DOI:10.3969/j.issn.1009-6868.2016.03.011
网络出版地址:http://www.cnki.net/kcms/detail/34.1228.TN.20160427.0826.002.html

编者按:网络空间安全作为一项新的全球治理议程,已经成为世界关注的焦点、各国政府的战略目标之一,但人们对网络空间安全的研究,还缺乏全面系统的理论指导,针对该问题,我刊特转载自《科学网》一篇由北京邮电大学杨义先、钮心忻教授撰写的《安全通论》(原文网址:http://blog.sciencenet.cn/blog-453322-948089.html)。在该文章中,由随机变量X和Y,构造了另一个随机变量$Z=[2(1+X+Y)]\mathrm{mod}3$,巧妙地将石头剪刀布的游戏问题,转化成了信道容量问题,从而对安全通论中的攻防问题进行深入、形象地研究。

安全通论——攻防篇之“石头剪刀布”

The General Theory of Security: "Rock Scissors Paper" in Offensive and Defensive

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2016) 03-0049-003

摘要:给出了“石头剪刀布”的一种“白富美”新玩法。所谓“白”,即思路清清楚楚、明明白白;所谓“富”,即理论内涵非常丰富;所谓“美”,即结论绝对数学美。安全通论的魅力也在这里得到了幽默体现。

关键词:概率;信道;安全

Abstract: In this paper, “clear, rich and charming” can be well explained the “rock scissors paper” in offensive and defensive. “Clear” means the clear thinking, “rich” refers to the rich theory connotation, and “charming” represents the harmony and singularity of mathematics. Charm of the general theory of security is also humorously shown in this paper.

Key words: probability; channel; security

杨义先/YANG Yixian
钮心忻/NIU Xinxin
(北京邮电大学,北京 100876)
(Beijing University of Posts and Telecommunications, Beijing 100876, China)

- “攻防”是安全的核心,所以在建立安全通论的过程中,需要多花一些精力去深入研究攻防
- 石头剪刀布的游戏问题,可以转化成了信道容量问题
- 石头剪刀布游戏是一种“非盲对抗”

利用安全通论,我们只需一张纸、一支笔,就把石头剪刀布玩成“白富美”。所谓“白”,即思路清清楚楚、明明白白;所谓“富”,即理论内涵非常丰富;所谓“美”,即结论绝对数学美。

1 信道建模

设甲与乙玩石头剪刀布,他们可分别用随机变量X和Y来表示:当甲出拳为“剪刀”、“石头”、“布”时,分别记为$X=0$、$X=1$、$X=2$;当乙出拳为剪刀、石头、布时,分别记为$Y=0$、$Y=1$、$Y=2$。根据概率论中的“大数定律”,频率的极限趋于概率,所以甲乙双方的出拳习惯,可以用随机变量X和Y的概率分布表示为:

(1)$P_r(X=0)=p$,即甲出剪刀的概率;$P_r(X=1)=q$,即甲出石头的概率;$P_r(X=2)=1-p-q$,即甲出布的概率。这里$0<p, q, p+q<1$;

(2)$P_r(Y=0)=r$,即乙出剪刀的概率;$P_r(Y=1)=s$,即乙出石头的概率;$P_r(Y=2)=1-r-s$,即乙出布的概率。这里$0<r, s, r+s<1$。

同样,我们还可以统计出二维随机变量(X,Y)的联合分布概率为:

(1)$P_r(X=0,Y=0)=a$,即甲出剪刀,乙出剪刀的概率;$P_r(X=0,Y=1)=b$,即甲出剪刀,乙出石头的概率;$P_r(X=0,Y=2)=1-a-b$,即甲出剪刀,乙出布的概率。这里$0<a, b, a+b<1$。

(2)$P_r(X=1,Y=0)=e$,即甲出石头,乙出剪刀的概率;$P_r(X=1,Y=1)=f$,即甲出石头,乙出石头的概率;$P_r(X=1,Y=2)=1-e-f$,即甲出石头,乙出布的概率。这里$0<e, f, e+f<1$。

(3)$P_r(X=2,Y=0)=g$,即甲出布,乙出剪刀的概率;$P_r(X=2,Y=1)=h$,即甲出布,乙出石头的概率;$Pr(X=2,Y=2)=1-g-h$,即甲出布,乙出布的概率。这里$0<g, h, g+h<1$[1-2]。

由随机变量X和Y,构造另一个随机变量$Z=[2(1+X+Y)]\mathrm{mod}3$。由于任意两个随机变量都可构成一个通信信道,所以以X为输入,以Z为输出,

