i(\beta),\omega^i(\beta)),\ i = 1,2, \text{ and } e(\beta) = (e'(\beta),e^2(\beta)).$$

Notice that, if $0 < \beta < 1$, then $e(\beta) \in E^2$; that $p(\beta)$ is the equilibrium price-list for $e(\beta)$ [i.e., $\sigma(e(\beta)) = p(\beta)$]; and that, for each $\beta$, "no trade" is the equilibrium trade.

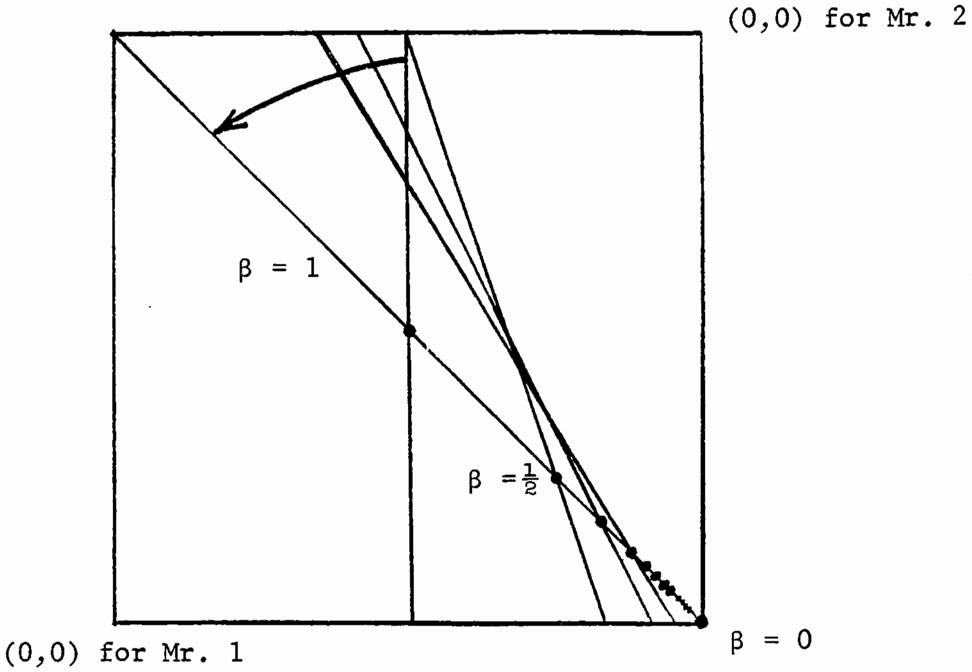

FIGURE 1

Figure 1 depicts an Edgeworth box representation of the endowment points $\omega(\beta)$ and the "price lines" for $p(\beta)$, for $\beta = \frac{1}{n}$ as $n = 1,2,\ldots$ As $\beta$ decreases from 1 to 0, $\omega(\beta)$ moves toward $\hat{\omega}$ in the lower right corner, and the price moves toward the price $\hat{p} = (\frac{1}{2},\frac{1}{2})$; but $\alpha^i(\beta)$ also moves toward $\hat{\alpha}^i = 1$ for $i = 1,2$, so that $e(\beta) \rightarrow \hat{e} \notin E^2$. We have sequences $p_n \rightarrow \hat{p} \in S$ and $e_n \rightarrow \hat{e} \notin E^n$, and $e_n \in \sigma^{-1}(p_n)$ for each $n$; adding the trade component, we have $(p_n,0) \rightarrow (\hat{p},0) \in \bar{M}$, $e_n \in \mu^{-1}(p_n,0)$ for each $n$, and $e_n \rightarrow \hat{e} \notin E^n$. Since $E^n$ is a complete metric space, this is sufficient to establish that $\mu^{-1}$ is not upper-semicontinuous at $(\hat{p},0)$.

