Common randomness and distributed control : a counterexample

Venkat Anantharam [a,*], Vivek Borkar [b]

[a] *EECS Department, University of California, Berkeley, CA 94720, USA*

[b] *School of Technology and Computer Science, Tata Institute for Fundamental Research, Homi Bhabha Road, Mumbai 400005, INDIA*

Abstract

When agents collaborate to perform a control task, it is of interest to characterize the set of joint probability distributions they can achieve on their joint action space when they are passively provided with external common randomness. We give a simple counterexample to a natural conjecture about this class of joint distributions.

Key words: common randomness, distributed control, game theory, information theory, sensor networks, stochastic control

1 Introduction

Consider a multiagent control problem where each agent takes actions based on its own observations. Often an external source, e.g. a satellite with a view of the entire field of operations, can passively provide common randomness to the agents, which enables them to increase the set of achievable joint distributions on their joint action space. It is of interest to characterize this set of achievable joint distributions on the joint action space of the agents. Our main contribution is to give a simple counterexample to a natural conjecture about this class of joint distributions.

* Corresponding author.
Email addresses: ananth@eecs.berkeley.edu (Venkat Anantharam), borkar@tifr.res.in (Vivek Borkar).

[1] Research supported by NSF grant CCF-0500234 and ONR grant N00014-1-0637.
[2] Research supported by CEFIPRA grant 2900-IT-1.

2 Motivation

Let us motivate the importance of the class of joint distributions we are studying, through a simple game theoretic example. For basic concepts from game theory see [6] or [12]. Further motivation for the study of common randomness comes from game theory, information theory, and cryptography, where its role has been extensively explored [1–4,7–10,13,14,18–20].

Consider a zero sum game between two players. Let $\mathcal{U}$ denote the set of pure strategies of player I and $\mathcal{V}$ the set of pure strategies of player II. Assume that both these sets are finite. Let $r : \mathcal{U} \times \mathcal{V} \mapsto \mathbf{R}$ denote the payoff to player I from player II when the pure strategies played are $u \in \mathcal{U}$ and $v \in \mathcal{V}$ respectively. Player I wishes to maximize and player II to minimize the expected payoff. Each player acts in his or her own interest, i.e. the game is *non-cooperative*. The traditional solution concept for a non-cooperative game is *Nash equilibrium*, i.e. a strategy pair where each player's strategy is a best response to that of the other player.

Nash equilibrium for zero sum games need not exist in pure strategies. A simple example is the zero sum game with pure strategy sets $\mathcal{U} = \{U, D\}$ and $\mathcal{V} = \{L, R\}$, and with the payoff function :

	L	R
U	1	0
D	0	1

However every zero sum game admits a Nash equilibrium in privately randomized strategies [16,17] [3]. Let $\mathcal{P}(\mathcal{U})$ and $\mathcal{P}(\mathcal{V})$ denote the respective sets of privately randomized strategies. A Nash equilibrium (σ^*, τ^*) is characterized by the saddle point condition :

$$r(\sigma^*, \tau^*) \stackrel{\Delta}{=} \sup_{\sigma \in \mathcal{P}(\mathcal{U})} \inf_{\tau \in \mathcal{P}(\mathcal{V})} r(\sigma, \tau) = \inf_{\tau \in \mathcal{P}(\mathcal{V})} \sup_{\sigma \in \mathcal{P}(\mathcal{U})} r(\sigma, \tau) \ ,$$

and in [16,17] it is shown that such a saddle point exists.