收稿时间:2016-03-22
网络出版时间:2016-04-27

我们就得到一个通信信道（X；Z），称之为“甲方信道”。

如果在某次游戏中甲方赢，那么就只可能有3种情况：

（1）甲出剪刀，乙出布，即X=0，Y=2，这也等价于X=0，Z=0，即甲方信道的输入等于输出；

（2）甲出石头，乙出剪刀，即X=1，Y=0，这也等价于X=1，Z=1，即甲方信道的输入等于输出；

（3）甲出布，乙出石头，即X=2，Y=1，这也等价于X=2，Z=2，即甲方信道的输入等于输出。

反过来，如果甲方信道将1 bit信息成功地从发端送到了收端，那么也只有3种可能的情况：

（1）输入和输出都等于0，即X=0，Z=0，这也等价于X=0，Y=2，即甲出剪刀，乙出布，即甲赢；

（2）输入和输出都等于1，即X=1，Z=1，这也等价于X=1，Y=0，即甲出石头，乙出剪刀，即甲赢；

（3）输入和输出都等于2，即X=2，Z=2，这也等价于X=2，Y=1，即甲出布，乙出石头，即甲赢。

综合以上正反两方面，共6种情况，就得到一个重要引理：

引理1：甲赢一次，就意味着甲方信道成功地把1 bit信息，从发端送到了收端；反之亦然。

再利用随机变量Y和Z构造一个信道（Y；Z），称之为“乙方信道”，它以Y为输入，以Z为输出。那么，仿照前面的论述，我们可得如下引理：

引理2：乙方赢一次，就意味着乙方信道成功地把1 bit信息，从发端送到了收端；反之亦然。

由此可见，甲乙双方玩石头剪刀布的输赢问题，就转化成了甲方信道和乙方信道能否成功地传输信息比特的问题。根据仙农第二定理[3]，我们知道：信道容量就等于该信道能够成功传输的信息比特数。所以，石头剪刀布的游戏问题，就转化成了信道容量问题[4]。

定理1（石头剪刀布定理）：如果剔除“平局”不考虑（即忽略甲乙双方都出相同手势的情况），那么则有：

（1）对甲方来说，对任意$k/n \leqslant C$，都一定有某种技巧（对应于仙农编码），使得在nC次游戏中，甲方能够胜乙方k次；如果在某m次游戏中，甲方已经胜出乙方u次，那么一定有$u \leqslant mC$。这里C是甲方信道的容量。

（2）针对乙方来说，对任意$k/n \leqslant D$，都一定有某种技巧（对应于仙农编码），使得在nD次游戏中，乙方能够胜甲方k次；如果在某m次游戏中，乙方已经胜出甲方u次，那么则有$u \leqslant mD$。这里D是乙方信道的容量。

（3）如果$C<D$，那么甲方会输；如果$C>D$，那么整体上甲方会赢；如果$C=D$，那么甲乙双方势均力敌。

下面我们就来分别计算甲方信道和乙方信道的信道容量。

（1）甲方信道（X；Z）的转移概率矩阵P，该矩阵为3X3阶，则有：

$P(0,0)=P_r(Z=0|X=0)=(1-a-b)/p$

$P(0,1)=P_r(Z=1|X=0)=b/p$

$P(0,2)=P_r(Z=2|X=0)=a/p$

$P(1,0)=P_r(Z=0|X=1)=f/q$

$P(1,1)=P_r(Z=1|X=1)=e/q$

$P(1,2)=P_r(Z=2|X=1)=(1-e-f)/q$

$P(2,0)=P_r(Z=0|X=2)=g/(1-p-q)$

$P(2,1)=P_r(Z=1|X=2)=(1-g-h)/(1-p-q)$

$P(2,2)=P_r(Z=2|X=2)=h/(1-p-q)$

使用信道转移概率矩阵P来计算信道容量，解方程组 $Pa=b$，其中a为列向量，则有：

$$a=(a_0,a_1,a_2)^T,$$

$$b=(\sum_{j=0}^{2}P(0,j)\log_2 P(0,j),\sum_{j=0}^{2}P(1,j)\log_2 P(1,j),\sum_{j=0}^{2}P(2,j)\log_2 P(2,j)) \quad (1)$$

