文章编号：2096-1618(2016)06-0558-07
稿件来源：科学网
网　　址：http://blog.sciencenet.cn/blog-453322-993540.html
发表时间：2016-07-30

安全通论(12)

——对话的数学理论

杨义先，　钮心忻
(北京邮电大学信息安全中心，北京 100876)

摘要：控制论的创始人维纳，于半个多世纪前(1950年)，在其著作《人有人的用处》中，花费了至少两章的篇幅，提出了一个有关“非协作式对话”的问题，他称之为“法庭辩论”。虽然维纳明明知道这个问题与博弈论有关，但是，由于那时的博弈论还很幼稚，根本不足以解决这个问题。所以，仙农在解决协作式对话时，不得不另辟奇径，用非常巧妙的数学手段给出了圆满的答案，从而创立了众所周知的《信息论》。如今，博弈论已基本成熟，相关的结果基本可以用来解决(至少是部分解决)维纳的“非协作式对话”问题了，所以，本文才有机会与维纳神交。具体地说，本文建立了一般对话的数学模型(因此，也是《信息论》的某种扩展)，并借助博弈论中的纳什均衡定理，给出了相关的对话极限(极大值)。当然，从数学完美程度上说，本文远远不如仙农的《信息论》。

1　协作式对话与问题的提出

人类历史，几乎就是一部对话史！

最早的人类，就像现在的动物那样，通过叫声和肢体动作来彼此对话，交流信息，沟通情感；后来有了语言，才开始了真正意义上的对话；再后来，有了文字、图像等，使得对话的手段更加丰富，对话的效果更好；如今，网络和多媒体的广泛使用，使得对话(特别是群体对话)在生活中的份量越来越重。

但是，古往今来，好像很少有人全面、深入、认真地思考过对话的本质！其实，对话可以分为三大类(协作式对话、骂架式对话、法庭辩论式对话，其中后两种对话是非协作式的)：

首先来看“协作式对话”。这是最常见的对话，此时对话双方(或多方)的目标就是共同努力，减少或消除彼此之间的不确定度(熵)。

研究协作式对话最成功的理论，当数仙农创立的《信息论》，其核心概念包括：

(1)概率为 p 的随机(话语)事件，它所包含的信息量为 $\log(1/p)$；

(2)由 n 个概率分别为 p_1、p_2、…、p_n，$p_1+p_2+\cdots+p_n=1$，的随机(话语)事件所组成的随机(话语)变量 X，所包含的信息量为 $H(X)=\sum_{i=1}^{n}p_i\log(1/p_i)$，这里 $H(X)$ 又称为随机(话语)变量 X 的熵，它也是在协作式对话中，对话双方(多方)所能够传达的信息的最大量值。注意：之所以叫做“协作式”对话，是因为，已经潜在地假设每个事件(概率为 p_i)对 X 的整体熵都是正贡献，即，整体熵 $H(X)$ 等于各个事件的信息量 $\log(1/p_i)$ 的以 p_i 为加权值的求和(而不是减法)。

(3)设 X 和 Y 分别是对话双方的随机(话语)变量，那么，条件概率事件 $p(Y=y\mid X=x)$，简记为 $p(y\mid x)$，所包含的信息量为 $\log(1/p(y\mid x))$。条件随机变量 $p(Y\mid X=x)$，简记为 $p(Y\mid x)$，所包含的信息量为 $H(Y\mid X=x)=\sum_{y\in Y}p(y\mid x)\log(1/p(y\mid x))$，它也是在条件 $X=x$ 下，条件随机变量的概率密度条件分布的熵(由于已经暗含协作式假定，所以，与上面的(2)类似，此时只考虑了加权和，而没有减法)。而当 X 取遍随机变量 X 的所有可能值后，条件分布熵的加权和 $\sum_{x\in X}p(X=x)H(Y\mid X=x)=H(Y\mid X)$ 就称为条件熵(再一次地，这里又暗含了协作式假设，所以，整体熵也是部分熵之和，而没有减法)。

(4)设 X 和 Y 分别是对话双方的随机(话语)变量，由于 Y 的贡献，使得 X 的熵 $H(X)$ 最多被减少 $H(X\mid Y)$，于是，称被减少后的剩余熵量 $H(X)-H(X\mid Y)$ 为 X 和 Y 的互信息，记为 $I(X;Y)$。此处再一次暗含了协作式假定，即，Y 的贡献是积极贡献，即，Y 必定减少整体熵，而不是增加熵。

(5)随机变量 X 和 Y，在给定随机变量 Z 的条件下，的条件互信息定义为：$I(X;Y\mid Z)=H(X\mid Z)-H(X\mid Y,Z)$(暗含的协作式假定痕迹也很明显)。

于是，仙农的整个《信息论》研究的就是在协作式对话中：(1)如何把话语 X 中的冗余信息进行充分压缩，使得其信息量达到最小值 $H(X)$，这便是仙农第一定理(信源编码定理)；(2)由于 Y 的积极贡献，使得有 $I(X;Y)$ 的信息量能够被传达给对话的另一方，那么，I

$(X;Y)$的最大值(即,仙农称为信道容量 C 的东西)是多少,又如何把这最大值的信息量无失真地传达给另一方,这便是仙农第二定理(信道编码定理)。

为了引出本文的另一主角,《控制论》的创始人维纳教授,我们插一个小曲:一般认为,信息论的创始人是仙农,他给出了信息的定量量度。但是,仙农自己却说"光荣应该属于维纳教授,他对于平衡序列的滤波和预测问题的漂亮解决,在这个领域里,对我的思想有重大影响"(见文献[13]导读部分的第 15 页)。当然,维纳也非常谦虚,他说"这个问题(本文作者注:即,压缩与传递问题)在贝尔电话研究所设计 Vocoder 系统时,就已经解决了,至少部分地解决了,有关的一般理论也已由这个研究所的仙农博士,以非常令人满意的形式提了出来(本文作者注:维纳标注的论文就是仙农那篇,创立《信息论》的经典论文,Shannon C. E., The mathematical theory ofcommunications, Univ. of Illinois Press, 1949)"(见文献[12]第 50 ~ 51 页)。