We now formulate a *distributed* zero-sum game. We think of the minimizing player as being represented by a number of distributed agents. For instance, actuators associated to the sensors in a sensor network may act as such a

[3] Note that the concept of Nash equilibrium only appeared later [11].

player in a game against an adversary [15]. For simplicity, focus on the situation where there are two agents that together form the minimizing player, call them II_A and II_B respectively. Thus we now have a game between three agents : I, II_A, and II_B, with the latter two working together as a single player against the first. Let $\mathcal{U}$, $\mathcal{V}_A$, and $\mathcal{V}_B$ denote the set of pure strategies of agents I. II_A, and II_B respectively; assume these are finite sets. Let $r : \mathcal{U} \times \mathcal{V}_A \times \mathcal{V}_B \mapsto \mathbf{R}$ denote the payoff to player I from player II when the pure strategies used are $u \in \mathcal{U}$, $v_A \in \mathcal{V}_A$, and $v_B \in \mathcal{V}_B$ respectively. Player I wishes to maximize and player II to minimize the expected payoff. A pair of pure strategies $u \in \mathcal{U}$ and $(v_A, v_B) \in \mathcal{V}_A \times \mathcal{V}_B$ would be called a Nash equilibrium if the strategy of each player is a best response to the strategy of the other player. More generally, this terminology can be applied to a pair of randomized strategies.

The importance of the set of joint probability distributions achievable by the collaborating distributed agents representing player II may be seen through an example. Let $\mathcal{U} = \mathcal{V}_A = \mathcal{V}_B = \{0, 1\}$, and let $r(u, v^A, v^B)$ be given by :

$u = 1$	$v_B = 1$	$v_B = 0$
$v_A = 1$	20	0
$v_A = 0$	1	30

and

$u = 0$	$v_B = 1$	$v_B = 0$
$v_A = 1$	20	1
$v_A = 0$	0	30

If the agents II_A and II_B are only allowed private randomization, there is no Nash equilibrium in this game *even in randomized strategies*. To see this, consider the randomized strategy of player I, choosing $u = 1$ with probability β, $0 \leq \beta \leq 1$. The following matrix gives the view the distributed player II has of the payoff :

	$v_B = 1$	$v_B = 0$
$v_A = 1$	20	$1 - \beta$
$v_A = 0$	β	30

When the agents representing player II have no common randomness, their best response is given by :

range	best response of II	best response of I to this
$\beta < \frac{1}{2}$	$(0, 1)$	$v = 1$
$\beta > \frac{1}{2}$	$(1, 0)$	$v = 0$
$\beta = \frac{1}{2}$	$(1, 0)$ or$(0, 1)$	$v = 0$ or $v = 1$ resp.

Examining this shows that there is no Nash equilibrium in this game. More generally, if not enough common randomness is provided to the agents II_A and II_B, there is again no Nash equilibria in randomized strategies. As in the preceding analysis, for the randomized strategy of player I of $u = 1$ with probability β, $0 \leq \beta \leq 1$, if there is less than one bit of common randomness available between the two agents comprising player II, the best response of this distributed player becomes :

range	best response of II	best response of I to this
$\beta = \frac{1}{2}$	uneven mixture of $(0,1)$ and $(1,0)$	$v = 0$ or $v = 1$ resp.

Again one sees that there is no Nash equilibrium.

In the game theoretic example of this section, the agents take actions without any observations. In control scenarios, collaborating agents would have individual observations and seek to create a joint distribution on their joint action space based on these observations and passively provided external common randomness. In the next section we discuss the control scenario.

3 Common randomness and distributed control

Consider a distributed controller comprised, for simplicity, of exactly two agents. The agents observe jointly distributed random variables A and B respectively . The agents are also provided with external common randomness, represented by a random variable W. The external randomness is assumed to be passively provided, hence independent of the observations. The agents wish take actions X and Y respectively. Each agent can choose its action using an arbitrary privately randomized function of its observation and of the externally provided common randomness. All the random variables are assumed to be finite. Let $\gamma(a, b)$ denote the joint distribution of the observations (A, B).

