Discussion Paper No. 938

SUFFICIENT STATISTICS, UTILITY THEORY, AND MECHANISM DESIGN

by

Donald G. Saari*

May 1991

*Departments of Mathematics and Economics, Northwestern University, Evanston, IL 60208.

SUFFICIENT STATISTICS, UTILITY THEORY, AND MECHANISM DESIGN

DONALD G. SAARI

Northwestern University; Departments of Mathematics and of Economics

ABSTRACT. It is shown how bordered hessians, sufficient statistics, and integrability conditions from utility theory are closely related to the characterization theorems for mechanism design. Then, new results are outlined about a theory for implicitly defined objective functions, about how to incorporate different kinds of information sets modeling, say, externalities into the theory, and about the actual construction of economic mechanisms.

Risking frostbite while standing outside on a cold Evanston day during the winter of 1977, Stan Reiter introduced me to the fascinating area of mechanism design. He posed a seemingly straightforward mathematical question about the composition of mappings. The motivation for his query derived from the now standard Mount-Reiter diagram ([MR])

(1.1)
$$\begin{tikzcd}
\Omega \subset \prod_{j=1}^{n} R^{k_j} \arrow[r, "P"] \arrow[d, "\mu_1 \cdots \mu_n"'] & R^a \\
M \arrow[ur, "h"'] &
\end{tikzcd}$$

which succinctly captures the issues of mechanism design issues introduced by L. Hurwicz $[H_1]$.

In the diagram, $P : \Omega \subset \prod_{j=1}^{n} R^{k_j} \rightarrow R^a$ represents the objective or performance function (a resource allocation, a choice function, etc.). To illustrate, suppose $\mathbf{x}_j \in R^{k_j}$ denotes the jth agent's characteristics; e.g., some of the components of $\mathbf{x}_j$ identify the Cobb-Douglas exponents for the utility function while the remaining components specify the initial endowment. In this way $\mathbf{X} = (\mathbf{x}_1, \cdots, \mathbf{x}_n)$ represents an economy and $P(\mathbf{X})$ designates a specified allocation; e.g., the Walrasian allocation. In general the objective mapping $P(\mathbf{X})$ is used to represent a goal, an objective, or even a basic philosophy.

This paper was written for a volume honoring Stan Reiter that is being edited by John Ledyard. I would like to thank Stan Reiter and Leo Hurwicz for introducing me to this area, and the two of them along with Ken Mount for the many delightful discussions about these issues of mechanism design. All three, of course, are among the original pioneers of this area. This research was supported by NSF Grant IRI-8803505 as well as earlier NSF IRI grants .

After an objective is specified, how is it to be realized? This is the problem of mechanism design. The solution is to define an appropriate organizational structure, or communication network among the agents. Such a construction involves determining "who should say what to whom." Namely, the jth agent needs to convey appropriate information to the other agents about her characteristics $\mathbf{x}_j$. "What" the jth agent tells the other agents is her message; in the MR diagram, this is represented by the mapping (or correspondence) $\mu_j(\mathbf{x}_j)$. The restriction that each agent's message depends on her characteristics and only indirectly (through communicated messages) on other agents characteristics is the *privacy preserving condition.* Using the *message space* $M = \{m = (m_1, \ldots, m_\beta)\}$, the correspondence μ_j often is represented implicitly by

$$\mu_j(\mathbf{x}_j) = \{m \in M | G_j(m, \mathbf{x}_j) = (g_1^j(\mathbf{x}_j, m), \ldots, g_{\alpha_j}^j(\mathbf{x}_j, m)) = \mathbf{0}\} \tag{1.2}$$

where $\alpha_j \leq k_j$ is an integer.

After appropriate information is gathered from the agents, decisions are made and action taken; this is the mapping h. If the right kind of organization is defined, the action realizes the goal; i.e., $h(m) = P(\mathbf{X})$ and the MR diagram commutes.

As an atypical but illustrative example, consider voting and choice theory. Here, the jth agent's characteristics $\mathbf{x}_j$ represent a preference ranking of the $n \geq 2$ candidates. In this model, a precise performance function may not be specified; instead $P(\mathbf{X})$ reflects a specified philosophy; e.g., the group's ranking of the candidates represents the "true wishes of the voters." Each voter's message is the way he or she marks the ballot; the mapping $h(m)$ is the election ranking resulting from a tally of the ballots. Whether or not the diagram commutes determines whether or not the process truly captures "the wishes of the voters."[1] As such, by using different objectives for P, the MR diagram forms a convenient encapsulation of the various themes from voting and choice theory.

In more typical examples, $P(\mathbf{X})$ is explicitly defined; e.g., $P(\mathbf{X})$ may be the Walrasian allocation. One message system that realizes this $P(\mathbf{X})$ is the usual price model where the excess demand vector at each price is an agent's message and h is the assignment of net trades at equilibrium. Alternatively, one could use the *complete disclosure organization* where each agent completely discloses all of his defining characteristics and then h (the central agent?) computes the Walrasian allocation. In general, if P can be realized by one organization, it can be realized by many different organizations.

So, for a given P, the idea is to find, or at least to characterize, all possible associated organizations; i.e, the mechanism design problem is to start with the specified objective function $\prod_{j=1}^n R^{k_j} \xrightarrow{P} R^a$ and then characterize all organizations that correspond to the rest of the MR diagram. This requires finding all ways in which a given mapping, P, can be factored into a composition

$$P(\mathbf{X}) = h(\mu_1(\mathbf{x}_1), \cdots, \mu_n(\mathbf{x}_n)). \tag{1.3}$$

A natural issue arises; if many different organizations can realize P, how does one select among them? It is not difficult to see that, in a real sense, the dimension of M

[1] An "impossibility theorem" is where no mechanism exists for a specified objective P.

forms a crude but useful measure of the efficiency of the associated organization.[2] After all, a larger dimensional M implies that more kinds of messages need to be communicated before appropriate action can be taken. For instance, the staggering informational requirements associated with complete disclosure are manifested by the large dimension of the associated message space.

We now can explain Reiter's question to me about composing functions (Eqs. 1.1, 1.3) to minimize the dimension of a message space; he was interested in determining the minimal dimension of a message space [MR] associated with an arbitrary but specified performance function P. As he posed the problem, it seemed to be straightforward. As I quickly learned, one must never confuse the clarity of Stan's questions with the potential simplicity of solution. Several months later, joined in our discussions by Leo Hurwicz, we developed such a theory [HRS] in terms of differential geometric tools.

A couple of years later I developed a dual approach ($[S_{1,2,3,4}]$) to the HRS theory that, in several ways, provides a conceptually simpler approach to understand and to resolve certain basic issues. For instance, this dual approach easily can be modified to model other kinds of communication networks $[S_4]$. Also, with this approach answers can be found for certain types of mechanism design questions such as determining the "kind of information" about agents' characteristics needed to realize a particular performance function, how to develop a theory for implicitly defined objective functions (which arise in economics through "optimality" considerations), how to adjust the theory when the privacy preserving constraint is modified to include models of externalities or from game theory, etc.

While this dual approach has advantages, it is based on differential ideals and other mathematical tools not widely used in economics. So in this paper these mathematical ideas are introduced in terms of concepts more traditionally used in economics. In this manner I relate this dual approach to sufficient statistics, to the bordered hessian, and to the classical integrability conditions from revealed preference theory. Then I motivate some new results; details will appear elsewhere.

2. Sufficient Statistic and Mechanism Design

It is instructive to compare the problems of mechanism design with the related issues confronting a statistician charged with the design of an estimator $\hat{\theta}$ for a parameter $\theta \in \Theta$. The relevant data is derived from m IID random variables $\mathbf{X} = \{X_i\}_{i=1}^m$ governed by a probability distribution based on the unknown θ. The idea is to use the observations $\mathbf{x} = (x_1, \cdots, x_m) \in R^m$ to determine the value of θ; i.e., *the statistical objective function* $F : R^m \to \Theta$ is $F(\mathbf{x}) = \theta$.

