文章编号：2096-1618(2016)06-0549-09
稿件来源：科学网
网　　址：http://blog.sciencenet.cn/blog-453322-989745.html
发表时间：2016-07-11

安全通论(11)

——《信息论》、《博弈论》与《安全通论》的融合：刷新您的通信观念

杨义先，　钮心忻
(北京邮电大学信息安全中心，北京 100876)

摘要：在信息领域，有一本圣经，叫《信息论》。在经济学领域，也有一本圣经，叫《博弈论》。这两本圣经，几乎同时诞生于20世纪中叶，分别由仙农和冯.诺伊曼创立。但是，过去七十年来，谁也没想到，这两本圣经其实是同一本圣经的上下两册，它们的灵魂是完全一致的。而偶然发现这个秘密，并将这两本圣经融合起来的，便是笔者正在努力探索中的《安全通论》。

0　引言

仙农和冯.诺伊曼无疑是第三次工业革命的灵魂人物。作为科学家，他们对信息社会的贡献无与伦比，堪称信息社会之父。

仙农的《信息论》可能是20世纪最重要的学问之一，而且，它对人类的影响还将持续下去，甚至会变得越来越重要。近百年来，正反两方面的事实证明：若没有《信息论》，就不会有人类的今天，更不可能有网络时代、大数据时代、云计算时代、物联网时代等等。

冯.诺伊曼的《博弈论》对人类文明的影响也大得惊人，特别是经天才数学家纳什精练后，《博弈论》几乎就成为了现代经济学的主宰，由它催生的诺贝尔奖至少一长串。

过去七十年来，《信息论》和《博弈论》在各自领域中，都扮演着“圣经”的角色。虽然，后人研究信息论在股票市场中的应用时，也偶尔提到“博弈”两字；在研究数据压缩时，也提到过“博弈”。同样，在经济学的许多著作中，“信息”或者“信息论”更是经常出现。但是，客观地说，无论是信息论研究中提到博弈，还是经济学(博弈论)研究中提到信息或信息论，其实，双方都只是在赶时髦，用用对方的名词概念，装点自己的门面而已，最多不过是借用一下思想。实际上，在信息论界，大家对《博弈论》知之甚少；同样，在博弈论界，大家对《信息论》也几乎不懂。可以说，在全世界，同时精通并深入研究《博弈论》和《信息论》的人屈指可数。

非常意外的是，我们在研究《安全通论》时，偶然发现，《信息论》和《博弈论》之间的关系之密切，完全超出了许多人的想象。甚至，刷新了人们过去对通信的观念，让通信，特别是网络通信，以全新的面貌重新登场。比如：

(1)过去，人们咬定，通信(1对1通信)就是比特信息从发端到收端的传输；其目的就是尽可能多地、可靠地传输比特流。但是，现在看来，通信其实还可以是一种博弈；是收信方和发信方之间，为了从对方获取最大信息量(互信息)的一种博弈。而且，这种博弈一定存在纳什均衡，此时，收信方和发信方各自从对方所获得的信息量相等，同为仙农称之的“信道容量”。

(2)网络通信的“信息传输极限”一直就是多用户网络信息论中的头等难题，其难度之大，以至于人们根本就不知道该如何来描述它。人们虽然自认为已经在“多输入单输出信道”等几种最简单的多用户网络信道容量计算方面，取得了最终结果(其实并非最终结果，详见本文第四节的论述)；但是，面对绝大部分的多用户网络的信道容量，人们仍然束手无策。甚至，像广播信道这种简单而常见的信道，都使大家不知所措。

为什么会出现这种尴尬局面呢？因为，如果按过去的观念，让比特串在多用户信道中去互相碰撞、转化、流动、传输，那么，当然就难以理出头绪，而且越传越乱。甚至，连每个用户终端对自己的传输需求，优化目标，都说不清楚，就更不可能有最优化结果了。

现在，重新来审视多用户网络通信，将它看成终端用户之间的一种“多参与者博弈”，其目的是要，从其锁定的对象终端处，获得最大的信息量。于是，网络信道容量这个大难题，便可以经过简单的两步轻松解决：

第1步，每个博弈者锁定自己的需求(即，优化目标)，比如，他对哪些终端的信息更感兴趣(兴趣大的赋予更大的权值，没兴趣的赋予0权值)，对哪些终端的信息要区别对待(不加区别的可以放在同一个组

内,统一考虑);

第 2 步,证明该种博弈刚好存在纳什均衡(非常幸运地得益于互信息函数 $I(X;Y)$ 的凹性)。而且,在纳什均衡状态时,每个终端就都得到了自己的最优化结果。

(3)"信道容量"其实并非像过去那么死板,更不是由几条固定直线切割而成的不变区域,而是在根据各博弈方的优化目标而变化的;优化目标不同,优化结果当然应该不同。而在网络通信中,各方的优化目标确实千差万别。

(4)《信息论》、《博弈论》和《安全通论》三者之间融合后,就有:红客与黑客之间的攻防对抗,其实既是红与黑的博弈,也是红与黑之间的通信。若将通信看作红《安全通论》中的红黑对抗,那么,这时红与黑的攻防招数相当,即,红客能实施的所有手段,黑客也能实施。若将《安全通论》中的红黑对抗看作通信,那么,这种通信是非对称的,即,比特的正向流动与反向流动性质不同。若将《安全通论》中的红黑对抗看作博弈,那么,由于每个红客或黑客的攻防招数是有限的,所以,无论怎么去定义其利益函数,这种博弈都一定存在纳什均衡(包含纯战略或混合战略)。

综上可知,在被融合的三论中,《博弈论》最广,《信息论》最深,《安全通论》粘性最强。虽然与《信息论》和《博弈论》相比,《安全通论》不过是九牛之一毛,但是,《安全通论》既然能把两大"牛理论"粘在一起,就说明其本身还是有一定价值的。

本文本来是作者《安全通论》系列论文中的第 11 部分,但是,由于《信息论》与《博弈论》的融合太出人意料,所以,我们将本文的题目和副标题换了个位,以突出"融合"之意。

由于许多博弈论专家不懂信息论,同样,许多信息论专家不懂博弈论,所以,为了读者阅读方便,我们在下面第二节和第三节中,分别把《博弈论》和《信息论》的最精华部分进行了凝练,熟悉的读者可以跳过,而直接进入本文的核心内容:第四节,三论融合。