本文无意研判《信息论》的创始人到底是谁,而是要提请读者注意:半个多世纪以来,经过仙农、维纳等全世界科学家们的不懈努力,人类已经在信息论及其应用方面取得了巨大成就,甚至建成了如今的信息社会。但是,必须指出:所有这些成果,都有一个暗含的假设:即,对话双方(多方)是彼此协作的,其目的是一致的,都是要想共同努力减少熵,或者说减少不确定度,而采用的手段便是增加信息(因为,信息是负熵嘛)。

难道对话真的只有"协作式对话"这一种吗?

在 1950 年之前,也许全人类都没有注意到这个问题;因为,甚至在维纳的名著《控制论》中,都处处隐含了"协作式对话"的痕迹。直到 1950 年,维纳出版了他的另一本重要著作《人有人的用处》(见文献[13]),才明确提出了这个问题。在[13]中,维纳甚至花费了两章(第四章"语言的机制和历史"和第六章"法律和通信")的篇幅来探讨"非协作式对话",下面,让我们摘录维纳的两段话吧,

第 1 段话,维纳说(文献[13]第四章"语言的机制和历史"第 78 页):"……正常的通信谈话,其主要敌手就是自然界自身的熵趋势,它所遭遇到的并非一个主动的、能够意识自己目的的敌人。而另一方面,辩论式的谈话,例如,我们在法庭上看到的法律辩论以及如此等类的东西,它所遭遇到的就是一个可怕得多的敌人,这个敌人的自觉目的就在于限制乃至破坏谈话的意义。因此,一个适用的、把语言看作博弈的理论应能区分语言的这两个变种,其一的主要目的是传送信息(本文作者注:这便是,仙农已经研究得相当完美的,协作式对话),另一种的主要目的是把自己的观点强加到顽固不化的反对者头人(本文作者注:这便是,非协作式对话)。我不知道是否有任何一位语言学家曾经做过专门的观察并提出理论上的陈述,来把这两类语言依我们的目的做出必要的区分,但是,我完全相信,它们在形式上是根本不同的……"。

从这段话中,我们可以确定两个重要的事实:(1)既然作为语言学家的儿子,维纳,都不知道是否曾经有过语言学家对"非协作式对话"做过研究,那么,维纳的父亲,著名的语言学家,也许也不知道。因此,非协作式对话很可能是维纳首先发现并明确提出的。(2)"协作式对话"与"非协作式对话"是"根本不同的",所以,以协作式对话为前提的仙农《信息论》确实还有值得扩展之处。

第 2 段话,维纳说(文献[13]第六章"法律与通信"第 97 页):"……噪声可以看作人类通信中的一个混乱因素,它是一种破坏力量,但不是有意作恶。这对科学的通信来说,是对的;对于二人之间的一般谈话来说,在很大程度上也是对的。但是,当它用在法庭上时,就完全不对了……"。

从这段话中,我们可以确定另外两个重要事实:(1)协作式对话的主要破坏力量是噪声,《信息论》已经对它有完美的研究了;(2)协作式对话的成果,完全不适合于法庭上的非协作式对话。

好了,我们不再摘录维纳语录了,有特殊兴趣的读者,可以自行阅读维纳的全书。下面,我们开始对维纳指出的非协作式对话进行更深入的研究。

2　骂架式对话

"骂架式对话"是与"协作式对话"完全对立的另一个极端。此时骂架双方(或多方)的主要(甚至唯一)目的就是增加混乱度(熵),通过千方百计提高不确定度,把对方搞糊涂。

你也许见识过泼妇骂街,她们完全失去了理智。对方的每句话,无论是否有道理,都是她痛骂的对象,不把对方的言路和思路封死,她决不罢休。

虽然,随着社会文明的进步,泼妇已经越来越少了;但是,骂架式对话却越来越多了,其中,最典型的代表就是微博上的匿名五毛党。他们(五毛)受雇后,与博主的所有对话,都是胡搅蛮缠,其唯一目的就是把水搅浑,让博主被误解。五毛们既没有道德,也谈不上原则,他们的对话决不是想与博主沟通,更不可能与博主协作。

不过,从理论研究角度来看,没必要专门研究骂架式对话,因为,它完全与协作式对话相反,所以,只要把信息论中的相关概念和结果乘以"-1",就差不多能照搬仙农的东西了。

此处,之所以要把"骂架式对话"单独列出来,主

要是想与它的另一个极端(协作式对话)对应起来。

其实,最复杂的情况,是下节中将要探讨的,介于两个极端(协作式对话和骂架式对话)之间的情况,即,辩论式对话。

3 辩论式对话

关于辩论式对话的描述,维纳已经说得很多了,不过,我们在正式为其建立数学模型之前,还是想再添点油,加点醋。

话说,某幼儿园的调皮蛋,小明,去看医生,说自己受伤了。

大夫见其腿上有泥,便让他摸摸。小明说痛。此时,这段对话,当然就减少了大夫的不确定度(即,熵被减少了,小明给出了正信息),他初步判断:小明的腿受伤了。

大夫又见小明脸上有汗,叫他擦擦。小明又说痛。此时,这段对话,却增加了大夫的不确定度,大夫开始有点迷糊了(即,熵被增加了,信息被减少了或出现了负信息):脸上没伤,咋也痛呢?