The associated "statistical mechanism design problem," then, is to create an estimator $\hat{\theta}$ to realize the goal $F(\mathbf{x}) = \theta$. In doing so, certain natural issues arise. The first is to extract the relevant aspects of the observations $\mathbf{x}$. Do we need the precise value of each observation x_j along with the order in which it occurred, or are there more efficient, compressed, aggregated forms of the data that dismiss irrelevant aspects of the observations by retaining only what is needed to accomplish

[2] Among the many other selection criteria is to determine whether the resulting organization is incentive compatible. Another choice is to minimize the complexity involved in the computations of agents' messages.

the specified goal? For example, in determining the probability that Tails will occur when a penny spinning on its edge finally falls, can we find a more precise estimate of θ by using the full listing $(T, T, T, H, \dots)$ from 100 spins of the penny, or would a count of the number of Tails suffice?[3] As one might expect, this informational concern was a central issue in statistics (Savage [Sav]); the solution is the ***sufficient statistic***.

Recall that a statistic is a random variable $T(\mathbf{X})$. The level sets of observations, $T^{-1}(t) = \{\mathbf{x} \in R^m | T_j(\mathbf{x}) = t\}$ partition the space of observations R^m. A statistic T is ***sufficient*** iff the conditional joint probability distribution of $\mathbf{X} = (X_1, \dots, X_m)$ given $T = t$ is independent of the value of θ; i.e., T is sufficient iff $Pr(\mathbf{X} = \mathbf{x} | T = t, \theta) = v(\mathbf{x}, t)$. Notice that this definition loosely requires a $T = t$ partition set to be in a "θ- level set" of the probability distribution.

A given F admits many different sufficient statistics. With the spinning penny illustration let T_1, T_2 represent, respectively, the number of tails in the first 50 and next 50 spins; it is easy to show that $T = (T_1, T_2)$ is a sufficient statistic. Another choice is the total count of tails $T_3 = T_1 + T_2$. Clearly, T_3 improves upon T; e.g., T_3 further compactifies the observations. (This is manifested by the larger dimension of the T_3 level sets; larger subsets of data are compressed into the same statistic.) T' is a ***minimal sufficient statistic*** if the data cannot be further compressed without losing sufficiency.

Notice the close relationship between the theory of sufficient statistics and the problem of mechanism design. As above, a first task in mechanism design is to determine what are the relevant aspects of the agents' characteristics to realize a specified P. In this comparison between the areas, the image values of P replace the value of θ, and a message m plays the same role as the value $T = t$ in statistics; i.e., the role of m is to identify relevant partition sets of the agents' characteristics. These partition sets, called ***information sets*** ([$S_{3,4}$]), are given by

$$\mathcal{U}_j(m) = \{\mathbf{x}_j \in R^{k_j} | g_j(\mathbf{x}_j, m) = 0\}.$$

The statistical partition sets $\{T^{-1}(t)\}_t$ identify the type of information needed to design an estimator; the information sets from mechanism design characterize the type of information needed to design an organization to realize P.

"Privacy preserving" introduces a complication for mechanism design not explicitly described in statistics. However, intuition about privacy preserving can be gained by examining $T = (T_1, T_2)$; both T_1 and T_2 satisfy a privacy preserving condition. (For instance, the outcome of T_1 is based only on the entries for the first 50 spins of the coin.) One way to analyze T_1 and T_2 is to divide the space of observations into the components $R^{100} = R^{50} \times R^{50}$ where the jth component characterizes the outcome of T_j, $j = 1, 2$. The T_j level sets give the number of Tails on the jth set of 50 spins of the penny, so neither level set characterizes the sufficient statistic T. Instead for each $(T_1, T_2) = (t_1, t_2)$, the level set of R^{100} characterizing T is the product

$$\{\mathbf{x} \in R^{50} | T_1(\mathbf{x}) = t_1\} \times \{\mathbf{x} \in R^{50} | T_2(\mathbf{x}) = t_2\} \subset R^{100}.$$

[3]It is amusing to note that the probability of Tails is 0.72; not the suspected 0.50 which results from a flipped penny. In the spinning penny the slightly heavier Head tilts the axis of rotation providing a prejudice toward Tails.

Similarly, in mechanism design, privacy preserving allows only agent j to use the entry $\mathbf{x}_j \in R^{k_j}$, so the "group partition sets" must be constructed from the individual information sets. As true for the sufficient statistic example, the individual information sets need to be designed so that the product

$$\prod_{i=1}^{n} \mathcal{U}_i(m) = \mathcal{U}_1(m) \times \cdots \times \mathcal{U}_n(m) \tag{2.1}$$

partitions the space $\prod_{j=1}^{n} R^{k_j}$ like that of a sufficient statistic. The set $\prod_{i=1}^{n} \mathcal{U}_i$, the *group information set*, is the product of the individual information sets. However, because the messages from an individual can use messages from other agents, the design of the individual information sets is more complicated than for sufficient statistics. This dependency on other agents' messages creates a delicate coordination condition captured by Eq. 2.1. Equation 2.1 is, then, an *"anti-Tower of Babble"* condition; it coordinates what each agent says so that the messages contribute toward the goal of realizing P.

The parallels with the theory of sufficient statistics continue. For the same reasons that $T^{-1}(t)$ is in a θ level set, the group information set $\prod \mathcal{U}_i$ must be in a level set of P.[4] An objective of statistics is to find a minimal sufficient statistic (which minimizes the dimension of the space of values $T = t$); the parallel objective for mechanism design is to find information sets that minimize the dimension of the message space M. A sufficient statistic need not define an estimator for θ; instead its role is to identify what kind of information is needed to design an estimator. Likewise the role of the individual and group information sets is to determine the kind of information needed in the design of an organization to realize P. With the wealth of estimators associated with a sufficient statistic, we need to select among them by using other criteria; e.g., an estimator is to be unbiased. Likewise, as there are a large number of different organizations that realize P, we need to use other criteria, such as incentive compatibility, to select among them.

To see further parallels between mechanism design and sufficient statistics, recall that the Halmos-Savage factorization theorem asserts that T is a sufficient statistic iff it admits the factorization $Pr(\mathbf{X} = \mathbf{x} | T = t, \theta) = v(\mathbf{x})g(t, \theta)$. (See, for instance, Lehmann [L].) For mechanism design, this factorization assertion is the requirement that the MR diagram commutes. Additional factorization requirements are given by the characterization theorems in Section 4.

3. Information Sets and Integrability Conditions for Utility Theory

An important aspect of the mechanism design problem, then, is to determine the information sets associated with a specified objective function P. These are the level sets of the *communication network* [S4] defined by (unknown) $\{G_j(\mathbf{x}_j, m)\}_{j=1}^{n}$, so an accompanying goal is to find these G functions. Notice the close parallels between this problem and the classical issue of integrability from economics. In utility theory, the problem is to find appropriate conditions so that an agent's preferences can be characterized by an utility function. Samuelson cleverly solved

[4] If not, then one message would correspond to more than one value of P; this would contradict the commuting of the diagram.

this problem in the setting of two goods. His idea uses the facts that each $\mathbf{x}$ is the demand for some price-income pair and that the budget line passing through $\mathbf{x}$ is a tangent line to the indifference curve. Thus, by use of his weak axiom of revealed preference (WARP), Samuelson [$Sam_{1,2}$] showed that the envelope created by the budget lines trace out the level sets for an agent's utility function.

