

# Chapter 26

## Common, Correlated, and Private Information in Control of Decentralized Systems

Jan H. van Schuppen

### 26.1 Introduction

Decentralized control involves the exchange of information of the two or more controllers influencing the decentralized control system. The communication between controllers may be carried out via the plant, then called signaling, or directly in the case of control with direct communication between controllers. Therefore, there is a need for understanding the communication exchange in particular: What information of a controller is of interest to which other controllers?

The problem of common and private information in decentralized control is then to formulate concepts, to develop theory and algorithms, and to use this theory for control of distributed or of decentralized systems.

In game theory, the same concepts and theory are useful. In case of zero-sum games, each of the players wants to prevent the communication of private information so as to obtain an advantage over other players.

In this short chapter, definitions of common, of private, and of correlated information are proposed. The case of Gaussian random variables is analyzed using the canonical variable decomposition. For a particular Gaussian stochastic control system, a decomposition is presented. Further research is mentioned.

The research issue of common and of private information in decentralized control was initiated by Ho, see [1, 2]. There is a clear link of the concepts of common and private information with those of information theory. The common information of two random variables was formulated and explored by Wyner, see [3, 4]. But that theory goes less far than is proposed in this paper.

---

J.H. van Schuppen (✉)

Van Schuppen Control Research, 1103 KB Amsterdam, The Netherlands

e-mail: jan.h.van.schuppen@xs4all.nl

© Springer International Publishing Switzerland 2015

J.H. van Schuppen and T. Villa (eds.), *Coordination Control of Distributed Systems*,

Lecture Notes in Control and Information Sciences 456,

DOI 10.1007/978-3-319-10407-2\_26

## 26.2 Motivation

Why is decomposition of the information available to a controller of a decentralized control system into common and private information useful for decentralized and for distributed control?

Suppose that there exist appropriate definitions of common, private, and correlated information of any controller with respect to the other controllers. Suppose also that a decomposition of the decentralized control system has been made such that the structure of the system matrix and that of the observation matrix of any controller are decomposed into the common, private, and correlated parts. To simplify the discussion, first assume that the decentralized control system has only two controllers.

In a decentralized control system, which information components should a controller send to the other controller? Recall that in decentralized control all controllers have the same control objective. There is no need to send the common information because both controllers observe the same output process. The private information of a controller may be useful to the other controller but only if it would help the other controller to better achieve the common control objectives. The case of information that is neither common nor private is more complicated; it depends on the amount of correlation involved. This aspect has to be treated in the planned theory. There are additional aspects in case there are many controllers; this case requires slightly adjusted concepts.

The communication of the information requires concepts and theory of coding theory and of real-time communication not discussed here at length.

## 26.3 Problem

**Problem 26.1** The *common and private information problem*. Formulate concepts, develop theory, and formulate algorithms for the use of common, private, and correlated information in control of decentralized control systems. Formulate decompositions of decentralized control systems in which the different concepts are distinguished.

## 26.4 Concepts

As to the formulation of the concepts of common and of private information, it is required to be as general as possible. From this point of view, a formulation in terms of stochastic systems with  $\sigma$ -algebras as spaces is preferred. In this chapter, attention is first focused on a  $\sigma$ -algebraic formulation and subsequently, attention is restricted to Gaussian random variables and to decentralized systems with Gaussian distributions for which more explicit concepts can be formulated.

Thus, for the observation vectors  $(y_1, y_2)$  with  $y_i : \Omega \rightarrow \mathbb{R}^{p_i}$  for  $i = 1, 2$ , consider the  $\sigma$ -algebras generated by these variables  $(F^{y_1}, F^{y_2})$ . Instead, one works with abstract spaces, the tuple of  $\sigma$ -algebras  $(F_1, F_2)$ , where one may associate with each  $F_i$  an observation space. Call these objects the *observation*  $\sigma$ -algebras. Denote the positive real line by  $\mathbb{R}_+ = [0, \infty) \subset \mathbb{R}$  and the associated Borel  $\sigma$ -algebra on that set by  $B(\mathbb{R}_+)$ .