我们可根据公式（1）来判断转移概率矩阵P。

（a）若P可逆，则此时有唯一解，即 $a=P^{-}b$，可计算 $C=\log_2(\sum_{j=0}^{2}2^{a_j})$

则有：

$$P_z(j)=2^{a_j-C}\ (j=0,1,2) \quad (2)$$

$$P_z(j)=\sum_{j=0}^{2}P_x(i)P(i,j)\ (i=0,1,2) \quad (3)$$

由公式（3）得到达到信道容量的X的概率分布，如果所有$P_x(i)$满足大于等于0，则可确认信道容量为C。

（b）若P不可逆，则方程有多组解，重复上述步骤，计算出多个C，按上述步骤分别计算各自的$P_x(i)$，通过判定是否满足大于等于0，舍去不满条件的解C。

（2）我们再来看乙方信道（Y；Z），首先它的转移概率矩阵Q，该矩阵为3X3阶，则有：

$Q(0,0)=P_r(Z=0|Y=0)=g/r$

$Q(0,1)=P_r(Z=1|Y=0)=e/r$

$Q(0,2)=P_r(Z=2|Y=0)=(r-g-e)/r$

$Q(1,0)=P_r(Z=0|Y=1)=f/s$

$Q(1,1)=P_r(Z=1|Y=1)=b/s$

$Q(1,2)=P_r(Z=2|Y=1)=(s-f-b)/s$

$Q(2,0)=P_r(Z=0|Y=2)=(1-a-b)/(1-r-s)$

$Q(2,1)=P_r(Z=1|Y=2)=(1-g-h)/(1-r-s)$

$Q(2,2)=P_r(Z=2|Y=2)=(1-e-f)/(1-r-s)$

我们使用信道转移概率矩阵Q来计算乙方信道容量，解方程组$Qw=u$，其中w，u为列向量，则有：

$$w=(w_0,w_1,w_2)^T$$

$$u=(\sum_{j=0}^{2}Q(0,j)\log_2 Q(0,j),\sum_{j=0}^{2}Q(1,j)\log_2 Q(1,j),\sum_{j=0}^{2}Q(2,j)\log_2 Q(2,j)) \quad (4)$$

我们可以根据公式（4）来判断转移概率矩阵Q。

（a）若Q可逆，则此时有唯一解，即 $w=Q^{-}u$，计算 $D=\log_2(\sum_{j=0}^{2}2^{w_j})$，则有

$$Q_z(j)=2^{w_j-D}\ (j=0,1,2)$$

$$Q_z(j)=\sum_{j=0}^{2}Q_y(i)Q(i,j)\ \ (i=0,1,2) \quad (5)$$

由公式（5）得到达到信道容量的X的概率分布，如果所有$Q_y(i)$满足大于等于0，则可确认信道容量为D。

（b）若Q不可逆则方程有多组解，重复上述步骤，计算出多个D，按上述步骤分别计算各自的$Q_y(i)$，通过判定是否满足大于等于0，舍去不满

条件的解 D。

2 巧胜策略

根据定理1，可知甲乙双方在石头剪刀布游戏中的胜负，其实已经事先就“天定”了，某方若想争取更大的胜利，那么他就必须努力“改变命运”。下面分几种情况来考虑：

（1）两个傻瓜之间的游戏。所谓两个傻瓜，意指甲乙双方都固守自己的习惯，无论过去的输赢情况怎样，他们都按既定习惯“出牌”。这时，从定理1，我们已经知道：如果 $C<D$，那么整体上甲方会输；如果 $C>D$，那么整体上甲方会赢；如果 $C=D$，那么甲乙双方势均力敌。

（2）一个傻瓜与一个智者之间的游戏。如果甲是傻瓜，他仍然坚持其固有的习惯出牌，那么双方对抗足够多的次数后，乙方就可以计算出对应于甲方的随机变量 X 的分布概率 p 和 q，以及相关的条件概率分布，并最终计算出甲方信道的信道容量；然后，再通过调整自己的习惯，增大自己的“乙方信道”的信道容量，从而使得后续的游戏对自己更有利，甚至使乙方信道的信道容量大于甲方信道的信道容量，最终使得自己稳操胜券。

（3）两个智者之间的游戏。如果甲和乙双方，都随时在总结对方的习惯，并对自己的出牌习惯做调整，即增大自己的信道容量。那么最终，甲乙双方的信道容量值将趋于相等，即他们之间的游戏竞争将趋于平衡，达到动态稳定的状态。

3 简化版

下面，我们再给出一个更抽象、更简捷的解决办法。

设甲与乙玩石头剪刀布，他们可分别用随机变量 X 和 Y 来表示：当甲出拳为剪刀、石头、布时，分别记为 $X=0$、$X=1$、$X=2$；当乙出拳为剪刀、石头、布时，分别记为 $Y=0$、$Y=1$、$Y=2$。根据概率论中的大数定律，频率的极限趋于概率，所以甲乙双方的出拳习惯，可以用随机变量 X 和 Y 的概率分布表示为：