It is reasonable to suspect the WARP argument to apply for $n \geq 3$ goods by using budget planes to trace out the indifference sets. It does not; the WARP argument breaks down as noted by several researchers (e.g., [Sam_2]) and as Gale [Ga] demonstrated with an example. The deficiencies of WARP were corrected in a fundamental paper by Houthakker [Ho] with his introduction of the strong axiom of revealed preferences (SARP). A way to interpret the strings of pairwise comparisons required by SARP is that the multiple comparisons are needed to carefully orient the tangent planes (budget planes) to force the resulting envelope to define level surfaces. This interpretation is consistent with what we know about surfaces in R^n. For lines, there are very few restrictions; after all, in a two-dimensional space little can go wrong with the orientation of the tangent lines. (Consequently we only need the existence theory for ordinary differential equations.) However, for higher dimensional surfaces in R^n, $n \geq 3$, the more delicate orientation problem requires more stringent integrability conditions to ensure that surfaces are defined.[5] This requires a differential theory for surfaces; the Frobenius Theory. (See, for instance, [Sp].) In fact some of the examples proving the need of these more stringent conditions for surfaces in R^n, $n \geq 3$, can be used to create other "Gale-type" examples demonstrating the need of SARP over WARP.

How does all of this tie into the mechanism design problem? In both cases indirect information is used to design the level sets. For utility functions, the goal is to characterize the indifference sets (via revealed preferences) in a way that satisfies the integrability conditions. In mechanism design the goal is to characterize the information sets (via considerations related to sufficient statistics) in a way that satisfies the integrability conditions. Indeed, in HRS we did this by characterizing the tangent planes of the information sets.

The dual to the HRS approach is to use the normal vectors for the information sets rather than the tangent planes. This is analogous to defining a utility function based on information about the supporting price vector at each $\mathbf{x}$, rather than the budget plane. In utility theory, the indifference sets are level sets of the (unknown) $U(\mathbf{x})$, so information about the normal vectors describes the direction of ∇U. Likewise, in mechanism design, the jth agent's information sets are the $\mathbf{x}_j$ level sets of g_i^j, $i = 1, \ldots, \alpha_j$, and information about the normal vectors provides information about $\nabla_{\mathbf{x}_j} g_i^j$. By understanding the space of normal vectors for the information sets, perhaps we can reconstruct the $\nabla_{\mathbf{x}_j} g_i^j$, and the actual messages. This is an advantage of the dual approach.

Any such theory must involve integrability conditions for normal vectors. I'll describe these ideas in terms of utility functions. Suppose information about the

[5] The division between $n \geq 3$ and $n = 2$ is common in economics. A dramatic illustration is Arrow's Impossibility Theorem where n is the number of candidates. This numerology is not a mere coincidence; it manifests the difference between the geometry of a line ($n = 2$) and a higher dimensional plane ($n \geq 3$). This is discussed in [S_5].

normal vectors is obtained that appears to define the gradient of a function; i.e., suppose we suspect that $\mathbf{v}(\mathbf{x}) = (v_1(\mathbf{x}), \ldots, v_n(\mathbf{x})) = \nabla U(\mathbf{x})$ for some function U. The integrability conditions use the fact that mixed partial derivatives agree; i.e, $\frac{\partial U(\mathbf{x})}{\partial x_i \partial x_j} = \frac{\partial U(\mathbf{x})}{\partial x_j \partial x_i}$. Thus, if

$$\frac{\partial v_j(\mathbf{x})}{\partial x_i} = \frac{\partial v_i(\mathbf{x})}{\partial x_j} \qquad \text{for all i, j,} \tag{3.1}$$

then there is reason to believe that $\mathbf{v}(\mathbf{x})$ is a gradient. A standard theorem asserts that, at least locally, this is true.

With differential forms (e.g., see [F, SP, W]), the differentiability conditions 3.1 become particularly simple. Recall that the differential dx_j is an element of length – an incremental change in the x_j direction. The vector field $\mathbf{v}(\mathbf{x})$ can be identified with an *one-form* by defining $v = \sum_{i=1}^n v_i(\mathbf{x})dx_i$. In particular, a gradient $\nabla U(\mathbf{x})$ is identified with the one-form

$$dU = \frac{\partial U(\mathbf{x})}{\partial x_1}dx_1 + \cdots + \frac{\partial U(\mathbf{x})}{\partial x_n}dx_n. \tag{3.2}$$

Higher dimensional measures, such as area, volume, etc., are obtained via the *wedge product* $\wedge$. One can identify this product with an element of area given by the product of two incremental elements of length in different directions. The main rule in the wedge product is an orientation whereby each of the *two-forms*

$$dx_i \wedge dx_j = -dx_j \wedge dx_i \tag{3.3}$$

define a two-dimensional element of area, but with different orientations. (The orientation is important for, say, fluid flow problems where we need to know which way the fluid is passing through an element of area of a surface. A related "fluid flow" problem arises in the study of strategic behavior [S_6].) A convenient consequence of this orientation is that $dx_j \wedge dx_j = -dx_j \wedge dx_j = 0$; this reflects the obvious fact that a two dimensional area cannot be constructed by incremental lengths both along the same line – area is not "length times length;" it is "length times width." By use of the wedge product, two-forms are constructed from two one-forms in a natural way where $\omega_1 \wedge \omega_2 = (a_1 dx_1 + a_2 dx_2 + a_3 dx_3) \wedge (b_1 dx_1 + b_2 dx_2 + b_3 dx_3) = a_1 dx_1 \wedge (b_1 dx_1 + b_2 dx_2 + b_3 dx_3) + a_2 dx_2 \wedge (b_1 dx_1 + b_2 dx_2 + b_3 dx_3) + a_3 dx_3 \wedge (b_1 dx_1 + b_2 dx_2 + b_3 dx_3)$, or, by the orientation rules,

$$(a_2 b_3 - b_2 a_3) dx_2 \wedge dx_3 + (a_3 b_1 - a_1 b_3) dx_3 \wedge dx_1 + (a_1 b_2 - b_1 a_2) dx_1 \wedge dx_2. \tag{3.4}$$

To see the type of area this two-form measures, identify ω_1, ω_2, respectively with the vectors $\mathbf{V}_1 = (a_1, a_2, a_3)$, $\mathbf{V}_2 = (b_1, b_2, b_3)$. The vectors $\mathbf{V}_1, \mathbf{V}_2$ define a parallelogram with area given by the magnitude of the vector

$$\mathbf{V}_1 \times \mathbf{V}_2 = \begin{vmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} = (a_2 b_3 - b_2 a_3, a_3 b_1 - a_1 b_3, a_1 b_2 - a_2 b_1) \tag{3.5}$$

where the $\mathbf{e}_i$ term in the top row of the determinant is the unit vector with unity in the ith component. Notice that the coefficients in Eqs. 3.4, 3.5 agree.

In general,

$$\omega_1 \wedge \omega_2 = (\sum a_i dx_i) \wedge (\sum b_j dx_j) = \sum_{i<j} (a_i b_j - b_i a_j) dx_i \wedge dx_j \tag{3.6a}$$

has a determinant interpretation of each coefficient. Let $A_{i,j}$ be the 2×2 determinant using the ith and jth columns from

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}.$$

Then

$$\omega_1 \wedge \omega_2 = \sum_{i<j} A_{i,j} dx_i \wedge dx_j. \tag{3.6b}$$

The integrability condition also involves the *exterior derivative.* Given a form $\omega = \sum_{j=1}^{n} a_j(\mathbf{x}) dx_j$, define

$$d\omega = \sum_{j=1}^{n} (da_j(\mathbf{x})) \wedge dx_j. \tag{3.7}$$

When this derivative is applied to $\omega = dU$ we obtain

$$\begin{aligned} d\omega = d^2U &= d(\frac{\partial U(\mathbf{x})}{\partial x_1}) \wedge dx_1 + \cdots + d(\frac{\partial U(\mathbf{x})}{\partial x_n}) \wedge dx_n = \\ &= \sum_{i<j} [\frac{\partial^2 U}{\partial x_i \partial x_j} - \frac{\partial^2 U}{\partial x_j \partial x_i}] dx_i \wedge dx_j = 0. \end{aligned} \tag{3.8}$$

In other words, the orientation rule of the wedge product along with the fact that mixed partial are equal forces all of the terms to cancel, so $d^2 \equiv 0$.