The essential feature of the example is the possibility of constructing a sequence of environments in $E^n$ which converges to an environment not in $E^n$, while the equilibrium prices for the sequence converge to a price in $S$ (i.e., to a price which is an equilibrium for some environment). Recent results [7,8,] have demonstrated that, if $\mathcal{E}$ is a class of environments on which the equilibrium allocation correspondence $\rho^*$ is single-valued (as the definition of a procedure requires), and if $\mathcal{E}$ includes, say merely the smooth, strictly convex, strictly monotone environments, then such sequences can always be constructed (sequences for which the limit environment does not yield a unique equilibrium, and thus is not in $\mathcal{E}$). In other words, on any interesting class $\mathcal{E}$ of environments, the equilibrium message correspondence (function) of the competitive procedure itself has an inverse which is not u.s.c. [12]

[12] The example seems to indicate, in fact, that any procedure $(\mu,g)$ which has a single-valued correspondence cannot realize $\rho^*$ on $\mathcal{E}$ if $\mu^{-1}$ is u.s.c.

We have established, then, that the condition "$\mu^{-1}$ is u.s.c." is an unreasonable one to require that procedures satisfy; is there nevertheless some <u>other</u> way to save the global result? Is there any reasonable limitation on procedures which will yield $M {\cdot}\!\geqq \bar{M}$ for all procedures which realize $\rho$? The next example, a variation of the example of [1, page 189], shows that even in the very limited Cobb-Doublas case, there are "quite reasonable" procedures which realize $\rho$, but use message spaces $M$ which do not satisfy the condition $M {\cdot}\!\geqq \bar{M}$.

<u>Example 2:</u> Let $n = \ell = 2$, and let $C$ denote the unit circle in $\mathbb{R}^2$, with its usual topology. Let $h:S \to I$ be a homeomorphism from $S$ to $I$, the open unit interval in $\mathbb{R}$, and let $\eta : I \twoheadrightarrow C$ be the correspondence defined as follows:

$$\eta(x) = \begin{cases} \{\frac{3}{2}x\pi\}, \text{ if } x < \frac{1}{3}; \\ \{\frac{3}{2}x\pi, (\frac{5}{2} - x)\pi\}, \text{ if } \frac{1}{3} \leqq x \leqq \frac{2}{3}; \\ \{(\frac{5}{2} - x)\pi\}, \text{ if } x > \frac{2}{3}. \end{cases}$$

Define the procedure $(\mu, g)$, and its message space $M$, as follows:

$$\mu = \eta \circ h \circ \bar{\mu} : E^n \twoheadrightarrow C \times \mathbb{R}^{n\ell};$$

$$M = \mu(E^n);$$

$\hat{g}: C \times \mathbb{R}^{n\ell} \to \mathbb{R}^{n\ell}$ is the projection which maps each $(c,z) \in C \times \mathbb{R}^{n\ell}$ into its second component;

and $g:M \to \mathbb{R}^{n\ell}$ is the restriction of $\hat{g}$ to $M$.

The correspondence $\mu$ is privacy-preserving, locally threaded and continuous (both u.s.c. and l.s.c.); and the function $g$ is continuous and locally sectioned. The procedure $(\mu, g)$, then, is not a pathological one. It is not true, however, that $M \cdot\!\geq \bar{M}$; indeed, $M \cong S \times \mathbb{R}^k$, where $k = (n-1)(\ell-1)$, and hence $\bar{M} \cdot\!> M$.

It should be clear by now that with the quasi-ordering $\cdot\!\geq$, no meaningful global result of the form "the competitive procedure is best" is obtainable. This fact could be interpreted in either of two ways. On one hand, we could admit that the competitive procedure simply isn't a globally best procedure, even in such limited cases as the Cobb-Douglas exchange economies. Alternatively, we could investigate more deeply the concept of informational size; we might find, for example, that we are able to formalize the notion of informational size in a different way, and that this new formalization yields the expected result that the competitive procedure is informationally best. Regarding the second approach, it should be pointed out that the local result -- the only result we have at this point -- is not of the form "$(\bar{\mu}, \bar{g})$ uses a locally smallest message space," but rather of the form "any alternative procedure $(\mu, g)$ uses a message space M, a subspace of which is locally homeomorphic to $\bar{M}$." In other words, we have used our particular definition of informational size only as a tool, not as a concept in terms of which the result is stated. There is nothing in the results obtained so far, then, to single out one notion of informational size.