1 《博弈论》核心凝练

为保持全文的完整性,本小节将《博弈论》的最核心成果(见参考文献[11-12])凝练如下。熟悉博弈论的读者,可以直接跳过此节。

博弈的标准式表述包括:(1)博弈的参与者;(2)每个参与者可供选择的战略(行动)集;(3)针对所有参与者可能选择的战略组合,每个参与者获得的收益。在一般的 n 个参与者的博弈中,把参与者从 1 至 n 排序,设其中任一参与者的序号为 i,令 S_i 代表参与者 i 可以选择的战略集合(称为 i 的战略空间,其实就是行动空间),其中任一特定的战略用 s_i 表示(或写为 $s_i \in S_i$ 表示战略 s_i 是战略集 S_i 中的要素)。令 $(s_1,s_2,\cdots,s_n)$ 表示每个参与者选定一个战略而形成的战略组合,u_i 表示第 i 个参与者的收益函数,$u_i(s_1,s_2,\cdots,s_n)$ 即为参与者选择战略 $(s_1,s_2,\cdots,s_n)$ 时,第 i 个参与者的收益。综合而言,有:

定义 1(博弈标准式):在一个 n 人博弈的标准式表述中,参与者的战略空间为 $S_1,S_2,\cdots,S_n$,收益函数为 $u_1,u_2,\cdots,u_n$,我们用 $G=\{S_1,S_2,\cdots,S_n;u_1,u_2,\cdots,u_n\}$ 表示此博弈。

定义 2(严格劣战略):在标准式的博弈 $G=\{S_1,S_2,\cdots,S_n;u_1,u_2,\cdots,u_n\}$ 中,令 s'_i 和 s''_i 代表参与者 i 的两个可行战略(即,s'_i 和 s''_i 是 S_i 中的元素)。如果对其他参与者的每个可能战略组合,i 选择 s'_i 的收益都小于其选择 s''_i 的收益,则称战略 s'_i 相对于战略 s''_i 是严格劣战略,即,如下不等式:

$$u_i(s_1,\cdots,s_{i-1},s'_i,s_{i+1},\cdots,s_n)<u_i(s_1,\cdots,s_{i-1},s''_i,s_{i+1},\cdots,s_n) \quad (1)$$

对其他参与者在其战略空间 $S_1,\cdots,S_{i-1},S_{i+1},\cdots,S_n$ 中每一组可能的战略 $(s_1,\cdots,s_{i-1},s_{i+1},\cdots,s_n)$ 都成立。

理性的参与者不会选择严格劣战略,因为,他(对其他人选择的战略)无法做出这样的推断,使这一战略成为他的最优反应。在博弈中,每个参与者要选择的战略,必须是针对其他参与者选择战略的最优反应,这种理论推测结果可以叫做"战略稳定"或"自动实施"的,因为,没有哪位参与者愿意独自离弃他所选定的战略,我们把这一状态称为"纳什均衡"。

定义 3(纯战略纳什均衡):在 n 个参与者标准式博弈 $G=\{S_1,S_2,\cdots,S_n;u_1,u_2,\cdots,u_n\}$ 中,如果战略组合 $\{s_1^*,s_2^*,\cdots,s_n^*\}$ 满足对每个参与者 i,s_i^* 是(至少不劣于)他针对其他 $n-1$ 个参与者所选战略 $\{s_1^*,\cdots,s_{i-1}^*,s_{i+1}^*,\cdots,s_n^*\}$ 的最优反应战略,则称战略组合 $\{s_1^*,s_2^*,\cdots,s_n^*\}$ 是该博弈的一个纳什均衡。即,

$$u_i\{s_1^*,\cdots,s_{i-1}^*,s_i^*,s_{i+1}^*,\cdots,s_n^*\}\geqslant u_i\{s_1^*,\cdots,s_{i-1}^*,s_i,s_{i+1}^*,\cdots,s_n^*\} \quad (2)$$

对所有 S_i 中的 s_i 都成立,亦即,s_i^* 是以下最优化问题的解:

$$\mathrm{Max}\ s_i\in S_i\ u_i\{s_1^*,\cdots,s_{i-1}^*,s_i,s_{i+1}^*,\cdots,s_n^*\} \quad (3)$$

(注:由于科学网博客显示器的限制,文中我们无法用标准公式来显示诸如"双重足标"等公式,所以,此处及后面,凡是在多重足标中,我们都不得不将 s_i 与 s_i 视为等同。幸好这样做并不会引起混乱。)

为更清晰地理解定义 3 中的纳什均衡,我们设想有一标准式博弈 $G=\{S_1,S_2,\cdots,S_n;u_1,u_2,\cdots,u_n\}$,博弈论为它提供的解为战略组合 $\{s'_1,s'_2,\cdots,s'_n\}$,如果

$\{s'_1, s'_2, \cdots, s'_n\}$不是 G 的纳什均衡,就意味着存在一些参与者 i,s'_i 不是针对$\{s'_1, \cdots, s'_{i-1}, s'_{i+1}, \cdots, s'_n\}$的最优反应战略,即在 S_i 中存在 s''_i,使得:

$$u_i(s'_1, \cdots, s'_{i-1}, s'_i, s'_{i+1}, \cdots, s'_n) < u_i(s'_1, \cdots, s'_{i-1}, s''_i, s'_{i+1}, \cdots, s'_n) \quad (4)$$

那么,如果博弈论提供的战略组合解$\{s'_1, s'_2, \cdots, s'_n\}$不是纳什均衡,则至少有一个参与者有动因偏离理论的预测,使得博弈的真实进行和理论预测不一致。因此,对给定的博弈,如果参与者之间要商定一个协议,决定博弈如何进行,那么,一个有效的协议中的战略组合必须是纳什均衡的战略组合,否则,至少有一个参与者不会遵守该协议。

再换一个角度来看纳什均衡:仍记 S_i 为参与者 i 可以选择的战略集,并且,对每一个参与者 i,s_i^* 为其针对另外 $n-1$ 个参与者所选战略的最优反应,则战略组合$(s_1^*, s_2^*, \cdots, s_n^*)$为博弈的纳什均衡,即,

$$u_i(s_1^*, \cdots, s_{i-1}^*, s_i^*, s_{i+1}^*, \cdots, s_n^*) \geqslant u_i(s_1^*, \cdots, s_{i-1}^*, s_i, s_{i+1}^*, \cdots, s_n^*) \quad (5)$$

对 S_i 中的每个 s_i 都成立。

但是,如果仅按定义 3 来定义纳什均衡,那么,在某些情况下,这样的纳什均衡就不存在,更一般的有:在博弈中,一旦每个参与者都竭力猜测其他参与者的战略选择,那么,就不存在“由定义 3 所定义的纳什均衡”,因为,这时参与者的最优行为是不确定的,而博弈的结果必然要包括这种不确定性。因此,又引入了所谓“混合战略”的概念,它可以解释为一个参与者对其他参与者行为的不确定性。从而,将纳什均衡的定义扩展到包括混合战略的情况。

