A Mathematical Theory of Human Machine Teaming

Pete Trautman

We begin with a disquieting paradox: human machine teaming (HMT) often produces results worse than either the human or machine would produce alone. Critically, this failure is not a result of inferior human modeling or a suboptimal autonomy: even with perfect knowledge of human intention and perfect autonomy performance, prevailing teaming architectures still fail under trivial stressors [3]. This failure is instead a result of deficiencies at the decision fusion level. Accordingly, efforts aimed solely at improving human prediction or improving autonomous performance will not produce acceptable HMTs: we can no longer model humans, machines and adversaries as distinct entities. We thus argue for a strong but essential condition: HMTs should perform no worse than either member of the team alone, and this performance bound should be independent of environment complexity, human-machine interfacing, accuracy of the human model, or reliability of autonomy or human decision making. In other words, this requirement is fundamental (Figure 1): the fusion of two decision makers should be as good as either in isolation. For instance, if the human model is incorrect, the performance of the team should still be as good as the autonomy in isolation. If the autonomy is unreliable, this should not impair the human. Importantly, most existing HMTs do not have a robust mechanism to “fuse” human and machine information, thus obviating any opportunity at producing “a team that performs greater than the sum of its parts”. In response to these shortcomings, we introduce a theory of interacting random trajectories (IRT) over the humans, machines, and (potentially adversarial) environment [3] that optimally fuses the three sources of information and achieves the following four objectives:

1. IRT is a unifying formalism: most HMT approaches are approximations to IRT.
2. IRT quantifies these approximations, and precisely predicts when architectures will fail.
3. We can predict, in advance of empirical evaluation, when IRT will succeed and fail.
4. The first three objectives, when combined with dimensionality reduction techniques, enable a human-collective/multi-agent decision fusion framework with performance bounds.

1. A Unifying Formalism for HMT To show that IRT is a unifying formalism, we must understand standard HMT decision fusion; we thus introduce linear blending:

$$u_{LB}(t) = K_h(t)u_h + K_R(t)u_R.$$  

At time $t$, $u_{LB}(t)$ is the team action, $u_h$ is the human operator input (joystick deflections, high level commands, or preset autonomous actions), $u_R$ is the autonomy command, and $K_h(t), K_R(t)$ are the operator and autonomy weighting factors, respectively, which can be functions of anything, subject to $K_h + K_R = 1$. As shown in [3], linear blending captures a wide variety of teaming approaches in low level shared control—we argue here that linear decision
fusion is used much more broadly in HMT. For instance, switching control (either human or machine has full control) is a special case of linear blending where \( K_h, K_R \) are either 0 or 1. Consider the following:

- Dynamic task allocation: an algorithm determines when the human or the machine should be in control of the task (switching control). This does not mean that the allocation method is linear, but that the decision fusion is linear. For instance, we might use an elaborate cognitive architecture to determine when the human takes full control. We point out that “shared mental models” are typically implemented in a switching control fashion, supervisory control approaches delegate to either the machines or the humans, and handoff tasks have been almost exclusively restricted to the case of switching control.

- Commercial autopilots are exclusively switching control.

- “Playbook” approaches: the human picks a “play”, and the machines execute, which is an example of switching control where \( K_h(0) = 1, K_R(1) = 1 \).

- Standard HCI: human inputs data, machine processes data/presents alternatives to human, human makes a decision. This is switching control: \( K_h(0) = 1, K_R(1) = 1, K_h(2) = 1 \).

Interacting random trajectories \([3]\) is a generalization of linear blending: it is a statistically sound and optimal approach to fusing coevolving human, machine and environment information. IRT relaxes human input to online data \( u_{ht}^i \equiv z_{ht}^i \) about the random human trajectory \( h: t \in \mathbb{R} \to X^h \) over the action space \( X^h \) (we generalize to multiple humans in Section 4), we take measurements \( z_{j,t}^{R_i} \) of the \( j \)’th machine trajectories \( f^R_j: t \in \mathbb{R} \to X^R \), and measurements \( z_{j,t}^{E_i} \) of the \( i \)’th environment agent trajectory \( f^E_i: t \in \mathbb{R} \to X^E \). We collapse the machines \( f^R = [f^R_1, \ldots, f^R_{mn}] \) and the environment \( f = [f^1, \ldots, f^{R_{mn}}] \) into collective random processes, and take the following as our decision fusion architecture (Equation 0.2).

\[
\begin{align*}
\hat{u}_{IRT}^T(t) & = \hat{f}_{t+1}^R \\
(h, f^R, f)^* & = \arg \max_{h, f^R, f} p(h, f^R, f | z_{1:t}^h, z_{1:t}^R, z_{1:t}^f).
\end{align*}
\]

This formulation enables a precise understanding of the assumptions that any linear fusion architecture impose on the team, thus providing a theoretical advantage, since we can now do analysis in advance of empirical evaluation across a broad range of approaches.