Call the tuple of  $\sigma$ -algebras  $F_1, F_2$  of a probability space  $(\Omega, F, P)$  *conditionally independent* given a third  $\sigma$ -algebra  $G \subseteq F$  if the following factorization property holds,

$$E[x_1 x_2 | G] = E[x_1 | G] E[x_2 | G], \quad \forall x_i \in L(\Omega, F_i; \mathbb{R}_+, B(\mathbb{R}_+)); \quad (26.1)$$

$$L(\Omega, F_i; \mathbb{R}_+, B(\mathbb{R}_+)) = \{x : \Omega \rightarrow \mathbb{R}_+ \mid x \text{ a random variable, } F_i\text{-measurable}\}.$$

Denote by  $(F_1, F_2 | G) \in \text{CI}$  that this triple of  $\sigma$ -algebras is *conditional independent*.

The problem is to define concepts on the relation of the two observation spaces. This will be done by the concept of common and privated information defined next.

**Definition 26.1** Consider two observation  $\sigma$ -algebras  $(F_1, F_2)$ .

- (a) Define the *common information* of the two observation  $\sigma$ -algebras as their intersection,

$$G_{\text{com}} = F_1 \cap F_2. \quad (26.2)$$

It follows immediately that the common information is a  $\sigma$ -algebra.

- (b) Call a  $\sigma$ -algebra  $G$  a *sufficient  $\sigma$ -algebra* for the tuple of  $\sigma$ -algebras  $(F_1, F_2)$  if it makes  $F_1$  and  $F_2$  conditionally independent,  $(F_1, F_2 | G) \in \text{CI}$ .
- (c) Define the *private information* of the observation  $\sigma$ -algebra  $F_1$  with respect to the  $\sigma$ -algebra  $G$  as a  $\sigma$ -algebra  $F_{1,p} \subseteq F_1$  which is a complement of the  $\sigma$ -algebra  $G$ . Thus,  $F_{1,p}$  is characterized by the three conditions,  
 (1)  $F_{1,p}$  is a  $\sigma$ -algebra; (2)  $F_{1,p} \subseteq F_1$ ; and (3)  $F_1 = G \vee F_{1,p}$ . A  $\sigma$ -algebra which is the private information of  $F_1$  with respect to  $G$  always exists;  $F_{1,p} = F_1$  will do, but that is also a trivial choice. More interesting is the next concept. The *independent private information* is defined to be a private information  $\sigma$ -algebra  $F_{1,p}$  if in addition the condition holds  
 (4)  $F_{1,p}$  and  $G$  are independent  $\sigma$ -algebras.

A private information  $F_{2,p} \subseteq F_2$  is then defined by symmetry.

A sufficient  $\sigma$ -algebra which makes the two  $\sigma$ -algebras  $F_1, F_2$  conditionally independent always exists, for example,  $F_1 \vee F_2$  will do. Such a  $\sigma$ -algebra is not unique; in general, there are many in continuous probability spaces even uncountably many. Of interest is therefore a minimal  $\sigma$ -algebra which makes a tuple of  $\sigma$ -algebras conditionally independent. Minimality refers to the ordering defined by set inclusion. A minimal sufficient  $\sigma$ -algebra is not unique in general. Of interest is therefore a classification of all such  $\sigma$ -algebras. See [5, 6] for further information.

The private  $\sigma$ -algebra  $F_{1,p}$  always exists. But it is not unique, there exist many such objects. Of interest is therefore a minimal private observation space. How this is to be formulated is not yet clear. An independent private observation space may not exist; there exists an example where the observation spaces are generated by finite-valued random variables. These concepts are subject of further investigation.

### 26.5 Common and Private Information of Gaussian Random Variables

Based on the concept of the canonical variable decomposition, one can define the concepts of common, correlated, and private information for a tuple of Gaussian random variables.

**Definition 26.2** Consider a tuple of Gaussian random variables  $y_i : \Omega \rightarrow \mathbb{R}^{p_i}$ ,  $i = 1, 2$ . Assume that these random variables have been transformed by a linear transformation,  $(y_1, y_2) \mapsto (S_1 y_1, S_2 y_2)$  for matrices  $S_1, S_2$ , to the *canonical variable decomposition* defined by the representation,

$$(y_1, y_2) \in G(0, Q),$$

$$Q = \left( \begin{array}{ccc|ccc} I_{p_{11}} & 0 & 0 & I_{p_{21}} & 0 & 0 \\ 0 & I_{p_{12}} & 0 & 0 & D & 0 \\ 0 & 0 & I_{p_{13}} & 0 & 0 & 0 \\ \hline I_{p_{21}} & 0 & 0 & I_{p_{21}} & 0 & 0 \\ 0 & D & 0 & 0 & I_{p_{22}} & 0 \\ 0 & 0 & 0 & 0 & 0 & I_{p_{23}} \end{array} \right) \in \mathbb{R}^{p \times p}, \tag{26.3}$$