规范地说,参与者 i 的一个混合战略,就是在其战略空间 S_i 中(一些或全部)战略的概率分布,于是,称前面 S_i 中的那些战略为 i 的纯战略。对于完全信息同时行动博弈来说,一个参与者的纯战略,就是他可以选择的不同行动。例如,在“猜硬币正反面”博弈中,S_i 含有两个纯战略,分别为“猜正面向上”和“猜反面向上”,这时,参与者 i 的一个混合战略为概率分布$(q, 1-q)$,其中 q 为“猜正面向上”的概率,$1-q$ 为“猜反面向上”的概率,且 $0 \leqslant q \leqslant 1$。混合战略$(0,1)$表示参与者的一个纯战略,即,只“猜反面向上”;类似地,混合战略$(1,0)$表示只“猜正面向上”的纯战略。

更一般地,假设参与者 i 有 K 个纯战略:$S_i = \{s_{i1}, s_{i2}, \cdots, s_{iK}\}$,则参与者 i 的一个混合战略就是一个概率分布$(p_{i1}, p_{i2}, \cdots, p_{iK})$,其中 p_{ik} 表示对所有 $k=1,2,\cdots,K$,参与者 i 选择战略 s_{ik} 的概率,由于 p_{ik} 是一个概率,所以对所有 $k=1,2,\cdots,K$,有 $0 \leqslant p_{ik} \leqslant 1$ 且 $p_{i1}+p_{i2}, \cdots + p_{iK}=1$。我们用 p_i 表示基于 S_i 的任意一个混合战略,其中包含了选择每个纯战略的概率,正如前面用 s_i 表示 S_i 内任意一个纯战略一样。

定义 4(混合战略):对标准式博弈 $G=\{S_1, S_2, \cdots, S_n; u_1, \cdots, u_n\}$,假设 $S_i = \{s_{i1}, s_{i2}, \cdots, s_{iK}\}$。那么,参与者 i 的一个混合战略为概率分布 $p_i = (p_{i1}, p_{i2}, \cdots, p_{iK})$,其中对所有 $k=1,2,\cdots,K$,都有 $0 \leqslant p_{ik} \leqslant 1$ 且 $p_{i1}+p_{i2}, \cdots + p_{iK}=1$。

为了将纳什均衡概念扩展到混合战略的最优反应,先把两人博弈的情况描述清楚(这也是我们为了在后面将《博弈论》与《信息论》融合,而做的准备工作)。

先考虑只有两个博弈者。令 J 表示第 1 个参与者(博弈者)S_1 中包含纯战略的个数,K 表示第 2 个博弈者 S_2 包含纯战略的个数,则 $S_1 = \{s_{11}, s_{12}, \cdots, s_{1J}\}$,$S_2 = \{s_{21}, s_{22}, \cdots, s_{2K}\}$,我们用 s_{1j} 和 s_{2k} 分别表示 S_1 和 S_2 中任意一个纯战略。

如果参与者 1 推断参与者 2 将以 $P_2 = (p_{21}, p_{22}, \cdots, p_{2K})$ 的概率选择战略$(s_{21}, s_{22}, \cdots, s_{2K})$,则参与者 1 选择纯战略 s_{1j} 的期望收益为:

$$\sum_{k=1}^{K} p_{2k} u_1(s_{1j}, s_{2k}) \quad (6)$$

且参与者 1 选择混合战略 $P_1 = (p_{11}, p_{12}, \cdots, p_{1J})$ 的期望收益为:

$$v_1(P_1, P_2) = \sum_{j=1}^{J} p_{1j} \left[\sum_{k=1}^{K} p_{2k} u_1(s_{1j}, s_{2k}) \right] = \sum_{j=1}^{J} \sum_{k=1}^{K} p_{1j} \cdot p_{2k} u_1(s_{1j}, s_{2k}) \quad (7)$$

其中,$p_{1j} \cdot p_{2k}$ 表示参与者 1 选择 s_{1j} 且参与者 2 选择 s_{2k} 的概率。根据公式(7),参与者 1 选择混合战略 P_1 的期望收益,等于按公式(6)给出的每个纯战略$\{s_{11}, s_{12}, \cdots, s_{1J}\}$的期望收益的加权和,其权重分别为各自的概率$(p_{11}, p_{12}, \cdots, p_{1J})$,那么,参与者 1 的混合战略$(p_{11}, p_{12}, \cdots, p_{1J})$要成为他对参与者 2 战略 P_2 的最优反应,其中任何大于 0 的 p_{1j} 相对应的纯战略,必须满足:

$$\sum_{k=1}^{K} p_{2k} u_1(s_{1j}, s_{2k}) \geqslant \sum_{k=1}^{K} p_{2k} u_1(s'_{1j}, s_{2k})$$

对 S_1 中每一个 s'_{1j} 都成立。这表明,如果一个混合战略要成为 P_2 的最优反应,那么,这个混合战略中每一个概率大于 0 的纯战略本身,也必须是对 P_2 的最优反应。反过来讲,如果参与者 1 有 n 个纯战略都是 P_2 的最优反应,则这些纯战略全部或部分的任意线性组合(同时,其他纯战略的概率为 0)形成的混合战略,同样是参与者 1 对 P_2 的最优反应。

为给出扩展的纳什均衡的正式定义,我们还需要计算:当参与者 1 和 2 分别选择混合战略 P_1 和 P_2 时,参与者 2 的期望收益。如果参与者 2 推断参与者 1 将分别以 $P_1 = (p_{11}, p_{12}, \cdots, p_{1J})$ 的概率选择战略$\{s_{11}, s_{12}, \cdots, s_{1J}\}$,则参与者 2 分别以概率 $P_2 = (p_{21}, p_{22}, \cdots, p_{2K})$ 选择战略$\{s_{21}, s_{22}, \cdots, s_{2K}\}$时的期望收益为

$$v_2(P_1, P_2) = \sum_{k=1}^{K} p_{2k} \left[\sum_{j=1}^{J} p_{1j} u_2(s_{1j}, s_{2k}) \right] = \sum_{j=1}^{J} \sum_{k=1}^{K} p_{1j} \cdot p_{2k} u_2(s_{1j}, s_{2k}) \quad (8)$$