The important fact is that the converse is true; if

$$d\omega \equiv 0, \tag{3.9}$$

then, at least locally, $\omega = dU$ for some function U. This is the differential version of the integrability condition Eq. 3.1.

When indirect methods are employed to determine the structure of the level sets, such when revealed preferences are used, one cannot expect the information to define a gradient $\omega = dU$. Instead, the best one might anticipate is the weaker integrable situation $\omega = h(\mathbf{x})dU$ where $h(\mathbf{x}) \neq 0$ and U are unknown functions. If so, then the goal is to solve for dU and U. For instance, if only information about the unit price vector is known, then all we have is $\omega = |\nabla U(\mathbf{x})|^{-1} dU$ where $h(\mathbf{x}) = |\nabla U(\mathbf{x})|^{-1}$.

The new integrability problem, then, is to identify when

$$\omega = h(\mathbf{x})dU \tag{3.10}$$

does or does not occur. To find these conditions, start with the desired situation Eq. 3.10 and differentiate. According to the product rule,

$$d\omega = dh \wedge dU + hd^2U = dh \wedge dU.$$

Unfortunately, $d\omega$ involves the unknown functions. So, using the assumption $\omega = h(\mathbf{x})dU$, we have that $dU = h^{-1}\omega$, or

$$d\omega = h^{-1}dh \wedge \omega.$$

In other words, if

$$d\omega = \beta \wedge \omega \tag{3.11}$$

for some one-form β, then we should suspect that Eq. 3.10 holds. To identify when Eq. 3.11 does occur, use the wedge product; after all $\omega \wedge d\omega = \omega \wedge (h^{-1}dh \wedge \omega) = -h^{-1}dh \wedge (\omega \wedge \omega) \equiv 0$ as $\omega \wedge \omega \equiv 0$. ($\omega \wedge \omega$ corresponds to a degenerate parallelogram.) The important fact is that the converse holds; if $\omega = \sum_{j=1}^{n} a_j(\mathbf{x})dx_j$ satisfies

$$\omega \wedge d\omega \equiv 0, \tag{3.12}$$

then, at least locally, Eq. 3.10 holds. Namely, there exist functions $H(\mathbf{x}), U(\mathbf{x})$, so that, at least locally, one has the integrable problem $H(\mathbf{x})\omega = dU$.

Equation 3.12 is a compact representation of the standard integrability conditions. To see this for the special case of $n = 3$ and a vector field $\mathbf{p}(\mathbf{x}) = (p_1(\mathbf{x}), p_2(\mathbf{x}), p_3(\mathbf{x}))$, the associated one-form is $\omega = \sum_{j=1}^{3} p_j dx_j$. The integrability conditions from Eq. 2.9 are are the standard

$$p_3[\frac{\partial p_2}{\partial x_1} - \frac{\partial p_1}{\partial x_2}] + p_2[\frac{\partial p_1}{\partial x_3} - \frac{\partial p_3}{\partial x_1}] + p_1[\frac{\partial p_3}{\partial x_2} - \frac{\partial p_2}{\partial x_3}] = 0$$

conditions found in, say, [V. Sam_2], etc.

SARP is used to ensure the alignment of the tangent planes defines surfaces; likewise we must expect related alignment concerns to arise when ω represents a normal vector to these planes. The differential $d\omega$ captures the movement of the normal vector (and the concomitant change in the tangent planes), so the alignment condition is the integrability requirement $\omega \wedge d\omega \equiv 0$.

The above approach suffices for a family of level sets coming from a single function, but more is needed for mechanism design. After all, each function defines a message and for many P (e.g., a Walrasian allocation) it is overly optimistic to expect an agent's relevant characteristics to be codified in a single number. Therefore, we need an integrability theory for $\alpha \geq 1$ equations. To develop insight, start with an integrable situation and use it to develop criteria (the integrability conditions) that identify when it arises. Again, because indirect methods are used to characterize the information sets, we cannot expect to end up with the desired gradients of g_j, or even with these gradients appearing in the form given by Eq. 3.9; instead, it is more likely that an integrable situation arises in a scrambled setting of α one-forms

$$\omega_i = \sum_{j=1}^{\alpha} a_{ij}(\mathbf{x})dg_j(\mathbf{x}), \qquad i = 1, \ldots, \alpha, \tag{3.13}$$

where the ω_i's are given but the fact they are expressed in terms of the integrable, but unknown dg_j's is not known. The goal is to identify when Eq 3.13 holds, and then solve for the dg_j's. (And then the g_j's.)

The conditions which identify when Eq. 3.13 holds are based on a multidimensional version of the argument used to derive Eq. 3.12. If Eq. 3.13 holds, we can use the α equations and α unknowns to solve for the dg_j's iff the matrix $((a_{i,j}))$ is nonsingular iff the vectors identified with $\{\omega_i\}_{i=1}^{\alpha}$ are linearly independent iff these vectors define a parallelogram with non-zero α-dimensional volume iff

$$r_\alpha = \omega_1 \wedge \cdots \wedge \omega_\alpha \neq 0 \tag{3.14}$$

is a nonzero measure of α-dimensional volume. Equation 3.14 ensures, then, that (at least locally) we can solve Eq. 3.13 for

$$dg_j = \sum_{k=1}^{\alpha} b_{jk}(\mathbf{x})\omega_k, \qquad j = 1. \ldots \alpha. \tag{3.15}$$

Following the lead of SARP and Eq. 3.12, we must expect the desired conditions to involve $d\omega_i = \sum_{j=1}^{\alpha} da_{ij} \wedge dg_j$. As true in the argument leading to Eq. 3.11, each term in the sum involves an (unknown) integrable factor dg_j. Using Eq. 3.15, we have that $d\omega_i = \sum_{j=1}^{\alpha} da_{ij} \wedge [\sum_{k=1}^{\alpha} b_{jk}(\mathbf{x})\omega_k] = \sum_{k=1}^{n} \beta_k \wedge \omega_k$ where β_k is a one- form involving $b_{jk}(\mathbf{x})$, da_{ij}, etc. Mimicking Eq. 3.11, an indicator that the integrability situation prevails is if each $d\omega_i$ can be expressed as

$$d\omega_i = \sum_{k=1}^{n} \beta_k \wedge \omega_k. \tag{3.16}$$

Whether Eq. 3.16 occurs can be determined by exploiting the fact $\omega_k \wedge \omega_k \equiv 0$. By using the repeated wedge product of $d\omega_i$ with each of the ω_k's, each term in the summation disappears. In other words, if Eq. 3.16 occurs, then it must be that

$$d\omega_i \wedge r_\alpha \equiv 0 \qquad i = 1, \ldots, \alpha. \tag{3.17}$$

The critical fact is that the converse is true. If Eqs 3.14, 3.17 hold, then so does Eq. 3.13. Namely, there are linear combinations (with scalar functions as coefficients) of the $\{\omega_j\}_{j=1}^{\alpha}$ which define integrable functions satisfying the usual mixed partial conditions.