Thus we can achieve joint distributions on (X, Y, A, B, W) of the form :

$$p(w)p(x \mid a, w)p(y \mid b, w)\gamma(a, b) \ . \tag{1}$$

This class is characterized by the conditions :

$$
\begin{aligned}
(A,B) &\sim \gamma(a,b) \\
W &\amalg (A,B) \\
I(X;Y \mid A,B,W) &= 0 \\
I(X;B \mid A,W) &= 0 \\
I(Y;A \mid B,W) &= 0 \ ,
\end{aligned}
\tag{2}
$$

that is to say (A,B) has joint distribution $\gamma(a,b)$, W is independent of (A,B), and certain conditional mutual informations are zero. For basic notions in information theory see e.g. [5]. To see that the form (1) implies the conditions (2) is straightforward. For the converse, first note that the first three parts of conditions (2) imply the form :

$$
p(x \mid a,b,w)p(y \mid a,b,w)\gamma(a,b)p(w) \ .
$$

The fourth part implies that $p(x \mid a,b,w) = p(x \mid a,w)$ and the fifth part implies that $p(y \mid a,b,w) = p(y \mid b,w)$, completing the proof. Note that the conditions (2) are also equivalent to :

$$
\begin{aligned}
(A,B) &\sim \gamma(a,b) \\
W &\amalg (A,B) \\
I(X;B,Y \mid A,W) &= 0 \\
I(Y;A,X \mid B,W) &= 0 \ .
\end{aligned}
\tag{3}
$$

This can be seen from the chain rules :

$$
\begin{aligned}
I(X;B,Y \mid A,W) &= I(X;B \mid A,W) + I(X;Y \mid A,B,W) \\
I(Y;A,X \mid B,W) &= I(Y;A \mid B,W) + I(X;Y \mid A,B,W) \ ,
\end{aligned}
$$

and the nonnegativity of mutual information.

We turn now to the main point of this note. The salient characteristic of the distributed creation of the pair (X,Y) from (A,B) is that X is created with access to A but without reference to B and Y is created with access to B but without reference to A. Thus it is natural to conjecture that for every (X,Y,A,B) with $(A,B) \sim \gamma(a,b)$ satisfying the conditions :

$$
\begin{aligned}
(A,B) &\sim \gamma(a,b) \\
I(X;B \mid A) &= 0 \\
I(Y;A \mid B) &= 0 \ ,
\end{aligned}
\tag{4}
$$

it would be possible to find some W (on a possibly augmented sample space) such that (X, Y, A, B, W) satisfy conditions (2). It turns out that this conjecture is false, as we will now show. Apart from the general discussion of the importance of externally provided common randomness in control and the formulation of distributed zero sum games, we view this counterexample as the main contribution of this paper. It highlights an inherent limitation on what is achievable by passively provided external common randomness.

Let $\mathcal{X} = \mathcal{Y} = \{1, 2, 3\}$ and $\mathcal{A} = \mathcal{B} = \{0, 1\}$. Let $\gamma(a, b)$ be the uniform distribution assigning probability $\frac{1}{4}$ to each (a, b). The joint distribution of (X, Y) conditioned on (a, b) is described as below :

(a,b)	$p(x,y \mid a,b)$	(a,b)	$p(x,y \mid a,b)$
$(1,1)$	$\begin{bmatrix} \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{3} \end{bmatrix}$	$(1,0)$	$\begin{bmatrix} 0 & \frac{1}{3} & 0 \\ \frac{1}{3} & 0 & 0 \\ 0 & 0 & \frac{1}{3} \end{bmatrix}$
(a,b)	$p(x,y \mid a,b)$	(a,b)	$p(x,y \mid a,b)$
$(0,1)$	$\begin{bmatrix} 0 & \frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{3} \\ \frac{1}{3} & 0 & 0 \end{bmatrix}$	$(0,0)$	$\begin{bmatrix} 0 & 0 & \frac{1}{3} \\ 0 & \frac{1}{3} & 0 \\ \frac{1}{3} & 0 & 0 \end{bmatrix}$

Here the rows of $p(x, y \mid a, b)$ are indexed by $x = 1, 2, 3$ and the columns by $y = 1, 2, 3$. Note that $p(x \mid a, b) = \frac{1}{3}$ for all (x, a, b), so $X \amalg (A, B)$. Similarly, $Y \amalg (A, B)$. This implies that (4) holds.