$$p, p_1, p_2, p_{11}, p_{12}, p_{13}, p_{21}, p_{22}, p_{23} \in \mathbb{N},$$

$$p = p_1 + p_2, p_1 = p_{11} + p_{12} + p_{13}, p_2 = p_{21} + p_{22} + p_{23},$$

$$p_{11} = p_{21}, p_{12} = p_{22},$$

$$D = \text{Diag}(d_1, \dots, d_{p_{12}}), 1 > d_1 \geq d_2 \geq \dots \geq d_{p_{12}} > 0, \tag{26.4}$$

$$y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} y_{11} \\ y_{12} \\ y_{13} \\ y_{21} \\ y_{22} \\ y_{23} \end{pmatrix}, y_{ij} : \Omega \rightarrow \mathbb{R}^{p_{ij}}, i = 1, 2, j = 1, 2, 3.$$

Call then  $Q$  the *covariance matrix* of the random variables  $(y_1, y_2)$  in the canonical variable decomposition. This is a slight abuse of terminology because only its (1,2)-block is usually called the covariance matrix of  $(y_1, y_2)$ .

Define then

$y_{11} = y_{21}$	Common information of $y_1$ and $y_2$
$y_{12}$	Correlated information of $y_1$ with respect to $y_2$
$y_{13}$	Independent private information of $y_1$ with respect to $y_2$
$(y_{11}, y_{12})$	Sufficient information of $y_1$ for the tuple $y_1, y_2$
$y_{21} = y_{11}$	Common information of $y_1$ and $y_2$
$y_{22}$	Correlated information of $y_2$ with respect to $y_1$
$y_{23}$	Independent private information of $y_2$ with respect to $y_1$
$(y_{21}, y_{22})$	Sufficient information of $y_2$ for the tuple $y_1, y_2$

**Proposition 26.1** *The following properties hold for the common, correlated, and private information of a pair of Gaussian random variables.*

- (a) *The three components  $y_{11}, y_{12}, y_{13}$  of  $y_1$  are independent random variables.*
- (b) *The three components  $y_{21}, y_{22}, y_{23}$  of  $y_2$  are independent random variables.*
- (c) *The equality  $y_{11} = y_{21}$  of these random variables holds almost surely; hence, the term common information is appropriate.*
- (d) *The tuple of random variables  $(y_{12}, y_{22})$  is correlated as shown by the formula*

$$E[y_{12}y_{22}^T] = D = \text{Diag}(d_1, \dots, d_{p_{12}}). \tag{26.5}$$

*Note that the different components of  $y_{12}$  and of  $y_{22}$  are independent random variables; thus,  $y_{12,i}$  and  $y_{12,j}$  are independent, and  $y_{22,i}$  and  $y_{22,j}$  are independent, and  $y_{12,i}$  and  $y_{22,j}$  are independent, for all  $i \neq j$ , and that  $y_{1,j}$  and  $y_{2,j}$  for  $j = 1, \dots, p_{12} = p_{22}$  are correlated.*

- (e) *The random variable  $y_{13}$  is independent of  $y_2$ , hence justifying the term of independent private information of  $y_1$  with respect to  $y_2$ . Similarly, the random variable  $y_{23}$  is independent of  $y_1$*

*Proof* The results are immediately obvious from the fact that the random variables are all jointly Gaussian and from the covariance matrix (26.3) of the tuple of random variables  $(y_1, y_2)$  in the canonical variable decomposition.