Next I express these integrability conditions in the more modern language used in Section 4. An *ideal* I generated by the α one-forms $\{\omega_i\}_{i=1}^{\alpha}$ (denoted by $I =<$

$\omega_1, \ldots, \omega_\alpha >$) is the space of all possible one-forms created by linear combinations of the $\{\omega_i\}_{i=1}^{\alpha}$ where the coefficients are smooth functions. At each point $\mathbf{x}$, the ideal defines a vector space – it is the space of vectors orthogonal to the desired level set at $\mathbf{x}$. So, the ideal describes how this vector space changes smoothly as $\mathbf{x}$ varies. The ideal has dimension α if at each $\mathbf{x}$ the vector space has a basis of dimension α iff a basis of the ideal defines the non- vanishing α-dimensional area $r_\alpha \neq 0$ but all $\alpha+1$ products are identically zero. An α-dimensional ideal is a *differential ideal* if Eqs. 3.14, 3.17 hold. If it is a differential ideal, then Eq. 3.13 holds. This means that there is a basis for the ideal expressed in terms of α differentials of functions; the intersection of the level sets of these functions define a $n-\alpha$ dimensional foliation. These are the Frobenius integrability conditions described as a differential ideal. In our application, the α functions will correspond to the communication functions in the communication networks while the level sets are the information sets.

4. Design of Message systems

Armed with integrability conditions, we now turn to the question of mechanism design. As differentiability conditions are involved, we require P to be a smooth mapping. Also, to remove obvious redundancies, we impose the following *efficiency assumptions* on the communication functions $G = (G_1, \ldots, G_n) : \prod_{j=1}^{n} R^{k_j} \times M \rightarrow R^{\sum \alpha_j}$. Recall, each G_j mapping consists of the communication functions $\{g_i^j\}_{i=1}^{\alpha_j}$. (See Sect. 1.)

Efficiency Assumptions $[S_1]$. a. $Dim(M) = \sum \alpha_j$; i.e., the dimension of M agrees with the number of $\{g_i^j\}$ functions.
b. At $(\mathbf{X}, m)$, the Jacobean of G with respect to m is non-singular.
c. At $(\mathbf{X}, m)$, the Jacobean of G with respect to $\mathbf{X}$ has maximal rank.

To characterize the information sets and the associated message system, a differential ideal is constructed for each agent. The idea is simple; place in each agent's ideal the one-forms representing normal vectors for the information sets. These one-forms are determined by conditions specifying what must and must not happen. In the current discussion, there are only four considerations: privacy preserving, sufficient statistic, coordination of messages, and integrability.

Privacy preserving requires the kth agent's messages to be independent of the other agents' characteristics – the other agents' characteristics are orthogonal to the kth agent's information sets.[6] Thus, if x_j^i is a component of another agents' characteristics, then $dx_j^i \in I_k$. So, if $[d\mathbf{X}]_k$ denotes the set of differentials of all coordinate functions *except* those of the kth agent, then $I_k \supset < [d\mathbf{X}]_k >$.

The "sufficient statistic" considerations require the information sets to be in level sets of P; i.e., $dP = (dP_1, \ldots, dP_a) \in I_k$. The differential of a coordinate function, say dP_1, is a sum involving the differentials of coordinates for the kth agent's characteristics and a sum involving differentials of all other coordinates;

$$dP_1 = \sum \frac{\partial P_1}{\partial x_i^k} dx_i^k + \sum \frac{\partial P_1}{\partial x_i^j} dx_i^j.$$

[6] Compare this situation with the (T_1, T_2) sufficient statistic. T_1 does not involve any entry from the second 50 flips of the coin, so each of these coordinates is orthogonal to a T_1 level set.

The second summation is a linear combination of privacy preserving terms $[d\mathbf{X}]_k$ already entered into I_k. So, by vector space operations, this summation can be eliminated leaving only $\sum \frac{\partial P_1}{\partial x_i^k} dx_i^k$ with any relevance for I_k. Denote this sum as $d_k P_1$, and let $d_k P = (d_k P_1, \ldots, d_k P_a)$. We then have that

$$I_k \supset < d_k P; [d\mathbf{X}]_k > . \tag{4.1}$$

The interaction effects ensure that the kth agent's message helps the other agents realize P. As indicated in Section 2, this interaction is captured by the product structure of the group information set (Eq. 2.1). As true for the individual information sets, the group information set is characterized by its normal vectors. It is clear from the form of $\prod_{i=1}^n \mathcal{U}_i(m)$ that the normal vectors for the product set come from the normal vectors for each of the individual information sets. However, those normal vectors representing privacy preserving play no role in the group information set, so they must be dropped. To see how to do this, notice that because the other agents must respect the privacy of the jth agent, their privacy preserving vectors span R^{k_j}. Consequently in the intersection of the agents' space of normal vectors for R^{k_j}, only the space of normal vectors for the jth agent survives. Using the ideal representation, this allows the normal vectors for the group information sets to be identified with the ideal

$$I = \cap_{k=1}^n I_k. \tag{4.2}$$

So far $I \supset < d_1 P, \ldots, d_n P >$.

Now comes the issue of integrability. To define the information sets, we need that $\{I_j\}_{j=1}^n$ and I are differential ideals. It is easy to show that if I is a differential ideal, then so are the ideals I_j. Therefore, the mechanism design problem hinges on whether I is a differential ideal. Just as SARP is not just a technicality, requiring I to be a differential ideal is not a mere technical detail; it is the crux of the mechanism design problem. After all, the integrability of I determines whether or not the agents' messages can be coordinated to realize P! For instance, the integrability of I distinguishes between the P's admitting an organization where each agent responds with messages of a single type (e.g., a bid), and those P requiring more refined messages reflecting different attributes of the agent's type (e.g., an excess demand for each of the n commodities). It turns out that P admits an organization where each agent's uses one kind of message iff I is a differential ideal with the entries already placed in I. But, for many choices of P, this is not be the case. As a simple example, let $P = \sum_{j=1}^4 x_j y_j$ where the first and second agents use, respectively, the value of $\mathbf{x}$ and $\mathbf{y}$ in their messages. With the above, $I_1 =< d_1 P = \sum_{j=1}^4 y_j dx_j; dy_1, dy_2, dy_3, dy_4 >, I_2 =< d_2 P = \sum_{j=1}^4 x_j dy_j; dx_1, dx_2, dx_3, dx_4 >$, $I =< \sum_{j=1}^4 y_j dx_j; \sum_{j=1}^4 x_j dy_j >$. It is straightforward (using Eq. 3.17) to verify that I_1, I_2 are differential ideals, but that I is not. Consequently it is impossible to construct information sets for these two agents to realize P where each agent's message ("sufficient statistic") can be collapsed into a single number; a refinement in the messages (information sets) is required.

If the above entries do not make I a differential ideal, then refined information sets are required. The refined, or lower dimensional information sets are created by adding appropriate one-forms (normal vectors) to the ideals to make I a differential ideal. As $I = \cap I_j$ these one-forms ω must first be added to an appropriate I_j in order to gain entry to I. But, to gain entry to I, an one-form ω_j added to I_j must be a linear combination of the differentials of the coordinates assigned to this agent. (I indicate in Section 5 how to find the ω_j's.) When an independent ω_j is added to I_j, the information sets become lower dimensional; i.e., each ω_j corresponds to adding another communication function g_i^j for the jth agent. We now arrive at the fundamental characterization theorem for mechanism design.

Privacy Preserving Characterization Theorem $[S_1]$.

Let $P : \prod_{j=1}^{n} R^{k_j} \to R^a$ be a smooth performance function. The following are necessary and sufficient conditions that a privacy preserving message system satisfying the efficiency assumptions on G with $dim(M) = \sum_{j=1}^{n} n_j$ exists which realizes P in a neighborhood of $\mathbf{X} \in \prod R^{k_j}$.

a. *For each j there is a differential ideal $I_j = < d_jP, \omega_{j,1}, \ldots, \omega_{j,s_j}; [d\mathbf{X}]_j >$ which is of dimension $n_j + \sum_{i \neq j} k_i$. The $\omega_{j,i}$'s are smooth one- forms.*

b. *The set $I = \cap_{j=1}^{n} I_j$ is a differential ideal of dimension $\sum_{j=1}^{n} n_j$.*

This characterization theorem plays the same role for mechanism design as the Halmos-Savage factorization theorem for the sufficient statistic and the SARP for revealed preference. As true for SARP and the sufficient statistic, it does not describe the information sets. Instead it specifies what conditions characterize those information sets that can be used to develop an organization to realize the given objective P.