Let us take a closer look now at the concept of informational size for topological spaces. We will first consider several examples which will give us a bit of insight into the quasi-ordering $\dot{\geqq}$ of Definition 1. Let $\mathbb{R}$ be the set of real numbers; let $I$, $\dot{I}$, and $J$ be the intervals $[0,1]$, $[0,1]$ and $(0,1)$, respectively; let $I^n$ be the n-dimensional cube (n-fold product of $I$); let $C$ be the circle in $\mathbb{R}^2$; and let $Q$ be the set of all rational numbers. Let all of those sets be endowed with their usual topologies, and let $D$ be any finite (or indeed any countable) discrete space of more than one member. Then we have

$$R \overset{\bullet}{\equiv} J \cdot> \dot{J} \cdot> I \overset{\bullet}{\equiv} C,$$

$$I^n \cdot> I \overset{\bullet}{\equiv} C, \text{ and } Q \cdot> D,$$

as we would expect, but none of the remaining pairs is related by $\geqq$. In particular, $I^n \cdot\ngeqq \mathbb{R}$, $\mathbb{R} \cdot\ngeqq Q$, and $\mathbb{R} \cdot\ngeqq D$.

If $\geqq$ denotes a quasi-ordering which relates topological spaces in terms of their "size," then, on the face of it, it certainly seems reasonable to expect that $\mathbb{R} > D$, and even that $I^n > \mathbb{R}$ and $\mathbb{R} > Q$, or at least $\mathbb{R} \geqq Q$. Going a bit further in the same vein, we might even be led to expect that whenever one space is a subspace of another, say $S \subseteqq X$, then the spaces will stand in the relation $S \leqq X$. This principle, together with the ideas underlying Definition 1, leads us to the following definition.

<u>Definition 3:</u> $X \geqq_S Y$ if and only if there is a subspace $X'$ of $X$ for which $X' \cdot\geqq Y$.

It is immediate that $X \cdot\geqq Y$ implies $X \geqq_S Y$. In other words, the relation $\geqq_S$ is nothing but an enlargement of $\cdot\geqq$: some pairs of spaces previously non-comparable (using $\cdot\geqq$) will now stand in the relation $\geqq_S$ (or $\equiv_S$) to one another, and some which were previously in the relation $\cdot>$ will now be the same size. The relation $\geqq_S$ is still a quasi-ordering of topological spaces, with homeomorphic spaces still the same size; indeed, it is the smallest quasi-ordering which both includes $\cdot\geqq$ and also satisfies the condition that $X \subseteqq Y$ implies $X \leqq Y$.

We are going to find it very helpful to introduce several more quasi-orderings, each of which captures some apsect of the notion of "size."

<u>Definition 4:</u>

a) $X \geqq_C Y$ means that $|X| \geqq |Y|$, i.e. that the cardinal number of $X$ is as large as the cardinal number of $Y$.

b) $X \geqq_D Y$ means that $\dim X \geqq \dim Y$; this relation is defined only when both $X$ and $Y$ are separable metric spaces.

c) $X \geqq_F Y$ (for "Frechet size") means that $Y$ can be imbedded homeomorphically in $X$, i.e., there is a subspace $X'$ of $X$ for which $X' \cong Y$.

d) $X \geqq_{LH} Y$ means that a subspace of $X$ is locally homeomorphic to $Y$; i.e., there is a subspace $X'$ of $X$ such that, for each point $p \in X'$ [resp., $q \in Y$], there is a neighborhood $U$ of $p$ [resp., $V$ of $q$] which is homeomorphic to a subspace of $Y$ [resp., $X'$].