在给出 $v_1(P_1,P_2)$ 和 $v_2(P_1,P_2)$ 之后，我们便可以重新表述纳什均衡的必要条件了，即，每一参与者的混合战略是另一参与者混合战略的最优反应：一对混合战略 (P_1^*,P_2^*) 要成为纳什均衡，则 P_1^* 必须满足

$$v_1(P_1^*,P_2^*)\geqslant v_2(P_1,P_2^*) \tag{9}$$

对 S_1 中战略所有可能的概率分布 P_1 都成立，并且 P_2^* 必须满足

$$V_2(P_1^*,P_2^*)\geqslant v_2(P_1^*,P_2) \tag{10}$$

对 S_2 中战略所有可能的概率分布 P_2 都成立。

定义 5（混合战略纳什均衡）：在两个参与者标准式博弈 $G=\{S_1,S_2;u_1,u_2\}$ 中，混合战略 (P_1^*,P_2^*) 是纳什均衡的充分必要条件是：每一参与者的混合战略，是另一参与者混合战略的最优反应，即，公式（9）和（10）必须同时成立。

在任何博弈中，一个纳什均衡（包括纯战略和混合战略均衡）都表现为参与者之间最优反应对应的一个交点，即使该博弈的参与者在两人以上，或有些（或全部）参与者有两个以上的纯战略。

到此，我们就可以介绍博弈论的最核心定理，称为“纳什均衡定理”，它由数学家纳什于 1950 年发现：

纳什均衡定理：在 n 个参与者的标准式博弈 $G=\{S_1,S_2,\cdots,S_n;u_1,u_2,\cdots,u_n\}$ 中，如果 n 是有限的，且对每个 i，S_i 也是有限的，则博弈存在至少一个纳什均衡，均衡可能包含混合战略。

该定理要求策略空间是有限的（即，每个参与者的可选策略个数有限），但是，如果策略空间是无限时，情况又会怎样呢？1952 年，Debreu、Glicksberg 和 Fan 证明了下面的定理 1，Glicksberg 证明了下面的定理 2。

定理 1：在 n 个参与者的标准式博弈 $G=\{S_1,S_2,\cdots,S_n;u_1,u_2,\cdots,u_n\}$ 中，如果 n 是有限的，且对每个 i，S_i 是欧式空间的非空紧凸集。如果收益函数 u_i 对 s_i $(s_i\in S_i)$ 是连续的，且对 s_i 是拟凹的，那么，该博弈存在纯战略纳什均衡。

定理 2：在 n 个参与者的标准式博弈 $G=\{S_1,S_2,\cdots,S_n;u_1,u_2,\cdots,u_n\}$ 中，如果 n 是有限的，且对每个 i，S_i 是度量空间的非空紧集。如果收益函数 u_i 是连续的，那么，该博弈存在混合战略的纳什均衡。

2 《信息论》核心凝练

为保持全文完整性，本小节将《信息论》的最核心成果（见文献[13]）凝练如下。熟悉《信息论》的读者，也可以直接跳过此节。

如果将所有可能的通信方案看成一个集合，那么，《信息论》就给出了这个集合的两个最重要的临界值：（1）数据压缩达到最低程度的方案，对应于该集合的下界 $\min I(X,X^*)$，即，所有数据压缩方案所需要的描述速率不得低于该临界值 $I(X,X^*)$，仙农信源编码定理；（2）数据传输率的最大值就是信道容量，$\mathrm{Max}I(X,Y)$，仙农信道编码定理。

网络信息论是当前通信理论研究的焦点，即，在干扰和噪声的情况下，如何建立大量发送器到大量接收器之间的通信同步率理论。但是，目前，全世界都正在泥潭中痛苦挣扎。

信息论的几个最基本的概念有：

熵：设随机变量 X 的概率分布函数为 $p(x)$，那么，X 的熵定义为 $H(X)=-\sum_{xp}(x)\log_2 p\ (x)$。熵的量纲为比特。熵可看作随机变量 X 的平均不确定度的度量，即，在平均意义下，为了描述该随机变量 X 所需要的比特数。特别，如果 X 是二值随机变量，比如，$p(X=1)=q$，$p(X=0)=1-q$，那么，$H(X)=-q\log q-(1-q)\log(1-q)$，它是实数区间[0,1]内，关于 q 的凹函数。

条件熵：一个随机变量 X，在给定另一个随机变量 Y 的条件下的熵，记为 $H(X\mid Y)$。

相对熵：两个概率密度函数为 $p(x)$ 和 $q(x)$ 之间的相对熵定义为 $D(p/\!/q)=\sum x\in Xp(x)\log[p(x)/q(x)]=Ep\log[p(X)/q(X)]$。

互信息：由另一个随机变量导致的，原随机变量不确定度的缩减量。具体地说，设 X 和 Y 是两个随机变量，那么，这个缩减量就是互信息 $I(X;Y)=H(X)-H(X\mid Y)=\sum_{x,y}p(x,y)\log\{p(x,y)/[p(x)p(y)]\}=D(p(x,y)/\!/[p(x)p(y)])$。互信息 $I(X;Y)$ 也是两个随机变量相互之间独立程度的度量，它关于 X 和 Y 对称，且非负；当且仅当 X 与 Y 相互独立时，其互信息为 0。

条件互信息：随机变量 X 和 Y，在给定随机变量 Z 的条件互信息定义为：$I(X;Y\mid Z)=H(X\mid Z)-H(X\mid Y,Z)=E_{p(x,y,z)}\log[p(x,y,z)/(p(x\mid z)p(y\mid z))]$。

定理 3：（互信息的凹凸性定理）：设二维随机变量 (X,Y) 服从联合概率分布 $p(x,y)=p(x)p(y\mid x)$。如果固定 $p(y\mid x)$，则互信息 $I(X;Y)$ 就是关于 $p(x)$ 的凹函数（互信息其实是任意闭凸集上的凹函数，因而，局部最大值也就是全局最大值。又由于互信息是有限的，所以，在信道容量的定义中，可以只使用 max，而不必用 sup。而且，这个最大值（信道容量）可以利用标准的非线性最优化技术求解）；而如果固定 $p(x)$，则互信息 $I(X;Y)$ 就是关于 $p(y\mid x)$ 凸函数。在条件互信息的情况下，如果固定 $p(y\mid x,z)$，则互信息 $I(X;Y\mid Z)$ 就是关于 $p(x\mid z)$ 的凹函数，也是关于 $p(x)$ 的凹函数。

