

**ECN 612 - HANDOUT - FALL 2011**  
**Chapter 3: Part 2**

**MATH**

Recall that if  $f : A \rightarrow B$  is a function, we may use  $f(A)$  to denote

$$\{b \in B : f(a) = b \text{ for some } a \in A\}.$$

**Definition 1** A function  $f : A \rightarrow B$  is injective (or one-to-one) if for each pair of distinct points in  $A$ , their images under  $f$  are distinct, i.e.,  $a = b$  if and only if  $f(a) = f(b)$ .

**Math Fact** If  $f : A \rightarrow f(A)$  is injective, then  $f^{-1} : f(A) \rightarrow A$  is injective.

**Math Fact** If  $f : A \rightarrow B$  and  $g : B \rightarrow C$ , are both injective functions, where  $f(A) = B$ , then  $g \circ f : A \rightarrow C$  is an injective function.

**CONSTRUCTING THE MECHANISM**

We assume throughout that any encoding function  $\nu : T \rightarrow \nu(T)$  is injective. Therefore, its inverse  $\nu^{-1} : \nu(T) \rightarrow T$  is also injective. Also, since  $\nu$  is injective, it follows that for our purposes, you may omit Lemma 8 and its Corollary on the previous handout. Finally,  $\nu^{-1} \circ \nu(t) = t$ , where  $t \in T$ .

In the next two parts, we show that given the following, we can derive a mechanism realizing the goal function  $F : \Theta \rightarrow Z$ .

- a goal function  $F : \Theta \rightarrow Z$
- a covering  $\mathcal{C}$  of  $\Theta$  that is generated by a self-belonging correspondence  $V : \Theta \Rightarrow \Theta$ , i.e.,  $\mathcal{C}_V = \mathcal{C} = \{K : K = V(\theta) \text{ for some } \theta \in \Theta\}$  (when  $K = V(\theta)$ ,  $\theta$  is said to be a *generator* of  $K$  and may be denoted by  $\theta_K$ ).
- $\mathcal{C}$  is contour contained, i.e., if  $K \in \mathcal{C}$ ,  $K \subseteq F^{-1}(z)$  for some  $z \in Z$  (or if  $K \in \mathcal{C}$ , the goal function  $F$  is constant on  $K$ )
- $\mathcal{C}$  has an SDR  $\Lambda : \mathcal{C} \rightarrow \Theta$ , with set  $T = \Lambda(\mathcal{C})$  a transversal for  $\mathcal{C}$
- there is an encoding function  $\nu : T \rightarrow \nu(T)$

The first mechanism is not necessarily privacy preserving, the second is. In both cases, define the function  $h : M' \rightarrow Z$  by

$$h = F \circ \nu^{-1}, \tag{1}$$

where to be precise, we should really replace  $F$  with  $F_T$  the restriction of  $F$  to  $T$ , i.e.,

$$F_T(\theta) = F(\theta),$$

where  $F_T : T \rightarrow Z$  (note that  $T \subseteq \Theta$ ), but we will not do so. Since  $\nu$  is injective,  $\nu^{-1}$  is a function and since  $F$  is a function, it follows that  $h$  is as well.

**A Mechanism That Isn't Necessarily Privacy Preserving**

Now we define the equilibrium message correspondence. Define  $\Omega : \Theta \Rightarrow \mathcal{C}$  by

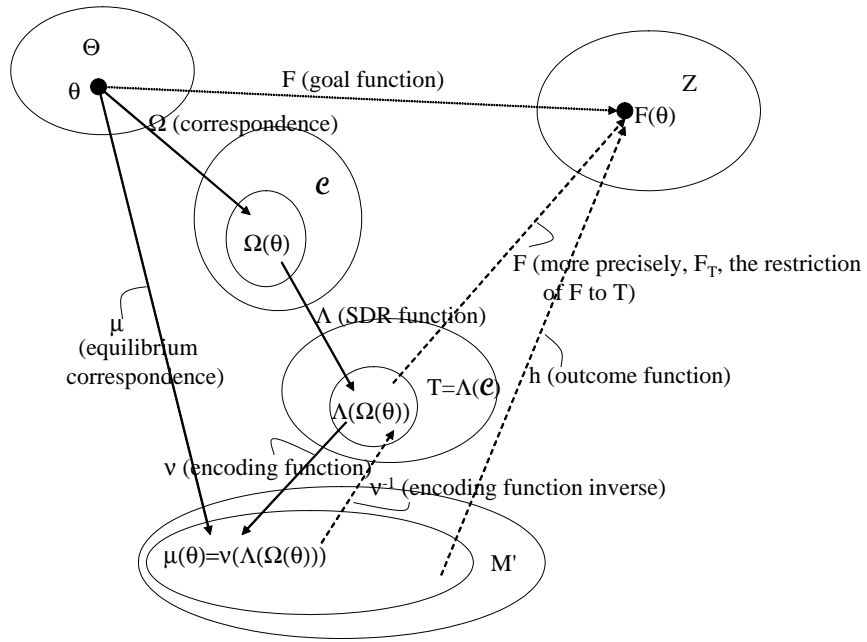
$$\Omega(\theta) = \{K \in \mathcal{C} : \theta \in K\}. \tag{2}$$