大夫再让小明摸摸肚子。小明还是说痛。此时,这段话把大夫搞崩溃了(即,熵又被增加了,信息又被减少了):这么小的儿童,不可能全身浮肿或疼痛呀?

最后,大夫让小明摸遍全身,结果,小明都说痛。这时,大夫灵感一现,哦~,原来是小明的手指受伤了(熵被减少至0,或者说获得了全部信息),至此,不确定度就全部消失了!

小明的故事虽然是笑话,但是,它确实告诉我们:有些对话能够减少熵,有些却又能增加熵;有些能够提供正信息,有些却提供的却是负信息。

"某些事件,使熵减少;某些事件,使熵增加"的例子还有很多,

比如:当你只有一个闹表时,你对时间是很确定的;但是,当你有两只闹表时,如果它们的时间显示不一样,那么,你对时间的不确定度会大增(熵也增加,信息减少),甚至不知所措;再进一步,如果你有三个或更多的闹表时,你对时间的不确定度又会减少(熵被减少或信息被增加),因为,你可以借助统计手段(少数服从多数)来做出基本正确的判断。

又比如:有些病症能够帮助大夫做出正确判断,但是,也有些病症会把大夫搞糊涂,从而才会出现那么多"疑难杂症"。

再回到法庭上。关于法官和律师之间的辩论,他们在大的原则上,肯定会有一定的底线(至少法律条文也确保了他们无法跨越底线),这时他们的对话就会以减少不确定度(熵)为目标,即,出现协作,传递正信息;但是,在一些细节方面,他们(特别是律师)肯定试图增加不确定度(熵),把法官搞糊涂(即,出现局部的骂架式对话,传递负信息),从而达到"重罪轻判"等目的。

好了,例子够多了,下面就来建立一般"法庭辩论式对话"的数学模型。

(1)概率为 p 的随机(话语)事件,它所包含的信息量为 $\log(1/p)$。但是,在协作式场景中,这个量取正值 $\log(1/p)$,即,该事件提供正信息;在骂架式场景中,这个量取负值 $-\log(1/p)$,即,该事件提供负信息。

(2)由 n 个概率分别为 $p_1、p_2、\cdots、p_n$,$p_1+p_2+\cdots+p_n=1$,的随机(话语)事件所组成的随机(话语)变量 X,所包含的信息总量为 $H(a,X)=\sum_{i=1}^{n}a_ip_i\log(1/p_i)$,这里 $a=(a_1,a_2,\cdots,a_n)$ 称为 X 的取向矢量,并且 $a_i=1$ 或 -1,对所有 $1\leqslant i\leqslant n$。当 $a_i=1$ 时,事件 p_i 提供了数量为 $p_i\log(1/p_i)$ 的正信息;当 $a_i=-1$ 时,事件 p_i 提供了数量为 $-p_i\log(1/p_i)$ 的负信息。当取向矢量 $a=(1,1,\cdots,1)$ 时,$H(a,X)$ 就退回到了仙农的协作式对话中的 $H(X)$;当取向矢量 $a=(-1,-1,\cdots,-1)$ 时,便出现了骂架式对话。需要指出的是,在协作式对话中,$H(a,X)$ 一定非负,即,随机(对话)变量 X 总是提供正信息,从而减少不确定性;在骂架式对话中,$H(a,X)$ 一定非正,即,随机(对话)变量 X 总是提供负信息,从而增加不确定性;在一般的辩论式对话中,$H(a,X)$ 可能为正(此时,X 贡献正信息),也可能为负(此时 X 贡献负信息)。为方便计,我们将 $H(a,X)$ 称为 X 的方向为 a 的方向熵,在不引起误解的情况下,简称为方向熵。

(3)设 X 和 Y 分别是对话双方的随机(话语)变量,它们的概率分布分别为 $\{p_1、p_2、\cdots、p_n\}$ 和 $\{q_1、q_2、\cdots、q_m\}$,它们的取向矢量分别为 $a=(a_1,a_2,\cdots,a_n)$ 和 $b=(b_1,b_2,\cdots,b_m)$。那么,条件概率事件 $p(Y=y_j\mid X=x_i)$,简记为 $p(y_j\mid x_i)$,所包含的信息量为 $\log(1/p(y_j\mid x_i))$。条件随机变量 $p(Y\mid X=x_i)$,简记为 $p(Y\mid x_i)$,所包含的信息量为 $H(b,Y\mid X=x_i)=\sum_{j=1}^{m}b_jp(y_j\mid x_i)\log(1/p(y_j\mid x_i))$,它实际上是条件随机变量 $p(Y\mid X=x_i)$ 的方向熵(方向矢量为 b)。而当 X 取遍所有可能的 x_i 后,我们就将这些带方向的条件分布熵进行带向加权和,得到 $\sum_{i=1}^{n}a_ip_iH(b,Y\mid X=x_i)=H(b,Y\mid a,X)$,并将就它称为带向条件熵。显然,当 $a=b=(1,1,\cdots,1)$ 时的带向条件熵,就是仙农信息论中的条件熵。注意:在一般情况下,$H(a,X\mid b,Y)$ 可能为正值,也可能为负值,这与仙农信息论中的恒正情况是不同的。

(4)设 X 和 Y 分别是对话双方的随机(话语)变量,它们的取向矢量分别为 $a=(a_1,a_2,\cdots,a_n)$ 和 $b=(b_1,b_2,\cdots,b_m)$。由于 Y 的出现,使得 X 的方向熵 $H(a,X)$ 最多被变化 $H(a,X\mid b,Y)$,于是,被变化后的