$0<P_x(X=x)=p_x<1$，$x=0,1,2$，$p_0+p_1+p_2=1$

$0<P_y(Y=y)=q_y<1$，$y=0,1,2$，$q_0+q_1+q_2=1$

$0<P_t(X=x,Y=y)=t_{xy}<1$，$x,y=0,1,2$，$\sum_{0\le x,y\le 2}t_{xy}=1$

$p_x=\sum_{0\le y\le 2}t_{xy}$，$x=0,1,2$

$q_y=\sum_{0\le x\le 2}t_{xy}$，$y=0,1,2$

石头剪刀布游戏的输赢规则是：若 $X=x$，$Y=y$，那么甲（X）赢的充分必要条件是：$(y-x)\bmod 3=2$。

现在我们构造另一个随机变量 $F=(Y-2)\bmod 3$。考虑由 X 和 F 构成的信道（X；F），即以 X 为输入，以 F 为输出的信道。那么，就有如下事件等式：若在某个回合中，甲（X）赢了，那么，就有 $(Y-X)\bmod 3=2$，从而得出 $F=(Y-2)\bmod 3=[(2+X)-X]\bmod 3=X$，也就是说：信道（$X$；$F$）的输入（$X$）始终等于它的输出（$F$）。换句话说，1个比特就被成功地在该信道中被从发端传输到了收端。

反过来，如果1个比特就被成功地在该信道中被从发端传输到了收端，那么就意味着信道（X；F）的输入（X）始终等于它的输出（F），也就是说：$F=(Y-2)\bmod 3=X$，这刚好就是 X 赢的充分必要条件。

结合上述正反两个方面的论述，就有：甲（X）赢一次，就意味着信道（X；F）成功地把1 bit信息，从发端送到了收端；反之亦然。因此，信道（X；F）也可以扮演甲方信道的功能。

类似地，若记随机变量 $G=(X-2)\bmod 3$，那么信道（Y；G）就可以扮演乙方信道的角色。

而现在信道（X；F）和（Y；G）的信道容量形式会更简捷，分别是：

$$（X;F）的信道容量=\mathrm{Max}_X[I(X,F)]=\mathrm{Max}_X[I(X,(Y-2)\bmod 3)]=\mathrm{Max}_X[I(X,Y)]=\mathrm{Max}_X[\sum t_{xy}\log(t_{xy}/(p_xq_y))] \quad (6)$$

这里的最大值，是针对所有可能的 t_{xy} 和 p_x 而取的，所以它实际上是 q_0、q_1、q_2 的函数。

$$（Y;G）的信道容量=\mathrm{Max}_Y[I(Y,G)]=\mathrm{Max}_Y[I(Y,(X-2)\bmod 3)]=\mathrm{Max}_Y[I(X,Y)]=\mathrm{Max}_Y[\sum t_{xy}\log(t_{xy}/(p_xq_y))] \quad (7)$$

这里的最大值，是针对所有可能的 t_{xy} 和 q_y 而取的，所以它实际上是 p_0、p_1、p_2 的函数。

4 结束语

“攻防”是安全的核心，所以在建立安全通论的过程中，多花一些精力去深入研究攻防也是值得的。

文章研究的石头剪刀布游戏则是一种“非盲对抗”，但由于它的普及率极高（几千年来，全世界每个人在童年时代几乎都玩过），所以我们以单独一篇论文的形式来研究它。有关其他一些有代表性的非盲对抗，我们将在随后的文章中研究。

参考文献

[1] 杨义先, 钮心忻. 安全通论（1）之“经络篇”[EB/OL]. [2015-12-08] http://blog.sciencenet.cn/blog-453322-944217.html

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

[3] THOMAS M C, THOMAS J A. 信息论基础 [M]. 阮吉寿，张华，译. 北京：机械工业出版社出版，2007

[4] LIN S, DANIEL J C. 差错控制码 [M]. 北京：机械工程出版社，2007

作者简介

杨义先，灾备技术国家工程实验室主任，北京邮电大学教授、博士生导师，信息安全中心主任，首批长江学者特聘教授，首届国家杰出青年基金获得者，中国密码学会副理事长；目前研究方向为网络空间安全、现代密码学和纠错编码等；获得包括国家发明奖和省部级科技进步奖等在内的各类科技奖励20余项，授权发明专利4项，主持和参与多项国家“863”、国家自然科学基金、省部级等科研项目；发表高水平论文500余篇，出版专著及教材20多部。

钮心忻，北京邮电大学计算机学院教授、博士生导师；长期从事网络与信息安全、信号与信息处理等方面的研究工作。