We take the equilibrium message space to be

$$M' = \nu(T), \tag{3}$$

where  $\nu$  is the encoding function. Define  $\mu = \nu \circ \Lambda \circ \Omega : \Theta \Rightarrow M'$  as

$$\mu(\theta) = \nu(\Lambda(\Omega(\theta))). \tag{4}$$



In the diagram above,  $\Omega(\theta)$  is the set of sets in the covering  $\mathcal{C}$  of  $\Theta$  which contain  $\theta$ ;  $\Lambda(\Omega(\theta))$  is the set of distinct representatives associated with those sets;  $\nu(\Lambda(\Omega(\theta)))$  is the image under the encoding function  $\nu$  of those distinct representatives.

We show that the mechanism  $\pi = (M', \mu, h)$  realizes  $F$ , i.e., we show that for every  $\theta \in \Theta$ ,  $F(\theta) = h(\mu(\theta))$ . From (1), (2), and (4),

$$\mu = \nu \circ \Lambda \circ \Omega, \quad (5)$$

$$h = F \circ \nu^{-1}, \quad (6)$$

and

$$\Omega(\theta) = \{K \in \mathcal{C} : \theta \in K\}. \quad (7)$$

Because the covering  $\mathcal{C}$  is  $F$ -cc, if

$$\bar{\theta} \in K \text{ for some } K \in \Omega(\theta), \text{ then } F(\bar{\theta}) = F(\theta). \quad (8)$$

By the definition of an SDR, part (i), for every  $K \in \mathcal{C}$ ,

$$\Lambda(K) \in K. \quad (9)$$

It follows from (7), (8), and (9) that for every  $K \in \Omega(\theta)$ ,

$$F(\Lambda(K)) = F(\theta).$$

Therefore, for every  $\theta \in \Theta$ ,

$$F(\Lambda(\Omega(\theta))) = F(\theta). \quad (10)$$

But by (5), (6), and (10),

$$F(\theta) \underset{\text{by (10)}}{=} F(\Lambda(\Omega(\theta))) = F(\nu^{-1}(\nu(\Lambda(\Omega(\theta)))) = \underbrace{F \circ \nu^{-1}}_{=h \text{ by (6)}} \left( \underbrace{\nu \circ \Lambda \circ \Omega(\theta)}_{=\mu \text{ by (5)}} \right) = h(\mu(\theta)). \quad \square$$

## Deriving A Mechanism That Is Privacy Preserving

We derive a mechanism which is privacy preserving from the previous construction. We do this for the case of two agents only (see your text for the case of  $N$  agents). Define  $h$  as at (1). What we change is how we define  $\Omega$  and  $\mu$ . Specifically, we replace  $\Omega : \Theta \Rightarrow \mathcal{C}$  with two correspondences,  $\Omega^1 : \Theta^1 \Rightarrow \mathcal{C}$  and  $\Omega^2 : \Theta^2 \Rightarrow \mathcal{C}$ , and we define  $\mu^1 : \Theta^1 \Rightarrow M$ ,  $\mu^2 : \Theta^2 \Rightarrow M$ , and  $\mu : \Theta^1 \times \Theta^2 \Rightarrow M'$ , where  $\mu(\theta) = \mu^1(\theta^1) \cap \mu^2(\theta^2)$ .

First, we define  $\Omega^i : \Theta^i \Rightarrow \mathcal{C}$ ,  $i = 1, 2$ , as

$$\Omega^1(\theta^1) = \{K \in \mathcal{C} : \text{there exists } \theta^2 \in \Theta^2 \text{ such that } (\theta^1, \theta^2) \in K\} \quad (11)$$

and

$$\Omega^2(\theta^2) = \{K \in \mathcal{C} : \text{there exists } \theta^1 \in \Theta^1 \text{ such that } (\theta^1, \theta^2) \in K\}. \quad (12)$$

Now consider the sets

$$\Lambda(\Omega^i(\theta^i)) \subseteq T,$$

$i = 1, 2$ . Each is a set of distinct representatives corresponding to the sets indicated; specifically, there is a one-to-one relationship between elements of  $\Omega^i(\theta^i)$  (which are sets) and elements of  $\Lambda(\Omega^i(\theta^i))$ . Since  $\nu : T \rightarrow M$  is injective ( $M$  is defined below), there is a one-to-one relationship between elements of  $\Omega^i(\theta^i)$  (which are sets) and elements of  $\nu(\Lambda(\Omega^i(\theta^i)))$ .