方向熵量 $H(a,X)-H(a,X\mid b,Y)$ 称为 X 和 Y 的带向互信息,记为 $I(a,X;b,Y)$,它也是由于 Y 的出现,使得 X 能够传递给 Y 的信息量。当 $I(a,X;b,Y)$ 为正时,X 能够给 Y 传递正信息;否则,X 就只能把 Y 给搞糊涂(即,传递负信息)。

(5)设随机变量 X、Y、Z 的取向矢量分别为 a、b、c。随机变量 X 和 Y,在给定随机变量 Z 的条件下,的带向条件互信息定义为:$I(a,X;b,Y\mid c,Z)=H(a,X\mid c,Z)-H(a,X\mid b,Y;c,Z)$。

好了,一般对话的数学模型就基本建成了。虽然,从中不难看出,仙农研究的协作式对话确实是一般对话的特例(即,方向矢量为(1,1,…,1)的特例),但是,除了骂架式对话(即,方向矢量为(-1,-1,…,-1)的情况)之外,仙农信息论的几乎所有结论、研究方法和数学工具等,在一般辩论式对话面前,都全都失灵了!这也许就是维纳的“法庭辩论问题”被搁置半个多世纪的原因之一吧,因为,虽然维纳已经猜到这个问题可能与博弈论有关,但是,由于那时冯. 诺伊曼的博弈论刚刚诞生,还相当幼稚(比如,还没有除零和博弈之外的纳什均衡),所以,科学家们完全找不到相应的数学工具去研究这个问题。虽然 2 年后(即,1952 年),就由 Glicksberg 等证明了如下可以用来研究这个问题的纳什均衡定理,但是,也许 Glicksberg 没有引起维纳的注意,而其他科学家可能又没有发现辩论式对话与《信息论》和《博弈论》之间的关系,所以,这才给了本文作者一个捡漏的机会,当然,其基础就是我们在文献[11]将《信息论》、《博弈论》和《安全通论》进行了完美的融合,否则,一般人也捡不到这个漏。而且,我们发现,针对一般的辩论式对话,即使是那几个曾在文献[11]中,在融合《信息论》与《博弈论》时立过大功的那几个定理,在这里也完全不再适用;代之,我们启用的是如下定理:

Glicksberg 定理(见文献[15]的定理 1.3):在一个 n 人标准式博弈 $G=\{S_1,\cdots,S_n;u_1,\cdots,u_n\}$ 中,如果参与者的战略空间 $S_1,\cdots,S_n$ 是度量空间的非空紧集;并且,各收益函数 $u_1,\cdots,u_n$ 是连续的。那么,该博弈存在纳什均衡(纯战略纳什均衡或混合战略纳什均衡)。

此外,为了给对话各方设计相应的博弈模型,我们做另一个合理的约定,

效率约定:假定在辩论式对话中,各方都是讲究效率的。即,对话各方若想彼此沟通,那么,他们就会努力传递尽可能多的“正信息”;如果他们想骂架,那么,他们也会努力传递尽可能多的“负信息”。形象地说,对话各方,若是朋友,就推心置腹;若是敌人,就要骂得对方肝胆俱裂!

好了,下面为各类辩论式对话设计相应的博弈模型,并探讨其优化结果。

情况 1:首先来看看常见的“1 对 1 对话”,例如,单边谈判。

构造一个标准式博弈 $G=\{S_1,S_2;u_1,u_2\}$,它有两个参与者,分别是甲方 X 和乙方 Y;他们的取向矢量分别是 a 和 b。如果 X 和 Y 分别是取 n 个和 m 个值的随机变量,那么,

参与者 1(甲方)的战略空间 S_1 定义为 $S_1=\{0\leqslant x_i\leqslant 1;1\leqslant i\leqslant n,\ x_1+x_2+\cdots+x_n=1\}$,它是边长为 1 的 n 维封闭立方体中的一个 $n-1$ 维封闭子立方体(当然,也就是度量空间的非空紧集)。

参与者 2(乙方)的战略空间 S_2 定义为 $S_2=\{0\leqslant y_i\leqslant 1;1\leqslant i\leqslant m,y_1+y_2+\cdots+y_m=1\}$,它是边长为 1 的 m 维封闭立方体中的一个 $m-1$ 维封闭子立方体(当然,也就是度量空间的非空紧集)。

对参与者 1 和 2 的任意两个具体的纯战略 $s_1\in S_1$(即,$s_1=(p_1,p_2,\cdots,p_n),p_1+p_2+\cdots+p_n=1$)和 $s_2\in S_2$(即,$s_2=(q_1,q_2,\cdots,q_m),q_1+q_2+\cdots+q_m=1$)分别定义他们的收益函数为:

参与者 1(甲方)的收益函数 $u_1(s_1,s_2)$ 定义为 $u_1(s_1,s_2)=\mid I(a,X;b,Y)\mid$,即,$X$ 和 Y 的带向互信息 $I(a,X;b,Y)$ 的绝对值,这里 X 和 Y 的概率分布函数分别由 s_1 和 s_2 定义为 $P(X=i)=p_i,(1\leqslant i\leqslant n,0\leqslant p_i\leqslant 1)$ 和 $P(Y=j)=q_j,(1\leqslant j\leqslant m,0\leqslant q_j\leqslant 1)$。该收益函数,显然是连续的。这里,之所以要取绝对值,是根据上面的效率约定。

参与者 2(乙方)的收益函数 $u_2(s_1,s_2)$ 定义为 $u_2(s_1,s_2)=\mid I(b,Y;a,X)\mid$。该收益函数,也是连续的。这里,之所以要取绝对值,也是根据上面的效率约定。

于是,Glicksberg 定理的所有条件都被满足,即,我们人为构造的标准式博弈 $G=\{S_1,S_2;u_1,u_2\}$ 就存在(纯战略或混合战略的)纳什均衡,此时,辩论对话的双方都达到了自己的理想极大值,比如,想骂人的也骂痛快了,想沟通的也心满意足了。注意:我们这里并未考虑多个纳什均衡的情况,也没有考虑诸如纳什均衡的精练等问题,只说是达到了极大值,而非最大值,可见,后续研究的内容还有很多,还有很多金矿有待读者去挖掘哟!