A generalized characterization theorem holds when the privacy preserving condition is relaxed to permit "common knowledge" or where certain agents' messages depend upon other agent's parameters. Presumably, with shared information, there is a reduction in the number of messages needed to realize P. For instance, if $P(x, y) = xy$, where x, y are known respectively by the first and the second agents, then two messages are needed; e.g., the first agent can communicate the value of x to the second agent who then computes the value of xy. However, if one agent, say the second, knows both values, then only one message is required – this agent computes and communicates the value of P. Using the close connection with the sufficient statistic, this potential savings in communications reflects the fact the level sets of P admits a cruder partition that satisfies the privacy condition; it is analogous to using T_3 rather than (T_1, T_2).

The first step leading to the following more general theorem requires modifying the "privacy preserving" conditions; i.e., $I_k \supset < [d\mathbf{X}]_k >$. For each $k = 1, \ldots, n$, specify the parameters that are off-limits in the design of the kth agent's communication functions; namely list the coordinates of other agents that are not accessible for the design of the kth agent's messages. This listing constitutes the *"privacy conditions."* Let $[[d\mathbf{X}]_{PC}]_k$ denote the differentials of these coordinates for the kth agent, and let β_k be the dimension of this set. Then $I_k \supset < d_kP; [[d\mathbf{X}]_{PC}]_k >$. For instance, modifying the earlier dot product example to permit both agents to use x_1, y_1 and the first agent to use y_4, then $[[d\mathbf{X}]_{PC}]_1 = \{dy_2, dy_3\}$, $\beta_1 = 2$, while $[[d\mathbf{X}]_{PC}]_2 = \{dx_2, dx_3, dx_4\}$, $\beta_2 = 3$.

There are other modifications required by the extension of privacy preserving; e.g., d_kP is the truncation of dP based on the differentials of coordinates accessible to the kth agent by the privacy conditions. Likewise, the rank assertions for the efficiency conditions are based on the larger set of variables. The more general characterization theorem follows.

Characterization Theorem.

Let $P : \prod_{j=1}^{n} R^{k_j} \to R^a$ be a smooth performance function with specified privacy conditions. The following are necessary and sufficient conditions that a message system satisfying the privacy conditions and the efficiency assumptions on G with $dimM = \sum_{j=1}^{n} n_j$ exists which realize P in a neighborhood of $\mathbf{X} \in \prod R^{k_j}$.

a. *For each j there is a differential ideal $I_j = < d_j P, \omega_{j,1}, \ldots, \omega_{j,i}; [[dX]_{PC}]_j >$ which is of dimension $n_j + \beta_j$. The $\omega_{j,i}$'s are smooth one-forms.*
b. *For each nonempty subset of indices $\mathcal{A} \subset \{1, 2, \ldots, n\}$, the set $I_{\mathcal{A}} = \cap_{j \in \mathcal{A}} I_j$ is a differential ideal.*
c. *The ideal $I = \cap_{j=1}^{n} I_j$ is of dimension $\sum_{j=1}^{n} n_j$.*

Notice that this characterization theorem includes the earlier one. To illustrate the new terms with the modified dot product example, we have that $I_1 \supset < d_1 P = \sum_{i=1}^{4} y_i dx_i + x_1 dy_1 + x_4 dy_4; dy_2, dy_3 >$, $I_2 \supset < d_2 P = \sum_{i=1}^{4} x_i dy_i + y_1 dx_1; dx_2, dx_3, dx_4 >$, and $I \supset < d_1 P, d_2 P >$.

These characterization theorems seem to require P to be given explicitly. This creates a complication for many economic models because, often, the performance function is defined implicitly (e.g., first order constraints) while satisfying additional constraints (e.g., budget constraints). Both complications arise in a two agent, two commodity exchange economy where the kth agent has a Cobb-Douglas utility functions $U_k(y_1, y_2) = y_1^{\alpha_k} y_2^{\beta_k}$ with initial endowment (w_1^k, w_2^k). The space of characteristics for the kth agent is $\Omega_k = \{\mathbf{x}_k = (\alpha_k, \beta_k, w_1^k, w_2^k) \in R_+^4\}$. The performance function, $P(\mathbf{x}_1, \mathbf{x}_2) = (a_1^1, a_2^1; a_1^2, a_2^2)$ is defined implicitly by the equations

$$\frac{\nabla U_1(a_1^1, a_2^1)}{|\nabla U_1(a_1^1, a_2^1)|} = \frac{\nabla U_2(a_1^2, a_2^2)}{|\nabla U_2(a_1^2, a_2^2)|}$$
$$\forall j \quad \sum_k w_j^k = \sum_k a_j^k$$
$$\forall k \quad ((w_1^k, w_2^k) - (a_1^k, a_2^k)) \cdot \nabla U_k(a_1^k, a_2^k) = 0 \tag{4.3}$$

While we could solve for P (the a_j^i's), this is a messy, nonlinear task. (For some models, solving for P may not be feasible.) However P is needed only to compute $d_k P$; these $d_k P$ terms can be found in a *linear fashion by implicitly differentiating the defining constraint equations and then solving the linear equations for $d_k P$.* Obviously, this is a much simpler linear problem. For instance, the last of the equations in Eq. 4.3 becomes

$$\begin{aligned} &((dw_1^k, dw_2^k) - (da_1^k, da_2^k)) \cdot (\alpha_k (a_1^k)^{\alpha_k - 1}, \beta_k (a_2^k)^{\beta_k - 1}) = \\ &- (w_1^k, w_2^k) - (a_1^k, a_2^k)) \cdot (\alpha_k(\alpha_k - 1)(a_1^k)^{\alpha_k - 2} da_1^k, \beta_k(\beta_k - 1)(a_2^k)^{\beta_k - 2} da_2^k. \end{aligned} \tag{4.4}$$

The following theorem asserts that this approach holds in general.

Characterization Theorem For Implicitly Defined Functions.

Let $P : \prod_{j=1}^{n} R^{k_j} \to R^a$ be a smooth performance function implicitly defined by the conditions

$$H_k(\mathbf{x}_1, \ldots, \mathbf{x}_n, P(\mathbf{X})) = 0 \quad k = 1, \ldots, J, \tag{4.5}$$

where each H_k is a smooth function. Suppose privacy conditions are specified. The following are necessary and sufficient conditions that a message system satisfying the privacy conditions and the efficiency assumptions on G with $dim(M) = \sum_{j=1}^{n} n_j$ exists which realizes P in a neighborhood of $\mathbf{X} \in \prod R^{k_j}$.

a. *For each j there is a differential ideal $I_j =< d_jP, \omega_{j,1}, \ldots, \omega_{j,s_j}; [[dX]_{PC}]_j >$ which is of dimension $n_j + \beta_j$. The $\omega_{j,i}$'s are smooth one-forms. The d_jP terms are found from the expressions linear in dx_j, dP*

$$dH_k(\mathbf{x}_1, \ldots, \mathbf{x}_n, P(\mathbf{X})) = 0 \quad k = 1, \ldots, J. \tag{4.6}$$

b. *For each nonempty subset of indices $\mathcal{A} \subset \{1, 2, \ldots, n\}$, the set $I_{\mathcal{A}} = \cap_{j \in \mathcal{A}} I_j$ is a differential ideal.*
c. *The ideal $I = \cap_{j=1}^{n} I_j$ is of dimension $\sum_{j=1}^{n} n_j$.*

The proofs of these last two theorems will appear elsewhere.