通信信道：它是这样一个系统，其输出信号按概率依赖于输入信号。其特征由一个转移概率矩阵 $p(y\mid$

x)决定,该矩阵给出了在已知输入情况下,输出的条件概率分布。

二元对称信道:输入与输出都只有两个符号(0,1),并且,输出与输入相同的概率为 $1-p$,输出与输入相异的概率为 p。这里 $0\leqslant p\leqslant 1$。

信道容量:对于输入信号为 X,输出信号为 Y,的通信信道,定义它的信道容量 C 为 $C=\max_{p(x)} I(X;Y)$。

好了,现在来介绍《信息论》中核心的定理,仙农信道编码定理。它可以描述为:

仙农信道编码定理:对于离散无记忆信道,小于信道容量 C 的所有码率都是可达的。或者可以形象地解释为:码率不超过信道容量 C 的所有信号,都能够被无误差地从发方传输到收方。

3　三论融合

有了上述第二节(《博弈论》)和第三节(《信息论》)的预备工作后,现在就可以介绍本文的核心内容了。我们将利用《安全通论》,把《博弈论》的核心(纳什均衡)和《信息论》的核心(信道容量)进行充分融合,并顺便解决网络信息论中存疑数十年的一些难题。

首先来重视审视一下经典的"1 对 1 通信":构造一个特殊的标准式博弈 $G=\{S_1,S_2;u_1,u_2\}$,它有两个参与者,分别是甲方(包含但不限于发信方 X)和乙方(包含但不限于收信方 Y),假设固定一个转移矩阵 $\boldsymbol{A}=[A_{ij}]$(它等同于确定某个信道的转移矩阵,即,$A_{ij}=p(x=i\mid y=j)$, $1\leqslant i\leqslant n$, $1\leqslant j\leqslant m$),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,也就是欧式空间的非空紧凸集)。

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,也就是欧式空间的非空紧凸集)。

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 $u_1(s_1,s_2)=\sum_{j=1}^{m} q_j \sum_{i=1}^{n} A_{ij}\log[A_{ij}/p_i]$。提醒:其实这个收益函数就是 $I(X;Y)$,即,X 与 Y 的互信息,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 $P(Y=j)=q_j$,$(1\leqslant j\leqslant m, 0\leqslant q_j\leqslant 1)$。根据定理 3(互信息的凹凸性定理),在信道 $p(x\mid y)$ 被固定的条件下,u_1 对 $s_1(s_1\in S_1)$ 是连续的,且对 s_1 是凹函数(当然更是拟凹的了)。

参与者 2(乙方)的收益函数 $u_2(s_1,s_2)$ 定义为 $u_2(s_1,s_2)=\sum_{i=1}^{n} p_i \sum_{j=1}^{m} B_{ji}\log[B_{ji}/q_j]$。提醒:其实这个收益函数就是 $I(Y;X)$,即,Y 与 X 的互信息。同样,根据定理 3(互信息的凹凸性定理),在信道 $p(x\mid y)$ 被固定的条件下(因为 $p(y\mid x)$ 已被固定,所以 $p(x\mid y)$ 也已被固定),u_2 对 $s_2(s_2\in S_2)$ 是连续的,且对 s_2 是凹函数(当然更是拟凹的了)。(注:虽然通过《信息论》,我们明明知道 $I(X;Y)=I(Y;X)$,即,该博弈中的两个参与者的收益函数是相等的,但是,为了使相关描述更像标准博弈,所以,我们故意如此赘述。后面有些赘述也是同样目的。)

于是,定理 1 中的条件就被全部满足,即,我们人为构造的标准式博弈 $G=\{S_1,S_2;u_1,u_2\}$ 就存在纯战略的纳什均衡。这就是说存在着某对纯战略 $s_1^*=(p_1^*,p_2^*,\cdots,p_n^*)$ 和 $s_2^*=(q_1^*,q_2^*,\cdots,q_m^*)$,它们分别对应于某对输入和输出的随机变量 X^* 和 Y^*(这里 $P(X^*=i)=p_i^*$, $1\leqslant i\leqslant n$, $p_1^*+p_2^*+\cdots+p_n^*=1$ 和 $P(Y^*=j)=q^*j$, $1\leqslant j\leqslant m$, $q_1^*+q_2^*+\cdots+q_{m=1}^*$),使得,同时成立

任意给定 $s_2\in S_2$,一定有 $u_1(s_1^*,s_2)\geqslant u_1(s_1,s_2)$,对所有 $s_1\in S_1$

和

任意给定 $s_1\in S_1$,一定有 $u_2(s_1,s_2^*)\geqslant u_2(s_1,s_2)$,对所有 $s_2\in S_2$

换句话说,根据信道容量的定义,就知道 $u_1(s_1^*,s_2^*)=u_2(s_1^*,s_2^*)=C$,信道 $p(y\mid x)$ 的信道容量,即,甲方和乙方博弈的纳什均衡点刚好就是当甲方作为该信道的发方时、乙方作为该信道的收信方时,的信道容量。所以,我们就把这个结果简述为如下定理 4。至此,我们就发现了《信息论》与《博弈论》之间的第一处核心融合,即:

定理 4:(信道容量与纳什均衡的融合定理):当信道固定时,若以输入和输出之间的互信息为收益函数,那么,发信方和收信方之间的标准式博弈一定存在纯战略的纳什均衡,而且,当达到纳什均衡时,他们的收益函数就刚好是收发双方之间的信道的信道容量。

特别说明:我们之所以将上述博弈构造成发方和发方之间的博弈,是因为这样比较形象直观。其实,更严谨地说,我们本应该构造一个由收发双方联合起来与信道之间的"三人博弈"(或者是信道与发信方(或收信方)之间的二人博弈),它的最终纳什均衡状态也刚刚达到信道容量的极限值,不过,由于这种博弈的描述比较复杂,而且效果又一样,所以此处略去。

上面的定理 4 几乎完全刷新了人们对通信的观念:原来,所谓通信,只不过是收发双方的一种特殊博

弈而已。那么,这种观念的刷新有价值吗?答案是:太有价值了,比如,基于这种新观念,我们就可以解决过去数十年来,网络信息论中有关信道容量的一些难题。注:用博弈论的思路去考虑 1 对 1 通信的意义不大,因为,仙农在这种情况下已经给出了非常漂亮的结果,但是,为什么我们要用 1 对 1 的情况为例来说明定理 4 呢,这主要是想使相关描述更简捷。再次提醒读者:千万别过分地被输入和输出的关系锁定,否则,就会对相关的博弈误解。