情况 2:再来看“1 对多的辩论式对话”,例如,诸葛亮舌战群儒。

记诸葛亮为 X,其取向矢量为 a;记 n 个群儒为 $Y_1,Y_2,\cdots,Y_n$;他们的取向矢量分别为 $b_1,b_2,\cdots,b_n$,注意,这里的每个 b_i 其实都是一个矢量哟。

现在考虑他们这(n+1)个参与者之间的如下标准式博弈 $G=\{S,S_1,S_2,\cdots,S_n;u,u_1,u_2,\cdots,u_n\}$:

参与者 0(诸葛亮 X)的战略空间 S 定义为 $S=\{0$

$\leqslant x_i \leqslant 1; 1 \leqslant i \leqslant m,\ x_1+x_2+\cdots+x_m=1\}$。

参与者 1(群儒 Y_1)的战略空间 S_1 定义为 $S_1=\{0 \leqslant y_{i1} \leqslant 1; 1 \leqslant i \leqslant N(1),\ y_{11}+y_{21}+\cdots+y_{N(1)1}=1\}$。

参与者 2(群儒 Y_2)的战略空间 S_2 定义为 $S_2=\{0 \leqslant y_{i2} \leqslant 1; 1 \leqslant i \leqslant N(2),\ y_{12}+y_{22}+\cdots+y_{N(1)2}=1\}$。

……

参与者 n(群儒 Y_n)的战略空间 S_n 定义为 $S_n=\{0 \leqslant y_{in} \leqslant 1; 1 \leqslant i \leqslant N(n),\ y_{1n}+y_{2n}+\cdots+y_{N(1)n}=1\}$。

综上可知,该博弈的各参与方的战略略空间都是度量空间的非空紧集。

对任何一组纯战略 X、Y_1、Y_2、…、Y_n,根据不同的利益目标(优化目标),上述$(n+1)$个博弈者之间的利益函数也是各不相同的,因此,相应的理想极大值也是各不相同的。为节省篇幅,我们不对所有细节情况一一论述,而是抽象地将所有情况“一网打尽”。

首先,从诸葛亮 X 的角度来看,他将 n 个群儒分成 K 个组 F_1、F_2、…、F_K使得每个群儒都在并只在某一个组中;而且,X 对于在同一个组中的不同群儒不加区别;对这 K 个组,诸葛亮 X 还分配了一个权重系数 d_1、d_2、…、d_K,这里 $d_1+d_2+\cdots+d_K=1$,对每个 $1 \leqslant i \leqslant K, 0 \leqslant d_i \leqslant 1$。于是,诸葛亮 X 的收益函数定义为

$$u(X,Y_1,Y_2,\cdots,Y_n)=\mid \sum_{i=1}^{K} d_i I(a,X;B_i,F_i \mid B_i^C,F_i^C) \mid$$

这里,$B_i=\{b_j, j \in F_i\}$,即,分组 F_i中各群儒的方向矢量之集合;F_i^C和 B_i^C分别表示除了 F_i和 B_i之外,所有其它群儒和他们的方向矢量组成的集合,而 $I(a,X;B_i,F_i \mid B_i^C,F_i^C)$表示在条件 F_i^C之下,X 和 F_i的带向条件互信息。与前面类似,收益函数之所以要取绝对值,也是基于效率约定而来的。

其次,再来看 n 个群儒,假定他们自愿分成 M 个联盟 R_1、R_2、…、R_M使得每个儒生都在且只在某一个联盟中;同一个联盟中的儒生都以本联盟利益为重(不考虑自己个人的利益。自私的儒生可以自己单独组成一个联盟),于是,对每个儒生 $i(1 \leqslant i \leqslant n)$,如果该儒生 $i \in R_j (1 \leqslant j \leqslant M)$,那么,他就按如下方式来定义其利益函数(即,同一个联盟中的所有儒生的利益函数都是相同的):

$$u_i(X,Y_1,Y_2,\cdots,Y_n)=\mid I(B_j,R_j;a,X \mid B_j^C,R_j^C) \mid$$

这里,$B_j=\{b_k, k \in R_j\}$,即,联盟 R_j中各儒生的方向矢量之集合;R_j^C表示除了 R_j之外,所有其他儒生联盟组成的集合,而 $I(B_j,R_j;a,X \mid B_j^C,R_j^C)$表示在条件 R_j^C之下,R_j与 X 的带向条件互信息。这里,收益函数取绝对值的原因,仍然是效率约定。

综上可知,该博弈的各参与方的收益函数都是连续的。

于是,在按上述过程定义的标准式博弈 $G=\{S, S_1,S_2,\cdots,S_n; u,u_1,u_2,\cdots,u_n\}$ 中,可以直接验证:Glicksberg 定理的条件被全部满足,即,该博弈存在(纯战略或混合战略的)纳什均衡。而达到纳什均衡状态时,诸葛亮与儒生们便得到了自己企望的极大理想结果,即,想沟通的,也达到极大值了;想骂的,也骂痛快了。