The following diagram depicts the relationships among the quasi-orderings we have defined. It is straightforward to verify each of the implications in the diagram, and it is easy to give examples which demonstrate that none of the implications is reversible.

$$\begin{tikzcd}
 & X \cong Y \arrow[dl, Rightarrow] \arrow[dr, Rightarrow] & & \\
X \geqq Y \arrow[dr, Rightarrow] & & X \geqq_F Y \arrow[dl, Rightarrow] & \\
 & X \geqq_S Y \arrow[d, Rightarrow] & & \\
 & X \geqq_{LH} Y \arrow[dl, Rightarrow] \arrow[dr, Rightarrow] & & \text{(if } X,Y \text{ separable metric spaces)} \\
X \geqq_C Y & & X \geqq_D Y &
\end{tikzcd}$$

With our enlarged definition of informational size, $\geqq_S$, we are able to obtain a very nice version of the global results 2 and $2^*$: the only condition, beyond admissibility, which is required of procedures is that their message spaces be Hausdorff; and the local results follow from the global ones as simple corollaries.

<u>THEOREM 4:</u> Let $(\mu, g)$ be a privacy-preserving procedure which realizes $\rho$ and which uses the message space $M$. If $M$ is Hausdorff, then $M \geqq_S \overline{M}$.

<u>Proof</u>:

Let $\varphi = \overline{\mu} \circ \mu^{-1}: M \twoheadrightarrow \overline{M}$. That $\varphi$ is a function is established in [1], in the proof of Theorem 31. We will construct a subspace $M'$ of $M$ on which the restriction $\varphi': M' \rightarrow \overline{M}$ is a c.l.s. surjection.

It can be shown, much as Mount and Reiter do in their proof of Theorem 35 of [1], that $\varphi^{-1}$ is locally threaded and that, for each $m \in \overline{M}$, the local thread $r_m: N_m \rightarrow M_m$ is a homeomorphism of a neighborhood of $m$ with a neighborhood $M_m$ of some $x \in \varphi^{-1}(m)$. We then let $M' = \bigcup_{m \in \overline{M}} M_m$; we have constructed $M'$ in such a way that $\varphi': M' \rightarrow \overline{M}$ (the restriction of $\varphi$ to $M'$) is onto $\overline{M}$ and is locally sectioned. In order to see that $\varphi'$ is continuous as well -- that is, that $\varphi$ is continuous on $M'$ -- we let $x \in M'$. Then there is an $m \in \overline{M}$ for which $M_m$ is a neighborhood of $x$; and the restriction of $\varphi$ to $M_m$ is just the continuous function $r_m^{-1}$. ||

Since the only properties we require of procedures are (a) that they be privacy-preserving, (b) that their message correspondences be locally threaded, and (c) that their message spaces be Hausdorff, and since each of those properties is inherited, then the Inheritance Lemma immediately yields the more extensive Theorem $4^*$.

THEOREM $4^*$: Theorem 4 also applies to any extension $\rho^*: \mathcal{S} \to \mathbb{R}^{n\ell}$ of $\rho$ to a superspace $\mathcal{S}$ of $E^n$.

We have already mentioned that the local results, Theorems 3 and $3^*$, are simple corollaries of Theorems 4 and $4^*$; in fact, Theorem 4 also follows as an easy consequence of Theorem 3. The two theorems are equivalent.[13/] The crucial facts here are, first, that $\overline{M}$ is homeomorphic to $\mathbb{R}^m$, where $m = (\ell - 1)n$, and second, that each neighborhood in $\mathbb{R}^m$ contains a subset which is homeomorphic to $\mathbb{R}^m$. Hence, the following lemma and theorems are obvious.