3.1 重新审视星形网络的信道容量

过去,《信息论》的做法是将星形网络分为"多输入单输出信道"和"广播信道(单输入多输出信道)"两种情况,而且还真的用仙农随机编码的思路,非常巧妙地把多输入信道的信道容量给"计算出来了"(后面将看到,其实,人们并没有完全计算出来,只是在一种特殊情况下计算出来了而已);但是,面对广播信道时,大家就束手无策了,并将这个难题遗留至今。

现在我们从博弈论的角度,再来看这个问题时,突然发现,原来人类走了一个大弯路,把简单问题复杂化了。

为了把这个问题说清楚,我们先回头看看 1 对 1 通信的情况:

看待一个随机变量时,有两个层次:其一,宏观一点,只看其分布概率,比如,将扔硬币这个随机变量 X,看成 $P(X=0)=P(X=1)=0.5$;其二,微观一点,用某个具体的样本来代表,比如,用一连串扔硬币的结果 $x_1,x_2,\cdots,x_n,\cdots$ 来表示。当然,同一个概率分布的不同具体样本之间的差别,可能会非常大,它们之间的平均汉明距离完全有可能大于 0;但是,所以具体样本的统计特性是相同的。

由于通信的情况很特殊,一方面,仙农将输入和输出信号都当作随机变量,用分布概率表示;另一方面,每次收端和发端所处理的序列都是实实在在的具体样本,即,二元序列。于是,人们就反复在概率分布和具体样本之间纠结,其中,最典型的案例是仙农自己:本来由于其凹性,互信息 $I(X,Y)$ 的最大值(max)和上确界(sup)就是一回事了,即,从分布概率角度来看,互信息的最大值是可达的(即,信道容量),既然,某个概率分布的随机变量 X 使 $I(X,Y)$ 达到最大值,那么,X 的某个具体样本也就一定能够达到该值,虽然并不知道到底是哪个样本能达到最大值。可是,仙农却还想进一步把那个达到最大值的具体样本给找出来,结果,虽然经过了一大堆复杂的随机编码推理,最终也仍然只证明了"达到最大值的那个样本存在",而并没有把那个达到最大值的样本给找出来。于是,才上演了半个多世纪以来,全世界信道编码理论专家们,挖空心思、前赴后继地追求仙农极限的苦剧。至今,仙农极限还摆在那里,可望而不可即!

仙农的这种技巧,在 1 对 1 通信中时,非常令人震撼;但是,在网络通信时,这种"随机编码"的思路,就将人类带入了死胡同,导致半个多世纪的迷茫。

现在,用博弈的观点来看,通过定理 4,在 1 对 1 通信时,收发双方达到纳什均衡的那个纯战略 s_1^* 和 s_2^*,就是真真切切的接收信号和发射信号。

先看 2 输入单输出信道:

此时,有两个发信方 X_1 和 X_2,有一个收信方 Y。现在考虑他们三者之间的一个标准式博弈 $G=\{S_1,S_2,S;u_1,u_2,u\}$:

参与者 1(发信方 X_1)的战略空间 S_1 定义为 $S_1=\{0\leqslant x_{i1}\leqslant 1:1\leqslant i\leqslant n,\ x_{11}+x_{21}+\cdots+x_{n1}=1\}$。

参与者 2(发信方 X_2)的战略空间 S_2 定义为 $S_2=\{0\leqslant x_{i2}\leqslant 1:1\leqslant i\leqslant N,\ x_{12}+x_{22}+\cdots+x_{N2}=1\}$。

参与者 3(收信方)的战略空间 S_3 定义为 $S_3=\{0\leqslant y_i\leqslant 1:1\leqslant i\leqslant m,y_1+y_2+\cdots+y_m=1$。

他们三者之间的战略空间虽然很清楚,但是,在定义其收益函数时,情况就完全不一样了,比如:对该三个参与者的任意纯战略 X_1、X_2 和 Y。

情况 1:如果两个发信方都是自私的,他们只想为自己争取最大利益;并且如果收信方不加区别地对待发信方,那么,他们的三个收益函数就分别定义为:$u_1(X_1,X_2,Y)=I(X_1;Y\mid X_2)$;$u_2(X_1,X_2,Y)=I(X_2;Y\mid X_1)$;$u_3(X_1,X_2,Y)=I(X_1,X_2;Y)$。

情况 2:如果两个发信方都是自私的,他们只想为自己争取最大利益;那么,发信各方的收益函数就分别定义为:$u_1(X_1,X_2,Y)=I(X_1;Y\mid X_2)$;$u_2(X_1,X_2,Y)=I(X_2;Y\mid X_1)$。如果收信方对两个发信方是区别对待的,那么收信方的收益函数定义为如下加权函数:$u_3(X_1,X_2,Y)=aI(X_1;Y\mid X_2)+bI(X_2;Y\mid X_1)$。$0\leqslant a,b\leqslant 1$ 并且 $a+b=1$。

情况 3:如果两个发信方是无私的,以争取发信方共同利益最大化为目标;收信方不加区别地对待发信方,那么,对该三个参与者的任意纯战略 X_1、X_2 和 Y,他们的三个收益函数就分别定义为:$u_1(X_1,X_2,Y)=u_2(X_1,X_2,Y)=u_3(X_1,X_2,Y)=I(X_1,X_2;Y)$。这便退化成了 1 对 1 通信。

情况 4:如果两个发信方都是无私的,以争取发信方共同利益最大化为目标;那么,发信各方的收益函数就分别定义为:$u_1(X_1,X_2,Y)=u_2(X_1,X_2,Y)=I(X_1,X_2;Y)$。如果收信方对两个发信方是区别对待的,那么收信方的收益函数定义为如果加权函数:$u_3(X_1,X_2,Y)=aI(X_1;Y\mid X_2)+bI(X_2;Y\mid X_1)$。$0\leqslant a,b\leqslant 1$ 并且 $a+b=1$。

仿照定理 4 的证明过程,可以直接验证:在上述 4 种情况下,定理 1 的条件都被全部满足,即,这些博弈都存在纯战略的纳什均衡 X_1^*、X_2^*、Y^*。而达到纳什均衡状态时,收发三方各自的纯战略 X_1^*、X_2^*、Y^*,便是对应于各自企望的最佳结果,而这些最大值所围成的区域,便是信道容量。由此可见,所谓的"信道容量"原来并非像过去那么死板,而是在根据各博弈方的目标而变化的;目标不同,结果当然应该不同。特别是,上述的情况 1,便是过去人们已经研究过的所谓"2 输入单输出信道"情况,显然,人们过去并没有完全解决"多输入单输出信道"的信道容量问题。

至此,我们便明白了,为什么过去广播信道的信道容量成为了难题,因为,大家没有博弈概念,没有搞清楚收发各方的优化目标,而是在"鱼和熊掌兼得"的情况下来试图计算所谓的信道容量,当然,就不可能有结果了。自己都不清楚自己想要什么,怎么可能有最佳策略呢!