情况 3:两派之间的辩论式对话,例如,鹰派与鸽派之间的辩论。

此时,鹰派有 n 个人 X_1、X_2、…、X_n,鸽派有 m 个人 Y_1、Y_2、…、Y_m;他们的方向矢量分别是 $a_1,a_2,\cdots,a_n$和 $b_1,b_2,\cdots,b_m$(注意,每个 a_i和 b_j其实都是一个矢量)。

显然,此时的情况是舌战群儒的扩展,它把 1 个诸葛亮,扩展成了多个。为了描述此时的理想极限,我们设计如下有$(n+m)$个人参与的标准式博弈:

$$G=\{S_1,S_2,\cdots,S_n,T_1,T_2,\cdots,T_m;u_1,u_2,\cdots,u_n,v_1,v_2,\cdots,v_m\}$$

参与者 i(鹰派人物 $X_i, 1 \leqslant i \leqslant n$)的战略空间 S_i定义为 $S_i=\{0 \leqslant x_{ji} \leqslant 1; 1 \leqslant j \leqslant N(i),\ x_{1i}+x_{2i}+\cdots+x_{N(i)i}=1\}$。

参与者 $n+i$(鸽派人物 $Y_i, 1 \leqslant i \leqslant m$)的战略空间 T_i定义为 $T_i=\{0 \leqslant y_{ji} \leqslant 1; 1 \leqslant j \leqslant N(n+i),\ y_{1i}+y_{2i}+\cdots+y_{N(n+i)i}=1\}$。

于是,博弈的各与方的战略空间,都是度量空间的非空紧集。

n 个鹰派人物自愿地将自己分为 Q 个联盟,P_1、P_2、…、P_Q使得每个鹰派人物都在且只在某一个联盟中;同一个联盟中的鹰派人物都以本联盟利益为重(不考虑自己个人的利益。自私的鹰派人物可以独自组成一个联盟)。进一步,联盟 P_i将全部 m 个鸽派人物分成 $M(i)$个组,$F_{i1},F_{i2},\cdots,F_{iM(i)}$使得每个鸽派人物都属于且只属于某个组。并且,联盟 P_i还分配了一个权重系数 d_{1i}、d_{2i}、…、$d_{M(i)i}$,这里 $d_{1i}+d_{2i}+\cdots+d_{M(i)i}=1$,对每个 $1 \leqslant i \leqslant Q, 0 \leqslant d_{ik} \leqslant 1$。

于是,对每个鹰派人物 $j, 1 \leqslant j \leqslant n$,如果该鹰派人物属于联盟 P_i,那么,他的利益函数 $u_j(X_1,X_2,\cdots,X_n,Y_1,Y_2,\cdots,Y_m)$就定义为

$$u_j(X_1,X_2,\cdots,X_n,Y_1,Y_2,\cdots,Y_m)=\mid \sum_{k=1}^{M(i)} d_{ki}\, I(A_i,P_i;B_{ik},F_{ik} \mid A_i^C,P_i^C;B_{ik}^C,F_{ik}^C) \mid$$

这里 $A_i=\{a_r, r \in P_i\}$,即,联盟 P_i中鹰派人物的方向矢量之集合;$B_{ik}=\{b_r, r \in F_{ik}\}$,即,联盟 P_i划分出的 F_{ik}组中鸽派人物的方向矢量之集合;这里 P_i^C和 A_i^C分别表示除联盟 P_i之外的所有鹰派人物组成的集合,以及他们的方向矢量集合;F_{ik}^C和 B_{ik}^C分别表示除分组 F_{ik}之外的所有鸽派人物组成的集合,以及他们的方向矢量集合;$I(A_i,P_i;B_{ik},F_{ik} \mid A_i^C,P_i^C;B_{ik}^C,F_{ik}^C)$表示,在条件 P_i^C,F_{ik}^C之下,P_i和 F_{ik}的带向互信息。这里,收益函数取绝对值的原因,仍然是效率约定。

鸽派的利益函数,也可以类似地定义。即,

鸽派中的全部 m 个人员,自愿将自己分为 W 个联盟,H_1、H_2、…、H_W使得每个鸽派人物都在且只在某一个联盟中;同一个联盟中的鸽派人物都以本联盟利益为重(不考虑自己个人的利益。自私的鸽派可以独自形成一个联盟)。进一步,联盟 H_i将全部 n 个鹰派人物分成 $D(i)$个组,E_{i1},E_{i2},…,$E_{iD(i)}$使得每个鹰派人物都属于且只属于某个组。并且,联盟 H_i还分配了一个权重系数f_{1i}、f_{2i}、…、$f_{D(i)i}$,这里 $f_{1i}+f_{2i}+\cdots+f_{D(i)i}=1$,对每个 $1\leqslant i\leqslant W$,$0\leqslant f_{ik}\leqslant 1$。

于是,对每个鸽派 j,$1\leqslant j\leqslant m$,如果该鸽派人物属于联盟 H_i,那么,他的利益函数 $v_j(X_1,X_2,\cdots,X_n,Y_1,Y_2,\cdots,Y_m)$就定义为

$$v_j(X_1,X_2,\cdots,X_n,Y_1,Y_2,\cdots,Y_m)=\mid\sum_{k=1}^{D(i)}f_{ki}\,I(B_i,H_i;A_{ik},E_{ik}\mid B_i^C,H_i^C;A_{ik}^C,E_{ik}^C)\mid$$