5. Bordered Hessians, Chen's Theorem, and the ideals

I've outlined the characterization theorems, but I haven't indicated how to find the $\omega_{i,j}$'s that often need to be added to the ideals I_j. Also, there remains Reiter's question to me about the minimal dimension of a message spaces associated with a given P. Solutions for both problems are outlined below. To keep the details from overwhelming the exposition, I'll concentrate on the privacy preserving, two agent setting where $P : \prod_{j=1}^{2} R^{k_j} \to R$.

According to the efficiency definition for G and the integrability conditions, the minimal dimension problem is a geometric one because $dim(M) = dim(I)$. But, it is not clear how to find the minimal value for $dim(I)$. Important information about this issue was obtained by P. Chen [$C_{1,2}$]. Using the approach of [S_1] and building on earlier ideas of L.Hurwicz [H_2] and S. Williams [W], Chen found a lower bound for $dim(M)$ in terms of the rank of the Bordered Hessian for $P(\mathbf{x}, \mathbf{y})$

$$BH(P) = \begin{pmatrix} ((\frac{\partial^2 P(\mathbf{x},\mathbf{y})}{\partial x_i \partial y_j})) & \nabla_{\mathbf{x}} P \\ (\nabla_{\mathbf{y}} P)^t & 0 \end{pmatrix} \tag{5.1}$$

where ∇U is a column vector. Steve Williams showed that if a message system for P has $dim(M) < min(k_1, k_2)$, then $BH(P)$ does not have full rank. Chen proved the stronger assertion that

$$dim(M) \geq rank(BH(P)). \tag{5.2}$$

To illustrate Chen's Theorem, notice for $P = \mathbf{x} \cdot \mathbf{y}, \mathbf{x}, \mathbf{y} \in R^n$, that

$$BH(P) = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & y_1 \\ 0 & 1 & 0 & \ldots & 0 & y_2 \\ \ldots & \ldots & \ldots & & & \ldots \\ 0 & 0 & 0 & \ldots & 1 & y_n \\ x_1 & x_2 & x_3 & \ldots & x_n & 0 \end{pmatrix} \tag{5.3}$$

has rank $n+1$; according to Chen's Theorem, $dim(M) \geq n+1$. One such message system is "parameter transfer" where the first agent sends all n values of his characteristics to the second agent who, in turn, computes and transmits the value of the dot product.

To show the connection between the rank of $BH(P)$ and the characterization theorem, I'll prove that if $rank(BH(P)) = 2$, then there is a message system where $dim(M) = 2$. According to the characterization theorem, this assertion requires $d_xP \wedge d_yP \wedge d(d_xP) \equiv 0$ and $d_xP \wedge d_yP \wedge d(d_yP) \equiv 0$. Using the equality of mixed partials, we have that $-d(d_xP) = d(d_yP) = \sum_{i,j} \frac{\partial^2 P}{\partial x_i \partial y_j} dx_i \wedge dy_j$, so it suffices to show that $d_xP \wedge d_yP \wedge d(d_yP) \equiv 0$. Now, let A_H be any 3×3 determinant in $BH(P)$ that includes elements from the bottom row and the last column. This determinant involves four indices – two choices for the dx_i and two for dy_j; let $H = \{i, j; s, k\}$, $i < j, s < k$ represent the indices, and let $[dx \wedge dy]_H = dx_i \wedge dx_j \wedge dy_s \wedge dy_k$. A simple expansion argument (see Eq. 3.6b) shows that

$$d_xP \wedge d_yP \wedge d(d_yP) = \sum_H A_H [dx \wedge dy]_H. \tag{5.4}$$

In other words, there is an intimate relationship between the properties of $BH(P)$ and the wedge product integrability conditions. For instance, as $rank(BH(P)) = 2$, all $A_H = 0$, so the integrability condition Eq. 3.17 is satisfied; there is an organization with $dim(M) = 2$. Chen's theorem asserts that one cannot do better than $dim(M) = 2$. Thus we have a simple proof of an earlier observation made by L. Hurwicz $[H_2]$ for $k_1 = k_2 = 2$, and in general by Chen $[C_{1,2}]$..

Proposition $[H_2, C_{1,2}]$. *For $n = 2$ a necessary and sufficient condition for a (local) communication network to exist with $dim(M) = 2$ is $rank(BH(P)) = 2$.*

To better understand how to obtain more general bounds on $dim(M)$, we need the notion of a rank of a two-form

$$\omega = \sum_{i,j} a_{ij} dx_i \wedge dy_j. \tag{5.5}$$

This *rank* is the smallest integer r so that

$$(\omega)^r = \overbrace{\omega \wedge \cdots \wedge \omega}^{k \text{ times}} \neq 0$$

but $(\omega)^{r+1} \equiv 0$. It turns out that r is the rank of the associated matrix $((a_{ij}))$.

If $rank(\omega) = r$, then there are $2r$ one-forms $\phi_1, \cdots, \phi_r; \psi_1, \cdots, \psi_r$ where each ϕ_i is a combination of the dx_j's, each ψ_i is a combination of the dy_j's, and

$$\omega = \sum_{i=1}^{r} \phi_i \wedge \psi_i. \tag{5.6}$$

The proof is by induction; if $\phi_1 = \sum_{j=1}^{n} a_{j1} dx_j$ and $\psi_1 = \sum_{j=1}^{n} [a_{1j}/a_{11}] dy_j$, then $\omega - \phi_1 \wedge \psi_1$ has no dx_1, dy_1 terms. Applying this change of variable argument to

$\omega - \phi_1 \wedge \psi_1$, the remaining independent one-forms are defined in a similar manner.[7] In fact, r is the minimal value for which such an expression (Eq. 5.6) holds.

So, if $rank(d(d_y P)) = r$, we know there is an expression

$$\omega = d(d_y P) = \sum_{i=1}^{r} \phi_i \wedge \psi_i. \tag{5.7}$$

To exploit this representation, express $d_x P, d_y P$ as

$$\begin{aligned} d_x P &= \sum_{j=1}^{r} b_j \phi_j + b_{r+1}\alpha \\ d_y P &= \sum_{j=1}^{r} c_j \psi_j + c_{r+1}\beta \end{aligned} \tag{5.8}$$

where α, β are remainder terms needed if $d_x P, d_y P \notin span(\{\psi_i, \phi_i\})$. To see how to use this representation, return to the special case where $rank(BH(P)) = 2$. This requires $rank(d(d_y P)) \leq 2$. For $r = 2$ and using the $\{\phi_j\}, \{\psi_j\}, \alpha, \beta$ coordinate system, we have that

$$BH(P) = \begin{pmatrix} 1 & 0 & 0 & b_1 \\ 0 & 1 & 0 & b_2 \\ 0 & 0 & 0 & b_3 \\ c_1 & c_2 & c_3 & 0 \end{pmatrix} \tag{5.9}$$

To keep $rank(BH(P)) = 2$, we need that $b_3 = c_3 = 0; b_1 c_1 = -b_2 c_2$. These conditions force $d_x P = b_1\phi_1 + b_2\phi_2$, $d_y P = f(\mathbf{x}, \mathbf{y})[-b_2\psi_1 + b_1\psi_2]$. In other words, the rank imposes stringent requirements on the one-forms. If $r = 1$, then b_3, c_3 don't exist, and the integrability conditions are that $b_2 c_2 = 0$. *In other words, $dim(I)$ is determined by the various ways $d_x P, d_y P$ can be expressed in terms of the basis representation (Eq. 5.7, 5.8) derived for $d(d_x P)$. The rank of $BH(P)$ characterizes those representations of Eq. 5.8 that satisfy the integrability of I for different values of $dim(I)$.*