Suppose it were possible to define finite random variables (X, Y, A, B, W) with (X, Y, A, B) having the above joint distribution and such that (1) holds. Then the conditions in (2) and (3) must hold, and we will use these in the ensuing analysis. Pick any $w \in \mathcal{W}$. Writing $p(x, y, a, b, w)$ for $P(X = x, Y = y, A = a, B = b, W = w)$, we have :

$$
\begin{aligned}
p(1,1,1,1,w) &\overset{(a)}{=} P(X=1, A=1, B=1, W=w) \\
&\overset{(b)}{=} P(X=1 \mid A=1, W=w) P(B=1 \mid A=1, W=w) P(A=1, W=w) \\
&\overset{(c)}{=} P(X=1 \mid A=1, W=w) P(B=0 \mid A=1, W=w) P(A=1, W=w) \\
&= P(X=1, A=1, B=0, W=w) \\
&= p(1,2,1,0,w) \ .
\end{aligned}
$$

Here (a) is valid because $\{X = 1, A = 1, B = 1\} \Rightarrow \{Y = 1\}$, (b) is valid by the conditional independence of X and B given (A, W), and (c) is valid because $P(B = 0 \mid A = 1, W = w) = P(B = 1 \mid A = 1, W = w)$.

If we had dropped the $X = 1$ condition at the first step and then replaced $A = 1$ by $A = 0$ we would have shown that

$$p(1, 1, 1, 1, w) = p(3, 1, 0, 1, w) \ .$$

We now list the equalities of this form that we can show. Keeping $A = 1$ and flipping B while leaving X unchanged gives the equations :

$$\begin{aligned} &p(1,1,1,1,w) = p(1,2,1,0,w) \ ; \\ &p(2,2,1,1,w) = p(2,1,1,0,w) \ ; \text{ and} \\ &p(3,3,1,1,w) = p(3,3,1,0,w) \ , \end{aligned}$$

the first of which was proved in detail above. Keeping $A = 0$ and flipping B while leaving X unchanged gives :

$$\begin{aligned} &p(1,2,0,1,w) = p(1,3,0,0,w) \ ; \\ &p(2,3,0,1,w) = p(2,2,0,0,w) \ ; \text{ and} \\ &p(3,1,0,1,w) = p(3,1,0,0,w) \ . \end{aligned}$$

Keeping $B = 1$ and flipping A while leaving Y unchanged gives :

$$\begin{aligned} &p(1,1,1,1,w) = p(3,1,0,1,w) \ ; \\ &p(2,2,1,1,w) = p(1,2,0,1,w) \ ; \text{ and} \\ &p(3,3,1,1,w) = p(2,3,0,1,w) \ , \end{aligned}$$

and finally, keeping $B = 0$ and flipping A while leaving Y unchanged gives :

$$\begin{aligned} &p(2,1,1,0,w) = p(3,1,0,0,w) \ ; \\ &p(1,2,1,0,w) = p(2,2,0,0,w) \ ; \text{ and} \\ &p(3,3,1,0,w) = p(1,3,0,0,w) \ . \end{aligned}$$

We conclude that $p(x, y, a, b, w)$ is the same for all (x, y, a, b) for the chosen w. Since this is true for every w, we conclude that $X \amalg Y$. But this is not true, because, for instance, $P(X = 3 \mid Y = 1) = \frac{1}{2} \neq P(X = 3)$.

4 Concluding remarks

We discussed the importance of externally provided common randomness in distributed control. We formulated a class of so called distributed zero sum games; this formulation is naturally motivated by problems in the emerging field of sensor networks. We discussed the characterization of the class of joint probability distributions that can be achieved on their joint action space by a set of distributed agents with individual observations, when they are passively provided with external common randomness. We gave a counterexample to a natural conjecture about this class of distributions. This counterexample brings out an inherent limitation on what is achievable by passively provided external common randomness.