2. Quantifying the Approximations in Existing HMT Approaches An important motivation for the lower bounding principle is the commonplace failure of existing HMT architectures—for many applications, trivial stressors lead to the team falling apart. Consider the case of a human and a robot sharing control of a platform in a congested environment (e.g., a shared control wheelchair navigating through a
crowd). In [3], we proved that state of the art HMT architectures fail the lower bounding criteria if environmental or operator predictions are multimodal in a Gaussian mixture representation; even under mildly challenging conditions, existing approaches can fuse two safe inputs into an unsafe shared control (Figure 3a). Furthermore, in [3], we proved that IRT respects the lower bounding property under a variety of circumstances (explored fully in [4]). Most existing approaches to fully autonomous navigation in human environments also fail the lower bounding property. For instance, as shown in [2], decoupling the components of the robot-crowd team leads to the freezing robot problem: once environment complexity exceeds a certain threshold, planning algorithms that independently model the human and the robot freeze in place. More broadly, as shown in Figure 3b, state of the art crowd navigation algorithms fail the lower bounding property: purely human crowds are safer and more efficient than human-robot crowds. The results in [3, 4] suggest that a coupled and evolving human-machine-world architecture is required to achieve the lower bounding property (Figure 3c). Further, linear fusion prevents the interleaving of human/machine capabilities, while IRT weaves complementary capabilities (Figure 4).

3. Predicting Capabilities of IRT Although a coupled HMT architecture is necessary to achieve lower bounding, can we prove that joint models preserve the property across a spectrum of team stressors? In Figure 4 we present a thought experiment showing how we can reason towards Figure 1, a shared control robot travels through a crowd waiting for an elevator. Without elevator arrival information, the robot’s best choice is to go right. When the elevator bell rings, the robot does not know what it means; a human, however, will recognize that the best path will be around the left side of the crowd and the worst path will be to the right. In Figure 4a, a high fidelity human model shows how IRT marries human information to robot path planning to exceed the lower bound; the linear architecture discards the human’s input and violates the lower bound (Figures 4a and 4c). In Figure 4b, IRT exceeds the lower bound and the linear architecture violates it (Figures 4b and 4c).

Constructing general instantiations of Figure 1 will require at least two advances. First, we must quantify performance error outside of the training set. IRT formulates teaming as a joint human-machine-world model, presenting an opportunity to interpret performance error as generalization error; such an approach allows us to use data to instantiate Figure 1.

Figure 5: Using learning theory and [3] to generate Figure 1. The “true” teaming action $u_{true}^T(h, f^R, f)$ and IRT teaming action $u_{IRT}^T(h, f^R, f)$ are separated by $\epsilon$ with probability $\delta$. The human, machine, and world $(h, f^R, f)$ are arguments of the teaming actions; we vary them to produce Figure 1.
to leverage important results from learning theory, and thus accelerate our understanding of HMT performance bounds. Second, to generate Figure 1, team stressors must be an argument of the predicted performance error. Since the human, autonomy, and world are arguments of IRT, these models are also arguments of the performance error (Figure 5).

4. Optimal Human Collective Representations
Many existing internet recommendation technologies (e.g., Netflix) are based on a simple observation: human preference is often low dimensional. Thus, when represented in the optimal basis, we can accurately predict human decision making from only a few example decisions.

With matrix completion \( \Pi \), we can exactly recover user preference for any movie with just a few reviews; however, this technology assumes that \( n_1 \) other humans have already entered \( k \) reviews, blurring the distinction between individual and collective. This begs a critical question for HMT: can we infer collective human decision making from just a few individual operator samples? We present three examples, and discuss the underlying mathematical challenge.

1. Supervisory control of \( N \) platforms: a single operator provides \( n \ll N \) waypoint inputs.

2. Human control of a robotic prosthesis: in a robotic prosthesis, there are \( N \) actuators, but the human can only provide \( n \ll N \) actuator inputs.

3. Big data analysis (find the bad guy in 1B images): an analyst can provide up to \( N \) image “insights” (derived from contextual clues). With time pressure, he provides \( n \ll N \) insights.

IRT, as described in Equation 0.2 provides a mathematical quantification of this problem:

\[
p(h, f^R, f | z_{1:t}) = p(f^R, f | z_{1:t}^R, f_{1:t}, h)p(h | z_{1:t}^R, f_{1:t}, h) \approx p(f^R, f | z_{1:t}^R, f_{1:t}, h) \sum_{i=1}^{n} w_i \delta(h - h_i)
\]

where we approximate \( p(h | z_{1:t}^h) \approx \sum_{i=1}^{n} w_i \delta(h - h_i) \); we interpret \( h_i \) as waypoints, actuator inputs, or analyst insights. However, if the rank of the collective human intent is \( r \) and \( k \) is the number of existing entries, \( \Pi \) tells us that \( n \geq C n_1^{1.2} r \log N - k \) inputs can complete \( n \to N \); in an important sense, we are completing a single operator using the “collective wisdom” of the \( n_1 \) participants.

Summary of Response: IRT (lower bounding paradox) and optimal human collective representations demand a radical rethinking of coevolving ecosystems of humans, machines and adversaries: the distinction between individual and collective has been muddled in an unintuitive (yet mathematically precise) way.

References
[1] E.J. Candes and B. Recht. Exact matrix completion via convex optimization. *Founds. of Comp. Math.*, 2008.
[2] P. Trautman et al. Robot navigation in dense crowds: the case for cooperation. In *ICRA*, 2013.
[3] P. Trautman. Assistive planning in complex, dynamic environments. In *IEEE Systems, Man, and Cybernetics* (http://arxiv.org/abs/1506.06784), 2015.
[4] P. Trautman. Interacting random trajectories: a discussion (http://tinyurl.com/gvc8hzd). Technical report, Galois Inc., 2016.
[5] P. Trautman and A. Krause. Unfreezing the robot: Navigation in dense interacting crowds. In *IROS*, 2010.