这里 $B_i=\{b_r,r\in H_i\}$,即联盟 H_i中鸽派人物的方向矢量之集合;$A_{ik}=\{a_r,r\in E_{ik}\}$,即,联盟 H_i划分出的 E_{ik}组中鹰派人物的方向矢量之集合。这里 H_i^C和 B_i^C分别表示除联盟 H_i之外的所有鸽派人物组成的集合,以及他们的方向矢量集合;E_{ik}^C和 A_{ik}^C分别表示除分组 E_{ik}之外的所有鹰派人物组成的集合,以及他们的方向矢量集合。$I(B_i,H_i;A_{ik},E_{ik}\mid B_i^C,H_i^C;A_{ik}^C,E_{ik}^C)$表示,在条件 H_i^C,E_{ik}^C之下,H_i和 E_{ik}的带向互信息。收益函数取绝对值的原因,仍然是前面的效率约定。

综上,该博弈的各参与方的收益函数也是连续函数。

在按上述过程定义的标准式博弈 $G=\{S_1,S_2,\cdots,S_n,T_1,T_2,\cdots,T_m;u_1,u_2,\cdots,u_n,v_1,v_2,\cdots,v_m\}$ 中,可以直接验证:Glicksberg 定理的条件被全部满足,即,该博弈存在(纯战略或混合战略的)纳什均衡。而达到纳什均衡状态时,无论是鹰派还是鸽派都得到了自己企望的极大理想结果,即,想沟通的,也达到极大值了;想骂的,也骂痛快了。

情况 4:多对多的辩论式对话,例如,头脑风暴研讨会。

考虑有 N 个人参加的头脑风暴研讨会。为避免过于复杂的公式足标体系,我们假设:每个人都是自私的,即,只考虑自己的利益,或者说,不再存在前面几种情况中的联盟。这种假定当然会遗漏一些可能的情况,但是,并不会有实质性的遗漏。况且,在实际应用中,每个人确实经常是几乎只考虑自身利益最大化。

设研讨会的 N 个成员,分别用随机变量 $X_1,X_2,\cdots,X_N$来表示,他们的方向矢量分别为 $a_1,a_2,\cdots,a_N$。并且 X_i是有 $M(i)$个取值的随机变量,$1\leqslant i\leqslant N$。

构造一个有 N 个人参与的标准式博弈 $G=\{S_1,S_2,\cdots,S_N;u_1,u_2,\cdots,u_N\}$ 如下:

参与者 i(研讨人员 X_i,$1\leqslant i\leqslant n$)的战略空间 S_i定义为 $S_i=\{0\leqslant x_{ji}\leqslant 1;1\leqslant j\leqslant M(i),\ x_{1i}+x_{2i}+\cdots+x_{M(i)i}=1\}$。该战略空间显然是度量空间的非空紧集。

对每个参与者 i,在假定他是自私的前提下,为了合理定义他的利益函数,我们考虑如下事实:研讨会中的每个人员,对参与者 i 来说,其重要程度是不会完全相同的(比如,小同行的意见可能更有价值等),因此,参与者 i 将其它 $N-1$ 个参与者分成 $N(i)$组,G_{i1},G_{i2},…,$G_{iN(i)}$,使得每个其它参与者都属于且只属于某个组。并且,参与者 i 还分配了一个权重系数 d_{1i}、d_{2i}、…、$d_{N(i)i}$,这里 $d_{1i}+d_{2i}+\cdots+d_{N(i)i}=1$,对每个 $1\leqslant j\leqslant N(i)$,$0\leqslant d_{ji}\leqslant 1$。

于是,参与者 i 的利益函数 $u_i(X_1,X_2,\cdots,X_n)$就定义为

$$u_i(X_1,X_2,\cdots,X_n)=\mid\sum_{k=1}^{N(i)}d_{ki}\,I(a_i,X_i;A_{ik},G_{ik}\mid A_{ik}^C,G_{ik}^C)\mid$$

这里 $A_{ik}=\{a_r,r\in G_{ik}\}$,即,分组 G_{ik}中各参与者的方向矢量之集合;而 G_{ik}^C和 A_{ik}^C分别表示除分组 G_{ik}和参与者 i 之外的所有参与者组成的集合,以及他们的方向矢量之集合。这里,$I(a_i,X_i;A_{ik},G_{ik}\mid A_{ik}^C,G_{ik}^C)$表示,在条件 G_{ik}^C之下,X_i和 G_{ik}的带向互信息。收益函数中取绝对值的原因,也是前面的效率约定。

于是,每个参与者的收益函数都是连续函数。

在按上述过程定义的标准式博弈 $G=\{S_1,S_2,\cdots,S_n;u_1,u_2,\cdots,u_n\}$ 中,可以直接验证:Glicksberg 定理的条件被全部满足,即,该博弈存在(纯战略或混合战略的)纳什均衡。而达到纳什均衡状态时,所有参与者都得到了自己企望的极大理想结果,即,想沟通的,也达到极大值了;想骂的,也骂痛快了。

4　结束语

在结束本文时,我们真的有好多话想说,虽然,这些话比较零碎:

首先是关于本文题目的考虑:(1)此文本来是系列论文《安全通论》的第 12 部分,而“对话的数学理论”应该只是副标题,但是,与第 11 部分类似,为了突出内容的特色,而且,维纳的问题也太重要,所以,我们将主标题和副标题的位置故意颠倒了。在后续的论文中,除非极特别的情况,我们将不再颠倒主、副标题了。(2)由于仙农研究协作式对话时,将其著名论文(即,创立《信息论》的那篇论文:Shannon C. E., The mathematical theory ofcommunications, Univ. of Illinois Press, 1949)取名叫“通信的数学理论”,所以,我们也仿照仙农,将此文取名为“对话的数学理论”。(3)曾经,我们还想将本文取名为“骂架的数学理论”(其实,骂架更能表现其实质),但是,考虑到这是一篇学术论文,应