下面,我们就在锁定收发各方的利益目标(优化目标)的条件下,给出广播信道相应的"信道容量",即,由纳什均衡状态所围成的区域。

在一般的"广播信道"中,有一个输入 X 和 n 个输出 $Y_1, Y_2, \cdots, Y_n$。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(发信方 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(收信方 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(收信方 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(收信方 Y_n)的战略空间 S_n 定义为 $S_n=\{0 \leqslant y_{in} \leqslant 1 : 1 \leqslant i \leqslant N(n),\ y_{1n}+y_{2n}+\cdots+y_{N(1)n}=1\}$。

对任何一组纯战略 $X, Y_1, Y_2, \cdots, Y_n$,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"信道容量"也是各不相同的。为了节省篇幅,我们不再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,从发信方 X 的角度来看,他将 n 个收信方分成 K 个组 F_1、F_2、…、F_K 使得每个收信方都在并只在某一个组中;而且,X 对于在同一个组中的不同收信方不加区别;对这 K 个组,发信方 X 还分配了一个权重系数 a_1、a_2、…、a_K,这里 $a_1+a_2+\cdots+a_K=1$,对每个 $1 \leqslant i \leqslant K, 0 \leqslant a_i \leqslant 1$。于是,发信方 X 的收益函数定义为

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

这里,F_i^C 表示除了 F_i 之外,所有其他收信方组成的集合,而 $I(X; F_i \mid F_i^C)$ 表示在条件 F_i^C 之下,X 与 F_i 之间的互信息。

其次,再来看 n 个收信方,假定他们自愿分成 M 个联盟 R_1、R_2、…、R_M 使得每个收信方都在且只在某一个联盟中;同一个联盟中的收信方都以本联盟利益为重(不考虑自己个人的利益。自私的收信方可以自己单独组成一个联盟),于是,对每个收信方 $i(1 \leqslant i \leqslant n)$,如果该收信方 $i \in R_j (1 \leqslant j \leqslant M)$,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收信方的利益函数都是相同的):

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

这里,R_j^C 表示除了 R_j 之外,所有其它收信方联盟组成的集合,而 $I(X; R_j \mid R_j^C)$ 表示在条件 R_j^C 之下,X 与 R_j 之间的互信息。

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,仿照定理 4 的证明过程,可以直接验证:定理 1 的条件被全部满足,即,该博弈存在纯战略的纳什均衡 X^*、Y_1^*、Y_2^*、…、Y_n^*。而达到纳什均衡状态时,收发各方的纯战略 X^*、Y_1^*、Y_2^*、…、Y_n^*,便是对应于各自企望的最佳结果,而这些可达的利益最大值所围成的区域,便是信道容量。

3.2　榆树网(Banyan)网络的信道容量

在榆树网中,有 n 个发信方 X_1、X_2、…、X_n 和 m 个收信方 Y_1、Y_2、…、Y_m。显然,榆树网是星形网的扩展,它把 1 个发(收)信方,扩展成多个。为了描述榆树网的信道容量,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(发信方 $X_i, 1 \leqslant i \leqslant n$)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 $n+i$(收信方 $Y_i, 1 \leqslant i \leqslant m$)的战略空间 T_i 定义为 $T_i=\{0 \leqslant y_{ji} \leqslant 1 : 1 \leqslant j \leqslant N(n+i),\ y_{1i}+y_{2i}+\cdots+y_{N(n+i)i}=1\}$。

n 个发信方自愿地将自己分为 Q 个联盟,P_1、P_2、…、P_Q 使得每个发信方都在且只在某一个联盟中;同一个联盟中的发信方都以本联盟利益为重(不考虑自己个人的利益。自私的发信方可以独自组成一个联盟)。进一步,联盟 P_i 将全部 m 个收信方分成 $M(i)$ 个组,$F_{i1}, F_{i2}, \cdots, F_{iM(i)}$ 使得每个收信方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 a_{1i}、a_{2i}、…、$a_{M(i)i}$,这里 $a_{1i}+a_{2i}+\cdots+a_{M(i)i}=1$,对每个 $1 \leqslant i \leqslant Q, 0 \leqslant a_{ik} \leqslant 1$。

于是,对每个发信方 $j, 1 \leqslant j \leqslant n$,如果该发信方属于联盟 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:

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

这里 P_i^C表示除联盟 P_i之外的所有发信方组成的集合;F_{ik}^C表示除分组 F_{ik}之外的所有收信方组成的集合;$I(P_i;F_{ik}\mid P_i^C,F_{ik}^C)$表示,在条件 P_i^C,F_{ik}^C之下,P_i与 F_{ik}之间的互信息。

收信方的利益函数,可以类似地定义。即,

m 个收信方自愿地将自己分为 W 个联盟,B_1、B_2、…、B_W使得每个收信方都在且只在某一个联盟中;同一个联盟中的收信方都以本联盟利益为重(不考虑自己个人的利益。自私的收信方可以独自形成一个联盟)。进一步,联盟 B_i将全部 n 个发信方分成 $D(i)$ 个组,$E_{i1},E_{i2},\cdots,E_{iD(i)}$使得每个发信方都属于且只属于某个组。并且,联盟 B_i还分配了一个权重系数 b_{1i}、b_{2i}、…、$b_{D(i)i}$,这里 $b_{1i}+b_{2i}+\cdots+b_{D(i)i}=1$,对每个 $1\leqslant i\leqslant W$,$0\leqslant b_{ik}\leqslant 1$。

于是,对每个收信方 j,$1\leqslant j\leqslant m$,如果该收信方属于联盟 B_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:

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

这里 B_i^C表示除联盟 B_i之外的所有收信方组成的集合;E_{ik}^C表示除分组 E_{ik}之外的所有发信方组成的集合;$I(B_i;E_{ik}\mid B_i^C,E_{ik}^C)$表示,在条件 B_i^C,E_{ik}^C之下,B_i与 E_{ik}之间的互信息。

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,仿照定理 4 的证明过程,可以直接验证:定理 1 的条件被全部满足,即,该博弈存在纯战略的纳什均衡 X_1^*、X_2^*、…、X_n^*、Y_1^*、Y_2^*、…、Y_m^*。而达到纳什均衡状态时,收发各方的纯战略 X_1^*、X_2^*、…、X_n^*、Y_1^*、Y_2^*、…、Y_m^*,便是对应于各自企望的最佳结果,而这些可达的利益最大值所围成的区域,便是信道容量。