References

[1] R. Ahlswede and I. Csiszár, "Common Randomness in Information Theory and Cryptography. Part I – Secret Sharing," *IEEE Transactions on Information Theory*, Vol. 39, No. 4, pp. 1121 -1132, 1993.

[2] R. Ahlswede and I. Csiszár, "Common Randomness in Information Theory and Cryptography. Part II – CR Capacity," *IEEE Transactions on Information Theory*, Vol. 44, No. 1, pp. 225 -240, 1998.

[3] R. Aumann, "Subjectivity and correlation in randomized strategies", *Journal of Mathematical Economics*, Vol. 1, pp. 67 -96, 1974.

[4] R. Aumann, "Correlated equilibrium as an extension of Bayesian rationality", *Econometrica*, Vol. 55, pp. 1 -18, 1987.

[5] T. M. Cover, and J. A. Thomas, *Elements of Information Theory*, Wiley, New York, 1991.

[6] D. Fudenberg and J. Tirole, *Game theory*, MIT Press, Cambridge, Massachusetts, 1991.

[7] P. Gacs and J. Korner, "Common information is far less than mutual information", *Problems in Control and Information Theory*, Vol. 21, pp. 149 -162, 1973.

[8] T. S. Han and S. Verdú, "Approximation Theory of Output Statistics". *IEEE Transactions on Information Theory*, Vol. 29, No. 3, pp. 752 -772, 1993.

[9] U. Maurer, "Secret Key Agreement by Public Discussion from Common Information," *IEEE Transactions on Information Theory*, Vol. 39, No. 3, pp. 733 -742, 1993.

[10] U. Maurer and S. Wolf, "Secret-Key Agreement Over Unauthenticated Public Channels – Parts I -III" *IEEE Transactions on Information Theory*, Vol. 49, No. 4, pp. 822 -831; pp. 832 -838; and 839 -851, 2003.

[11] J. Nash, "Equilibrium points in n-person games", *Proceedings of the National Academy of Sciences*, Vol. 21, pp. 128 - 140, 1950.

[12] G. Owen, *Game Theory*, Academic Press, San Diego, 1995.

[13] S. Venkatesan and V. Anantharam, "The Common Randomness Capacity of a Pair of Independent Discrete Memoryless Channels". *IEEE Transactions on Information Theory*, Vol. 44, No. 1, pp. 215 -224, 1998.

[14] S. Venkatesan and V. Anantharam, "The Common Randomness Capacity of a Network of Discrete Memoryless Channels". *IEEE Transactions on Information Theory*, Vol. 46, No. 2, pp. 367 -387, 2000.

[15] R. Vidal, O. Shakernia, H. J. Kim, D. H. Shim, and S. Sastry, "Probabilistic Pursuit-evasion Games : theory, implementation, and experimental evaluation". *IEEE Transactions on Robotics and Automation*, Vol. 18, No. 5, pp. 662 -669, 2002.

[16] J. von Neumann, "Zur Theorie der Gesellschaftsspiele", *Mathematische Annalen*, Vol. 100, pp. 295 -320, 1928.

[17] J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton University Press, Princeton, New Jersey, 1944.

[18] H.S. Witsenhausen, "On sequences of pairs of discrete random variables", *SIAM Journal on Applied Mathematics*, Vol. 28, pp. 100 -11, 1975.

[19] Hans S. Witsenhausen, and Aaron D. Wyner, "A conditional entropy bound for a pair of discrete random variables", *IEEE Transactions on Information Theory*, Vol. IT-21, No. 5, pp. 493 -501, 1975.

[20] Aaron D. Wyner, "The Common Information of Two Dependent Random Variables". *IEEE Transactions on Information Theory*, Vol. IT-21, No. 2, pp. 163 -179, 1975.