Lemma : If $M \geqq_{LH} \overline{M}$, then $M \geqq_F \overline{M}$.

THEOREM 5: Let $(\mu, g)$ be a privacy-preserving procedure which realizes $\rho$ and which uses the message space $M$. If $M$ is Hausdorff, then $M \geqq_F \overline{M}$ -- i.e., $\overline{M}$ can be imbedded homeomorphically in $M$.

THEOREM $5^*$: Theorem 5 also applies to any extension $\rho^*: \mathcal{S} \to \mathbb{R}^{n\ell}$ of $\rho$ to a superspace $\mathcal{S}$ of $E^n$.

[13/] Strictly speaking, then, the proof provided above for Theorem 4 is superfluous. It was included to demonstrate how one would work with $\geqq_S$ in the general case -- when $\overline{M}$ is not a finite-dimensional Euclidean space.

Summarizing, the three statements $M \geqq_F \bar{M}$, $M \geqq_S \bar{M}$, and $M \geqq_{LH} \bar{M}$ are all equivalent to one another, and hence Theorems 3, 4 and 5 are equivalent, as are Theorems $3^*$, $4^*$, and $5^*$.

The following example shows that we cannot dispense with the condition that the message space be Hausdorff.

Example 3: Let $A$ be the simplex $S$, with the cofinite topology (the proper closed subsets of $A$ are precisely the finite subsets) instead of the usual (Euclidean) topology. Let $(\mu, g)$ be the procedure which differs from $(\bar{\mu}, \bar{g})$ only in substituting the space $A$ for $S$ in its message space. In other words, where $\bar{\mu}$ maps $E^n$ onto $\mu(E^n) = \bar{M} \subseteqq S \times \mathbb{R}^{n\ell}$, we have $\mu(e) = \bar{\mu}(e)$ for each $e \in E^n$ (hence, as sets, $M = \bar{M}$, but they have different topologies); and where $\bar{g}$ maps $\bar{M}$ into $\mathbb{R}^{n\ell}$, we have $g$ mapping $M$ into $\mathbb{R}^{n\ell}$, with $g(\rho, y) = \bar{g}(\rho, y) = y$, for each $(\rho, y) \in M$.

The space $M$ is a $T_1$-space ("points are closed"); it is "almost, but not quite" Hausdorff. It is not true that $M \geqq_F \bar{M}$; if it were true, then a subspace of $M$ (and thus a subspace of $A \times \mathbb{R}^{m-(\ell-1)}$) would be a homeomorphic to $\mathbb{R}^m$, which is clearly impossible. Of course, neither $M \geqq_S \bar{M}$, $M \geqq \bar{M}$, nor $M \geqq_{LH} \bar{M}$ can be true, either.

However, $(\mu, g)$ is quite a reasonable procedure in nearly every other respect: it is privacy-preserving; $\mu$ is locally threaded; in fact, $\mu$ is a continuous function.[14] $(\mu, g)$ satisfies very strong conditions,

[14] The function $\mu$ is not locally sectioned, but this is too much to hope for here: since $\mu$ and $\bar{\mu}$ are identical as functions, if $\mu$ were locally sectioned then $M$ and $\bar{M}$ would be homeomorphic (see [10]).

but has a message space which is not quite Hausdorff, and the relation $M \geqq_F \bar{M}$ fails to hold.

Finally, some interesting questions about this approach remain unresolved. First, although we cannot be sure that $M \geqq_F \bar{M}$ when $M$ is not Hausdorff, it still might be true that $M$ cannot be strictly smaller than $\bar{M}$. In other words, is it still true that $\bar{M}$ is minimal (although not smallest) when we admit non-Hausdorff spaces?