Now define  $M = \nu(\Lambda(\Omega^1(\theta^1))) \cup \nu(\Lambda(\Omega^2(\theta^2)))$  and define  $\mu^i : \Theta^i \Rightarrow M$ ,  $i = 1, 2$ , by

$$\mu^1(\theta^1) = \{m \in M : m = \nu(\Lambda(K)) \text{ for some } K \in \Omega^1(\theta^1)\} \quad (13)$$

and

$$\mu^2(\theta^2) = \{m \in M : m = \nu(\Lambda(K)) \text{ for some } K \in \Omega^2(\theta^2)\}. \quad (14)$$

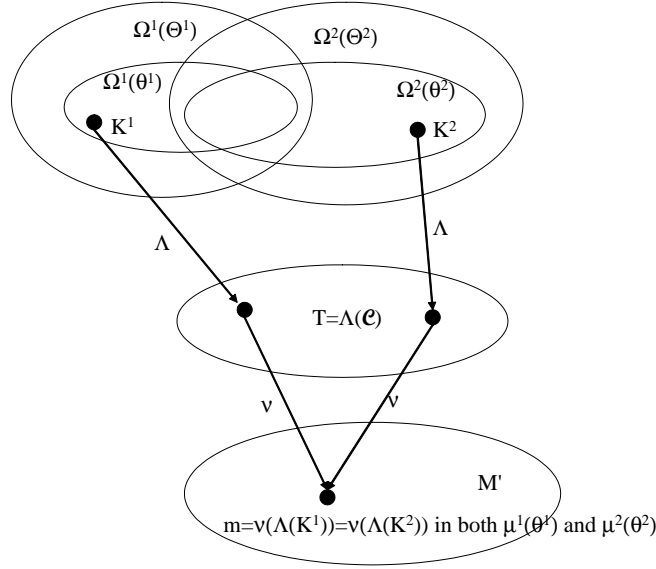
Define  $\mu : \Theta = \Theta^1 \times \Theta^2 \Rightarrow M'$  by

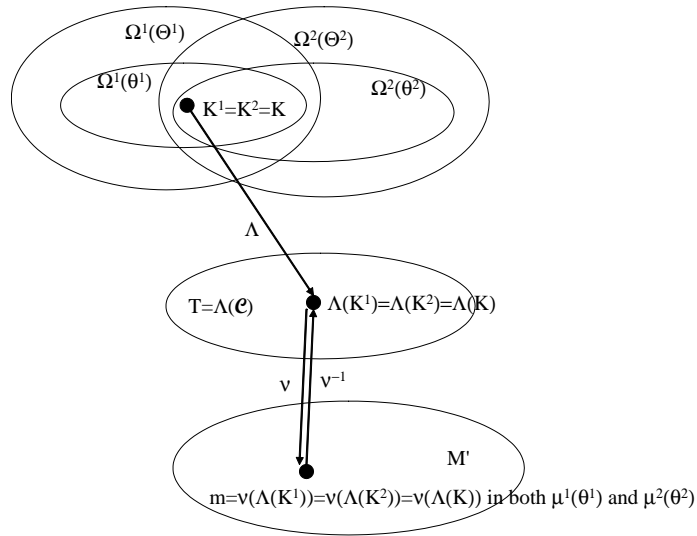
$$\mu(\theta) = \mu^1(\theta^1) \cap \mu^2(\theta^2). \quad (15)$$

(We end up showing that  $M' = \nu(\Lambda(\Omega^1(\theta^1))) \cap \nu(\Lambda(\Omega^2(\theta^2)))$ .)

Let  $m \in \mu(\theta) = \mu^1(\theta^1) \cap \mu^2(\theta^2)$  be arbitrary. We show that there exists  $K \in \Omega^1(\theta^1) \cap \Omega^2(\theta^2)$  such that  $m = \nu(\Lambda(K))$ . This idea is represented in the following diagrams. Given that  $m \in \mu^1(\theta^1)$  and  $m \in \mu^2(\theta^2)$ , use (13) and (14) to find that there exist  $K^1 \in \Omega^1(\theta^1)$  and  $K^2 \in \Omega^2(\theta^2)$  such that

$$\nu(\Lambda(K^1)) = m = \nu(\Lambda(K^2)). \quad (16)$$





But since  $\nu$  and  $\Lambda$  are both one-to-one functions, so is  $\nu \circ \Lambda$ , and therefore,  $K^1 = K^2 = K \in \Omega^1(\theta^1) \cap \Omega^2(\theta^2)$ ; we rewrite (16) as

$$m = \nu(\Lambda(K)). \quad (17)$$

It is also the case that  $\theta \in K$  (since  $K \in \Omega^1(\theta^1) \cap \Omega^2(\theta^2)$ ) and that  $\Lambda(K) \in K$  (by SDR (i)). Since  $\mathcal{C}$  is an  $F$ -cc covering of  $\Theta$ , it follows that

$$F(\theta) = F(\Lambda(K)). \quad (18)$$

Now we show that the mechanism realizes  $F$ . That is, we show that if  $m \in \mu(\theta) = \mu^1(\theta^1) \cap \mu^2(\theta^2)$ , then  $h(m) = F(\theta)$ . We find that

$$h(m) \underset{\text{by (1)}}{=} F(\nu^{-1}(m)) \underset{\text{by (17)}}{=} F(\nu^{-1}(\nu(\Lambda(K)))) = F(\Lambda(K)) \underset{\text{by (18)}}{=} F(\theta). \quad \square$$

## REFERENCES

Hurwicz and Reiter.

Munkres, *Topology*.