该严肃些,所以就只好放弃“骂架”。

其次是“对话”的理解:本文所研究的对话含义,当然包括普通百姓的日常对话(协作式或非协作式),但是,绝不仅限于此。其实,“对话”是网络空间安全中,红客和黑客之间“攻防对抗”的,高度抽象的理想模型。我们之所以在正文中没有明示这一点,原因是,不想转移读者的注意力,毕竟我们是想推进“维纳法庭辩论问题”的解决。不过,细心的读者,应该能够从本文的副标题(《安全通论(12)》)找到一点感觉。

第三点,现在国内学术界有一种说法,叫做“控制论已死”。确实,维纳发表《控制论》以后的情形,完成不同于仙农发表《信息论》以后的情形:响应仙农的著作排山倒海,响应维纳的著作却寥寥无几。但是,这只是假象,其实,包括个人计算机的发明、互联网的创建、人工智能的突破等等,赛搏时代的几乎所有重大突破,都是在维纳控制论思想指引下进行的。或许是因为维纳的著作太高深,后人很难在学术上“接盘”,才使人产生了“控制论已死”的错觉。实际上,《控制论》书中的某些章节,甚至某几行字,都可能开创一门重要的新学科。若不信,等着瞧!

第四点,关于《控制论》的名词翻译:维纳《控制论》的英文原名本来是 Cybernics,它确实研究了许多与“控制”相关的问题。在机械和电子时代,将 Cybernics 翻译成“控制论”好像还有一定的道理。可如今已经是赛搏(Cyber)时代了,半个多世纪前,维纳撰写的专著《Cybernics(赛搏学)》却生生地被翻译成了《控制论》,而且,在全国都家喻户晓了,要想“平反”已经很难了。但是,严重的后果是:维纳的《赛搏学》不仅仅限于控制呀,它过去、现在和将来都将在思维方法和科学目标等方面不断指导人类前进呀! 如果我们永远将错就错,那么,一定会误导许多后生,忽略掉许多重要的思想、方法和课题。

第五点,我有一个感觉(也许不正确),那就是:如果拿远古圣人老子和孔子,来与 IT 时代圣人维纳和仙农,相比较的话,我总觉得仙农有点像孔子,完完整整地建立了一套绝妙的思想体系,让人类直接受益匪浅。而维纳有点像老子,其思想高度深入云霄;一般人很难理解,但是,只要吃透他的三言二语,可能就能让你醍醐灌顶。总之,维纳的著作在中国被严重轻视了,但愿这不是因为把《赛搏学》翻译成《控制论》而造成的!

参考文献:

[1] 杨义先,钮心忻. 安全通论(1)之“经络篇”[EB/OL]. http://blog. sciencenet. cn/blog-453322-944217. html,2015-12-18.

[2] 杨义先,钮心忻. 安全通论(2):攻防篇之“盲对抗”[EB/OL]. http://blog. sciencenet. cn/blog-453322-947304. html,2016-01-01.

[3] 杨义先,钮心忻. 安全通论(3):攻防篇之“非盲对抗”之“石头剪刀布游戏”[EB/OL]. http://blog. sciencenet. cn/blog-453322-948089. html,2016-01-04.

[4] 杨义先,钮心忻. 安全通论(4):攻防篇之“非盲对抗”之“童趣游戏”[EB/OL]. http://blog. sciencenet. cn/blog-453322-949155. html,2016-01-09.

[5] 杨义先,钮心忻. 安全通论(5):攻防篇之“非盲对抗”收官作及“劝酒令”[EB/OL]. http://blog. sciencenet. cn/blog-453322-950146. html,2016-01-13.

[6] 杨义先,钮心忻. 安全通论(6):攻防篇之“多人盲对抗”[EB/OL]. http://blog. sciencenet. cn/blog-453322-954445. html,2016-02-04.

[7] 杨义先,钮心忻. 安全通论(7):黑客篇之“战术研究”[EB/OL]. http://blog. sciencenet. cn/blog-453322-956051. html,2016-02-14.

[8] 杨义先,钮心忻. 安全通论(8):黑客篇之“战略研究”[EB/OL]. http://blog. sciencenet. cn/blog-453322-958609. html,2016-02-25.

[9] 杨义先,钮心忻. 安全通论(9):红客篇[EB/OL]. http://blog. sciencenet. cn/blog-453322-960372. html,2016-03-04.

[10] 杨义先,钮心忻. 安全通论(10):攻防一体的输赢次数极限[EB/OL]. http://blog. sciencenet. cn/blog-453322-984644. html,2016-06-14.

[11] 杨义先,钮心忻. 安全通论(11):信息论、博弈论与安全通论的融合[EB/OL]. http://blog. sciencenet. cn/blog-453322-989745. html,2016-07-11.

[12] N 维纳. 控制论[M]. 郝季仁,译. 北京:科学出版社,2015.

[13] N 维纳. 人有人的用处[M]. 陈步,译. 北京大学出版社,2014.

[14] David M Kreps. 博弈论基础[M]. 高峰,译. 北京:中国社会科学出版社,1999.

[15] Drew Fudenberg, Jean Tirole. 博弈论[M]. 黄涛,译. 北京:中国人民大学出版社,2016.

[16] Thomas M Cover, Joy A Thomas. 信息论基础[M]. 阮吉寿,张华,译. 北京:机械工业出版社出版,2007.