3.3 全连通网络的信道容量

所谓 N 个用户的全连通网络,就是在该网络中,每个用户既是收信方,同时又是发信方。那么,如何来考虑这种网络中的信道容量呢? 其实,若利用上面的博弈思路,只要每个用户自己的目标锁定后,那么,由他们所构成的 N 个参与者的博弈,就一定存在纳什均衡,而且,他们各自的最大利益也能够在纳什均衡状态下被确定,而且,这些最大值所围成的区域,便是可达的信道容量。非常幸运的是:互信息函数及其线性组合的凹性,保证了纯战略纳什均衡的存在性。

为了避免过于复杂的公式足标体系,我们在全连通网络中假设:每个用户都是自私的,即,只考虑自己的利益,或者说,不再存在前面几小节中的联盟。这种假定当然会遗漏一些可能的情况,但是,对网络信息论的研究并没有实质性的影响。况且,在实际应用中,每个网络用户确实是几乎自考虑自身利益最大化。

设网络中的 N 个用户分别用随机变量 $X_1,X_2,\cdots,X_N$来表示,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(用户 X_i,$1\leqslant i\leqslant n$)的战略空间 S_i定义为 $S_i=\{0\leqslant x_{ji}\leqslant 1;1\leqslant j\leqslant M(i),\ x_{1i}+x_{2i}+\cdots+x_{M(i)i}=1\}$。

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:网络中的每个用户,对参与者 i 来说,其重要程度是不会完全相同的,因此,参与者 i 将其他 $N-1$ 个用户分成 $N(i)$ 组,$G_{i1},G_{i2},\cdots,G_{iN(i)}$,使得每个其他用户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:

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

这里 G_{ik}^C表示除分组 G_{ik}和参与者 i 之外的所有用户组成的集合;$I(X_i;G_{ik}\mid G_{ik}^C)$表示,在条件 G_{ik}^C之下,X_i与 G_{ik}之间的互信息。

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,仿照定理 4 的证明过程,可以直接验证:定理 1 的条件被全部满足,即,该博弈存在纯战略的纳什均衡 X_1^*、X_2^*、…、X_n^*。而达到纳什均衡状态时,各用户的纯战略 X_1^*、X_2^*、…、$X*_n$,便是对应于各自企望的最佳结果,而这些可达的利益最大值所围成的区域,便是信道容量。

4 结束语

“没有缺点”本身就是缺点!

你看,仙农在创立 1 对 1 通信的《信息论》时,非常巧妙地利用了转移矩阵来描述信道和互信息等重要概念,以至于后人在研究多用户网络信息论时,首先想到的就是“照猫画虎”,而且,还真的在“多输入单输出信道”中取得了重要成果,求出了(实际上只是部分求出了)所谓的“信道容量”。但遗憾的是,人们误入了歧途,数十年的停滞不前便是最有力的证明。

过去人们仿照仙农,用各种各样的转移概率来描述多用户网络系统,比如,在多接入单输出信道时,用

转移概率 $P(y \mid x_1,x_2,\cdots,x_m)$ 来描述;在广播信道时,用转移概率 $P(x_1,x_2,\cdots,x_m \mid y)$ 来描述;在中继信道时,用转移概率 $P(y,y_1 \mid x,x_1)$ 来描述等等。从表面上看来,这样的描述好像并没有问题,因为,确实仅仅通过 $P(y \mid x_1,x_2,\cdots,x_m)$ 是求不出 $P(x_1,x_2,\cdots,x_m \mid y)$ 的值,所以,有理由认为多输入信道和广播信道完全不同。但是,仔细分析后,便会发现,人们这样做,大有画蛇添足的味道。

因为,实际上,对任意一个 n 用户 $(Y_1,Y_2,\cdots,Y_n)$ 的网络通信系统,只要有足够多的收发信息样本,比如,足够长时间地从各用户终端连续记录下了随机变量 $(Y_1,Y_2,\cdots,Y_n)$ 的同时刻的比特串 $(y_{1i},y_{2i},\cdots,y_{ni})$,$i=1,2,\cdots$,那么,根据"频率趋于概率"的大数定律,便可以得到 n 维随机变量 $(Y_1,Y_2,\cdots,Y_n)$ 的全部概率分布,由此,便可以知道该 n 维随机变量的所有各种转移概率、所有随机分量的概率分布等等。

换句话说,无论是多输入信道 $P(y \mid x_1,x_2,\cdots,x_m)$ 也好,或者是广播信道 $P(x_1,x_2,\cdots,x_m \mid y)$ 也好,反正,只要根据各用户端足够多的传输信息比特,那么,联合概率分布 $P(y,x_1,x_2,\cdots,x_m)$ 就是已经,当然,转移概率 $P(y \mid x_1,x_2,\cdots,x_m)$ 和 $P(x_1,x_2,\cdots,x_m \mid y)$ 也可同时已知,那么,这时再去区分什么"多输入信道"或"广播信道"还有意义吗?

在多用户情形下,"用转移概率去描述信道"是行不通的,同样,想用一些直线去切割出"信道容量"也更行不通。此时的重点应该是说清楚每个用户的真正通信意图到底是什么,或者说,每个用户的优化目标是什么。否则,如果优化目标都不明确,哪可能有明确的结果呢?

如何才能把每个用户的通信意图,优化目标,说清楚呢?"权重"和"条件互信息"便是最直观的办法。对重要的通信对象,可以将其"权重"提高;对其他用户可以调低权重;对根本不关心的用户,可以将其权重设为0。而"条件互信息"则给出了从所关心的用户群那里,能够获得的信息数量。当然,与《信息论》最核心的仙农信道编码定理一样,本文的博弈论方法也只是给出了网络通信中,各用户达到自己企望值的最大可达目标值,并未给出如何达到这个目标,具体的逼近方法仍然是要由编码和译码专家们去挖掘。

仙农的《信息论》天生就是为 1 对 1 的通信系统设计的,不适合于多用户情形。

冯.诺伊曼的《博弈论》天生就是为多人博弈而设计的,1 对 1 博弈仅仅是其特例。

《安全通论》的攻防对抗思想,很偶然地把《信息论》和《博弈论》粘接起来了,于是,便可以用《博弈论》的多用户优势,去弥补《信息论》的多用户缺陷,从而,解决了网络信息论的基本问题:信道容量。这便是本文的奥妙所在。

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

[12] DrewFudenberg,Jean Tirole,博弈论[M]. 北京:中国人民大学出版社,2016.

[13] 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.