From the above argument, we see that even if $rank(d(d_y P) = 2$ and $\phi_1 = d_x P, \psi_1 = d_y P$, terms need to be added to either I_1 or I_2 to make I a differential ideal. This is because, so far, we have

$$\phi_1 \wedge \psi_1 \wedge \sum_{i=1}^{2} \phi_i \wedge \psi_i = \phi_1 \wedge \psi_1 \wedge \phi_2 \wedge \psi_2 \neq 0.$$

However, if ϕ_2 is added to I_1, then we would have that $\phi_1 \wedge \psi_1 \wedge \sum_{i=1}^{2} \phi_i \wedge \psi_i \equiv 0$. In general, this observation suggests that once the representation Eq. 5.7 is found, we can solve the problems of finding the minimal value for $dim(M)$ and of finding what ω_i's to add to the ideals. After all, if from the ith term in this sum either ϕ_i is added to I_1 or ψ_i is added to I_2, then $d(d_x P) \wedge r_\alpha \equiv 0$. (This entry in r_α will

[7] This row reduction argument can be modified to show why r is the rank of $((a_{ij}))$.

annihilate the ith term in the sum in Eq. 5.7.) Which terms need to be added to the ideals is determined by Eq. 5.8; e.g., if $d_x P = \phi_2$, then it is not necessary to add a term with index two. However, one further problem arises; after the ψ's and ϕ's have been added, we need to verify the new integrability conditions of the form

$$d\psi_i \wedge r_\alpha \equiv 0. \tag{5.10}$$

Equation 5.10 would be satisfied if we are fortunate enough that the ϕ's and/or ψ's in an integrable form like Eq. 3.10. This requires still another integrability condition: when is it true that

$$d_x P = df_0(\mathbf{x}) + \sum_{j=1}^{k} g_j(\mathbf{x}, \mathbf{y}) df_j(\mathbf{x})? \tag{5.11}$$

Whenever such a situation arises, by choosing $\omega_j^1 = df_j(\mathbf{x})$ I becomes a differential ideal. This solves both problems of determining the choices of ω_j^i and the minimal dimension of M.

Following and using the kinds of arguments used in Section 3, conditions ensuring that Eq. 5.11 holds can be determined. As above, the idea is to use the multiple wedge product of $d(d_x P)$ with itself to discover when the Frobenius integrability conditions ensure that Eq. 5.11 holds. The integrability condition is that if

$$\begin{aligned} (d(d_x P))^{k+1} \wedge d_x P &\equiv 0 \\ (d(d_x P))^k \wedge d_x P &\neq 0, \end{aligned} \tag{5.12}$$

then Eq. 5.11 is true. As discovered by the discussion about Eq. 5.9, this relationship necessarily is based on how $d_x P$ can be expressed relative to the basis representation for $d(d_x P)$.

Theorem. *For $n = 2$ agents and a performance function*

$$P : R^{k_1} \times R^{k_2} \to R,$$

let integers c_1 and c_2 be such that

$$\begin{aligned} (d(d_x P))^{c_1+1} \wedge d_x P \equiv 0, \quad (d(d_x P))^{c_1} \wedge d_x P \neq 0, \\ (d(d_y P))^{c_2+1} \wedge d_y P \equiv 0, \quad (d(d_y P))^{c_2} \wedge d_y P \neq 0. \end{aligned}$$

There exists a (local) organization with $dim(M) \leq 2 + min(c_1, c_2)$.

By comparing this estimate with Chen's Theorem, it follows that very tight estimates now exist for the dimension of M. Moreover, the above indicates how to find the $\omega_{i,j}$ to be added to the ideals; in turn, how to address the problem of creating the communication network. To illustrate with the dot product of $\mathbf{x}, \mathbf{y} \in R^4$, recall from Chen's result that $dim(M) \geq 5$. Because $-d(d_x P) = \sum_{i=1}^4 dx_i \wedge dy_i$, it follows that $(d(d_x P))^3 \wedge d_x P \neq 0$, and $(d(d_x P))^4 \wedge d_x P \equiv 0$. According to the above theorem, there is an organization where $dim(M) \leq 5$. One $dim(M) = 5$ organization is the parameter transfer given above.

As a concluding comment, extensions for $n \geq 2$ agents, for different privacy conditions, and for $P : \prod_{j=1}^n R^{k_j} \to R^a, a \geq 2$ are obtained in much the same way. The main difficulty is an algebraic one; e.g., the difficulty is to keep track of which ϕ_j's and ψ_j's are in the span of entries already added to the ideals. Conclusions in this direction will be reported elsewhere.

REFERENCES

[C_1] Chen, P, 1990, A lower bound for the dimension of the message space of the decentralized mechanisms realizing a given goal.

[C_2] Chen, P., 1989, *"On the efficiency and complexity of computational and economic processes,"* Ph. D. dissertation (Northwestern University).

[F] Flanders, H., *"Differential Forms with Applications to the Physical Sciences,* Dover Publications, New York, 1989.

[Ga] Gale, D., 1960, A note on revealed preference, Economica, 348- 354.

[G] Gardner, R., 1968, Some applications of the retraction theorem in exterior algebra, J. Diff. Geom. **2**, 25-31.

[Ho] Houthakker, H. S., 1950, Revealed preference and the utility function, Economica, 159-174.

[H_1] Hurwicz, L.,1960, Optimality and informational efficiency in resource allocation processes, in: K. Arrow, S. Karlin, P. Suppes, eds., *"Mathematical methods in the Social Sciences"* (Stanford University Press), 27-46.

[H_2] Hurwicz, L., 1986, On informational decentralization and efficiency in resource allocation mechanisms, in: S. Reiter, ed., *"Studies in Mathematical Economics"*, Mathematical Association of America, Washington, D.C.

[HRS] Hurwicz, L., S. Reiter, and D. G. Saari, 1978, On constructing mechanisms with message spaces of minimal dimension for smooth performance functions, Mimeo. (University of Minnesota.)

[L] Lehmann, E.L., 1986, *"Testing Statistical Hypotheses,"* Wiley, New York.

[MR] Mount, K., and S. Reiter, 1974, The informational size of message spaces, JET **8**, 66-78.

[S_1] Saari, D. G., (1984), A method for constructing message systems for smooth performance functions, JET **33**, 249-274.

[S_2] Saari, D. G., 1985, The representation problem and the efficiency of the price mechanism, J. Math Econ, **14**. 135-167.

[S_3] Saari, D. G., 1988, On the types of information and on mechanism design, Jour Computational and Applied Math. **22**, 231-242.

[S_4] Saari, D. G., 1990, On the design of complex organizations and distributive algorithms, Complexity Theory **6**. 102-118.

[S_5] Saari, D. G., 1991, Calculus and Extensions of Arrow's Theorem, Jour Math Econ.

[S_6] Saari, D. G., 1990, Susceptibility to manipulation, Public Choice **64**, 21-41.

[Sam_1] Samuelson, P, 1938, A note on the pure theory of consumer's behaviour; and an addendum, Economica, 61-71.

[Sam_2] Samuelson, P., 1950, The problem of integrability in utility theory, Economica, 75-105.

[Sav] Savage, L., 1954, *"The Foundations of Statistics,"* John Wiley.

[Sp] Spivak, M., 1970, *"Differential Geometry, Vol 1,"* Publish or Perish, Inc., Boston.

[V] Varian, H., 1978, *"Microeconomic Analysis,"* W. W. Norton, New York.

[W] Warner, F., 1970, *"Foundations of Differentiable Manifolds and Lie Groups,"* Scott Foresman, Glenview, Ill.

[Wi] Williams, S., 1982, *A geometric study of smooth decentralized economic mechanisms,* Ph. D. dissertation (Northwestern University).

DEPARTMENT OF MATHEMATICS, NORTHWESTERN UNIVERSITY, EVANSTON, ILLINOIS 60208-2730