**Proposition 26.2** *Consider the concepts of common, correlated, and private information for a tuple of Gaussian random variables of Definition 26.2. Then, the following conditional independence properties hold:*

$$(F^{y_1}, F^{y_2} | F^{y_{11}, y_{12}}) \in \text{CI}; \quad (F^{y_1}, F^{y_2} | F^{y_{21}, y_{22}}) \in \text{CI}; \tag{26.6}$$

$$(F^{y_{11}, y_{12}}, F^{y_{21}, y_{22}} | F^{y_{11}, y_{12}}) \in \text{CI}; \quad (F^{y_{11}, y_{12}}, F^{y_{21}, y_{22}} | F^{y_{21}, y_{22}}) \in \text{CI}. \tag{26.7}$$

*These formulas display the sufficient information of the tuple of random variables  $(y_1, y_2)$ .*

The above decomposition of a tuple of Gaussian random variables allows conjectures about the use of common, private, and sufficient information for information exchange and control in decentralized or distributed systems. Consider the setting of the decomposed Gaussian random variables of the previous section, see Definition 26.2. The independent private information of Controller 1 with respect to Controller 2,  $y_{13}$ , is useful to Controller 2 for its tasks of estimation and control. Therefore, that independent private information  $y_{13}$  is best sent from Controller 1 to Controller 2. The information of Controller 1 which is correlated with the information of Controller 2, above denoted by  $y_{12}$ , may be of interest to Controller 2 only if the correlation coefficient  $d_i$  is sufficiently high. If the correlation coefficient is low, then it does not seem of interest to send the information. See Chap. 27 for an application.

## 26.6 Common and Private Information of Gaussian Systems

There follows a first definition of a Gaussian system in which the common and private information is made explicit in the decomposition of the system. At the time this chapter is completed, there does not yet exist a procedure to decompose an arbitrary Gaussian system into its common and private components.

**Definition 26.3** A Gaussian system with a common–private information decomposition. Consider a Gaussian system with the following rather specific decomposition.

$$x(t+1) = \begin{pmatrix} A_{11} & 0 & 0 \\ 0 & A_{22} & 0 \\ 0 & 0 & A_{33} & 0 \\ 0 & 0 & 0 & A_{44} \end{pmatrix} x(t) + \begin{pmatrix} M_{11} & 0 & 0 \\ 0 & M_{22} & 0 \\ 0 & 0 & M_{33} & 0 \\ 0 & 0 & 0 & M_{44} \end{pmatrix} v(t), \quad (26.8)$$

$$x(t_0) = x_0,$$

$$y(t) = \begin{pmatrix} y_{11}(t) \\ y_{12}(t) \\ y_{13}(t) \\ y_{21}(t) \\ y_{22}(t) \\ y_{23}(t) \end{pmatrix} = \begin{pmatrix} C_{11} & 0 & 0 & 0 \\ 0 & C_{12} & 0 & 0 \\ 0 & 0 & C_{13} & 0 \\ C_{11} & 0 & 0 & 0 \\ 0 & C_{22} & 0 & 0 \\ 0 & 0 & 0 & C_{24} \end{pmatrix} x(t) + \begin{pmatrix} N_{11} & 0 & 0 & 0 \\ 0 & N_{22} & 0 & 0 \\ 0 & 0 & N_{33} & 0 \\ N_{11} & 0 & 0 & 0 \\ 0 & N_{52} & 0 & 0 \\ 0 & 0 & 0 & N_{44} \end{pmatrix} w(t).$$

In this decomposition,  $y_{11}$  and  $y_{21}$  are called the *common output processes* of Observer 1 and Observer 2. The tuple  $(y_{12}, y_{22})$  is called the *correlated output processes* of the two output processes. The process  $y_{13}$  is called the *private output process of Observer 1* relative to Observer 2, while  $y_{23}$  is called the *private output process of Observer 2* relative to Observer 1. The stochastic processes  $v$  and  $w$  are discrete time-independent Gaussian white noise processes.

The usefulness of the decomposition of the outputs and states of the above-defined common–private Gaussian system is then directly obvious from the terms and from the decomposition of the system matrices.

Further research is needed into the general decomposition of a Gaussian system by linear transformations of state and of output spaces. A further problem is to relate the informational decomposition also to the cost function or the control objectives.

## 26.7 Further Research

The following research issues seem useful for control of decentralized and of distributed control systems.

1. Investigate further the  $\sigma$ -algebraic concepts of common, private, and sufficient information. Investigate decompositions of finite-valued random variables in regard to common and private information.
2. Explore decompositions of a triple and of a higher number of tuples of random variables in regard to common, private, and correlated information. Particular cases include Gaussian random variables and finite-valued random variables.
3. Investigate decompositions of decentralized stochastic control systems such that the decomposition displays the common, private, and correlated information.
4. Investigate the use of the concepts of common and private information for state estimation or filtering by two or more controllers. See Chap. 27 for an initial approach to this problem.
5. Investigate the interaction of information and control, which requires new concepts of information decomposition.