A second open question arises from Example 2. Although it is decidedly non-pathological in every other respect, the procedure there differs in one important way from the competitive procedure. The message correspondence $\bar{\mu}$ is single-valued, but the correspondence $\mu$ of Example 2 is, for some members of its domain, doubleton-valued. Suppose that we require that the message correspondence be a function; can we then achieve stronger results -- e.g., $M \cdot\!\geqq \bar{M}$, as in Theorems 2 and $2^*$. I would conjecture that the answer is "no" (in other words, that a single-valued analogue of Example 2 exists), if we do not require that the message function be locally sectioned; if we include the latter requirement, then the result $M \cdot\!\geqq \bar{M}$ follows from a fundamental result on cls functions. [15]

If we focus attention on message functions, in contrast to correspondences, we raise a third unresolved question, which is couched in terms of the following definition. The relation $X \geqq_A Y$ in the definition can be paraphrased as "anything $Y$ can do, $X$ can do."

Definition 5: $X \geqq_A Y$ if, for every composition $g \circ f : E \to A$ of cls functions $f : E \to Y$, and $g : Y \to A$, there are cls functions $f' : E \to X$ and $g' : X \to A'$, and an imbedding $i : A \to A^{i}$, such that $g' \circ f' = i \circ g \circ f$. In other words, for every "cls diagram" $E \xrightarrow{f} Y \xrightarrow{g} A$, there is a cls diagram $E \xrightarrow{f'} X \xrightarrow{g'} A'$ and an imbedding $i : A \to A'$ such that the following diagram commutes:

$$\begin{tikzcd}
 & & X \arrow[dr, "g'"] & \\
E \arrow[urr, "f'"] \arrow[r, "f"'] & Y \arrow[r, "g"'] & A \arrow[r, "i"'] & A'
\end{tikzcd}$$

If the relation $X \geqq_F Y$ holds, must $X \geqq_A Y$ hold as well? If so, then Theorems 5 and $5^*$ yield a proposition of the following form: if $(\mu, g)$ is a procedure which uses a message space $M$ and which realizes the same performance as the competitive procedure, then any performance which can be realized with $\bar{M}$ can also be realized with $M$.

[15] See [9].

# APPENDIX

The following definitions, which appear in [1], are used in this paper.

Definition A1 (Definition 6, p. 173, [1]): A correspondence $\mu: X \twoheadrightarrow Y$ is locally threaded if, for each $p \in X$, there is a neighborhood $U$ of $p$ and a continuous function $t: U \to Y$, called a p-local thread of $\mu$, for which $t(x) \in \mu(x)$ for each $x \in U$.

Definition A2 (Definition 7, p. 173, [1]): A function $f: X \to Y$ is locally sectioned if the correspondence $f^{-1}: Y \twoheadrightarrow X$ is locally threaded; a continuous and locally sectioned function will be referred to as a c.l.s. function.

Definition A3(Definition 1, p. 169, [1]): Let $X$, $M$, and $Z$ be given spaces, and $f: X \to Z$ a function. A pair $(\mu,g)$ is a procedure which realizes $f$, and uses the "message space" $M$, if

(i) $\mu: X \twoheadrightarrow M$ is a locally threaded correspondence on $X$ into $M$;

(ii) $g: M \to X$ is a c.l.s. function on $M$ into $Z$;

(iii) for each $x \in X$, $g$ is constant on $\mu(x)$, and has value $f(x)$.

Definition A4 (Definition 2, p. 170, [1]): Let $X = \Pi_{i=1}^{n} X_i$. A correspondence $\mu: X \twoheadrightarrow Y$ is a coordinate correspondence if there are correspondences $\mu_i: X_i \twoheadrightarrow Y$ $(i = 1, \ldots, n)$ such that, for each $x \in X$, $\mu(x) = \bigcap_{i=1}^{n} \mu_i(x_i)$.

Definition A5 (Definition 3, p. 170, [1]): Let $X = \Pi_{i=1}^{n} X_i$, M, and Z be given spaces, and let $(\mu, g)$ be a procedure which realizes f and uses M. We say that $(\mu, g)$ preserves privacy if $\mu$ is a coordinate correspondence.