## 26.8 Further Reading

A reader novel to the topic is advised to read the tutorial paper by Ho, [7], and a paper relating information decompositions to information theory, see [8]. This chapter is related to the following other chapters of the book: Chaps. 18, 20, and 24.

Early papers on the concepts of common and of private information are [1, 9]. The  $\sigma$ -algebraic concept of common information was published by Aumann, see [10].

The canonical variable decomposition of Gaussian random variables was proposed by Hotelling, see [11]. A book about the canonical variable decomposition and its applications is [12]. The use of this decomposition for stochastic realization of Gaussian random variables is described in [13].

The decomposition of Gaussian systems in regard to common and private information sketched in this paper is under development by the author. The geometric theory of linear systems used may be found in the book by Wonham, [14]. Decompositions of coordinated linear systems are derived in [15]. The  $\sigma$ -algebraic stochastic realization problem is treated in [5, 6].

Books on information theory include [16–18]. The concept of mutual information of two variables has been investigated from the information theoretic viewpoint in [3, 4, 19]. Related to the topic of this chapter is the *agreement problem*. The reader is referred to the papers of Teneketzis and Varaiya for agreement in the context of control theory [20, 21], and to the paper by Aumann [10].

## References

1. Hexner G, Ho YC (1977) Information structure: common and private. *IEEE Trans Inf Theor* 23:390–393
2. Ho YC, Hexner G, Martin C (1976) Two person information structure. Part I: information structure: common and private. Part II: private information structures of A with respect to B. Report 663, Division of Engineering and Applied Physics, Harvard University, Cambridge, MA, USA, July 1976
3. Wyner AD (1975) The common information of two dependent random variables. *IEEE Trans Inf Theor* 21:163–179
4. Wyner AD (1978) A definition of conditional mutual information for arbitrary ensembles. *Inf Control* 38:51–59
5. van Schuppen JH (1982) The strong finite stochastic realization problem—Preliminary results. In: Bensoussan A, Lions JL (eds) *Analysis and optimization of systems*, vol 44., *Lecture Notes in Control and Information Sciences* Springer, Berlin, pp 179–190
6. van Schuppen JH (2000) Stochastic realization of  $\sigma$ -algebras. In: *Proceedings of 14th international symposium MTNS (published on CD-ROM only)*, Université de Perpignan, Perpignan
7. Ho YC (1980) Team decision theory and information structures. *Proc IEEE* 68:644–654
8. Ho YC, Karstner P, Wong E (1978) Teams, signaling and information theory. *IEEE Trans Autom Control* 23:305–311
9. Dick R, Hexner G, Ho Y (1977) On common information in decision problems. *IEEE Trans Inf Theor* 23:393–396
10. Aumann RJ (1976) Agreeing to disagree. *Ann Statist* 4:1236–1239
11. Hotelling H (1936) Relation between two sets of variates. *Biometrika* 28:321–377
12. Gittens RD (1985) *Canonical analysis—A review with applications in ecology*. Springer, Berlin
13. van Putten C, van Schuppen JH (1983) The weak and strong Gaussian probabilistic realization problem. *J Multivariate Anal* 13:118–137
14. Wonham WM (1979) *Linear multivariable control: a geometric approach*. Springer, Berlin
15. Kempker PL, Ran A, van Schuppen JH (2012) Controllability and observability of coordinated linear systems. *Linear Algebra its Appl* 437:121–167
16. Cover TM, Thomas JA (1991) *Elements of information theory*. Wiley, New York
17. Gallager RG (1968) *Information theory and reliable communication*. Wiley, New York
18. Ihara S (1993) *Information theory for continuous systems*. World Scientific, Singapore
19. Witsenhausen HS (1976) Some remarks on the concept of state. In: *Directions in large-scale systems, many-person optimization, and decentralized control (Proceedings Symposium, Wakefield, MA, 1975)*, Plenum, New York, pp 69–75
20. Teneketzis D, Varaiya P (1984) Consensus in distributed estimation with inconsistent beliefs. *Syst Control Lett* 4:217–221
21. Washburn RB, Teneketzis D (1984) Asymptotic agreement among communicating decision-makers. *Stochastics* 13:103–129