文章编号：2096-1618(2016)03-0237-05
稿件来源：科学网
网　　址：http://blog.sciencenet.cn/blog-453322-950146.html
发表时间：2016-01-13

安全通论(5)

——攻防篇之“非盲对抗”及“劝酒令”

杨义先，　钮心忻
(北京邮电大学信息安全中心，北京 100876)

摘要：“非盲对抗”变化多端，很难“一招致胜”，只好“见招拆招”。不过，这倒增添了不少乐趣。你看，酒友们在宴会上玩的“划拳”和“猜拳”等劝酒令，也成了《安全通论》的严肃研究内容。仍然采用统一的“信道容量方法”，给出了醉鬼“赢酒杯数”和“罚酒杯数”的理论极限，还给出了醉鬼获胜的调整技巧。当然，这些内容也是《安全通论》不可或缺的组成部分。还针对所有“输赢规则线性可分”的“非盲对抗”，给出了统一的解决方案。

0　引言

以网络空间安全、经济安全、领土安全等为代表的所有安全问题的核心，就是“对抗”！所以，无论花多少篇幅，都必须把它研究透彻，至少是要尽可能透彻。那怕是多次变换角度，甚至利用古老游戏和时髦娱乐项目，来全面深入地研究安全对抗问题，都是值得的。

“安全经络”是《安全通论》的第一块基石，文献[1]已经打好了这块基石。

“安全对抗”是《安全通论》的第二块基石。“安全对抗”分为两大类：盲对抗、非盲对抗。为了打好这第二块基石，我们已经在文献[2]中，统一研究了“盲对抗”，并给出了黑客(红客)攻击(防守)能力的精确极限。针对“非盲对抗”，我们虽然已经找到了统一的研究方法(信道容量法)，但是，由于“非盲对抗”的模型千变万化，我们只好“见招拆招”。比如，分别在文献[3]和[4]中，以国际著名的“石头剪刀布游戏”、国内家喻户晓的“猜正反面游戏”和“手心手背游戏”为对象，研究了“非盲对抗”的3个有趣实例，给出了输赢极限和获胜技巧。本文则利用《安全通论》对酒桌上著名的两个实例(划拳、猜拳)进行分析，仍然采用统一的“信道容量方法”，给出了“赢酒杯数”和“罚酒杯数”的理论极限，还给出了醉鬼获胜的调整技巧。当然，这些内容也是《安全通论》不可或缺的组成部分。此外，针对“非盲对抗”的很大一个子类(输赢规则线性可分的情况)，我们给出了统一的解决方案。

1　“猜拳”赢酒

“猜拳”，在北京又称“棒打老虎”，是宴会上，主人和客人闹酒的法宝之一。其游戏规则是：在每个回合中，主人和客人同时独立亮出如下4种手势之一：虫子、公鸡、老虎、棒子。然后，双方共同根据如下“胜负判定规则”来决定该罚谁喝一杯酒：

“虫子”被“公鸡”吃掉；“公鸡”被“老虎”吃掉；“老虎”被“棒子”打死；“棒子”被“虫子”蛀断。

除此之外，主客双方就算平局，互不罚酒。

一个回合结束后，主客双方再进行下一回合的“猜拳”。

将此“猜拳游戏”用数学方式表示出来便是：设主人和客人分别用随机变量 X 和 Y 来表示，它们的可能取值有4个：0,1,2,3。具体地说：

当主人(或客人)亮出“虫子”时，记，$X=0$(或 $Y=0$)；

当主人(或客人)亮出“公鸡”时，记，$X=1$(或 $Y=1$)；

当主人(或客人)亮出“老虎”时，记，$X=2$(或 $Y=2$)；

当主人(或客人)亮出“棒子”时，记，$X=3$(或 $Y=3$)。

如果某回合中，主人亮出的是 x(即，$X=x$，$0\leqslant x\leqslant 3$)，而客人亮出的是 y(即，$Y=y$，$0\leqslant y\leqslant 3$)，那么，本回合，主人赢(即，罚客人一杯酒)的充分必要条件是：$(x-y)\bmod 4=1$；客人赢(即，罚主人一杯酒)的充分必要条件是：$(y-x)\bmod 4=1$；否则，本回合就算“平局”，即主客双方互不罚酒，接着进行下一回合的“斗酒”。

这个“猜拳”游戏显然是一种“非盲对抗”。主人和客人到底谁输，谁赢呢？最多会被罚多少杯酒呢？他们怎样才能让对方多喝，而自己少喝呢？下面就用《安全通论》的“信道容量法”，来回答这些问题。

由概率论中的大数定律，频率趋于概率，所以，根据“主人(X)”和“客人(Y)”的习惯，即，过去他们“斗酒”的统计规律(如果他们是初次见面，那么，不妨让

他们以“热身赛”方式,先“斗酒”一阵子,然后,记下他们的习惯就行了),就可以分别给出 X 和 Y 的概率分布,以及(X,Y)的联合概率分布:

$0<P_r(X=i)=p_i<1, i=0,1,2,3; p_0+p_1+p_2+p_3=1;$

$0<P_r(Y=i)=q_i<1, i=0,1,2,3; q_0+q_1+q_2+q_3=1;$

$0<P_r(X=i,Y=j)=t_{ij}<1, i, j=0,1,2,3; \sum_{0\leqslant i,j\leqslant 3}t_{ij}=1$。

$p_x=\sum_{0\leqslant y\leqslant 3}t_{xy}, x=0,1,2,3;$

$q_y\sum_{0\leqslant x\leqslant 3}t_{xy}, y=0,1,2,3$。

为了分析“主人”赢酒情况,我们构造一个随机变量 $Z=(Y+1)\bmod 4$。然后,再用随机变量 X 和 Z 构成一个信道$(X;Z)$,称它为“猜拳主人信道”,即,该信道以 X 为输入,以 Z 为输出。

下面来分析几个事件等式。如果某回合中,主人亮出的是 x(即,$X=x, 0\leqslant x\leqslant 3$),而客人亮出的是 y(即,$Y=y, 0\leqslant y\leqslant 3$),那么:

如果本回合“主人”赢,那么,就有$(x-y)\bmod 4=1$,即,$y=(x-1)\bmod 4$,于是,$z=(y+1)\bmod 4=[(x-1)+1]\bmod 4=x \bmod 4=x$,换句话说,此时,“猜拳主人信道”的输出 Z 始终等于输入 X,也就是说:一个“比特”被成功地从输入端 X,发送到了输出端 Z。

反过来,如果在“猜拳主人信道”中,一个“比特”被成功地从输入端 X,发送到了输出端 Z;那么,此时就该“输出 z 始终等于输入 x,即,$z=x$”,也就有:$(x-y)\bmod 4=(z-y)\bmod 4=[(y+1)-y]\bmod 4=1 \bmod 4=1$,于是,根据“猜拳”规则,就该判“主人赢”,即,客人罚酒一杯!

结合上述正反两种情况,我们便有:

引理 1 在“猜拳”游戏中,“主人赢一次”就等价于“1 个“比特”被成功地从“猜拳主人信道”(X,Z)的输入端,发送到了输出端”。

由引理 1,再结合仙农信息论的著名“信道编码定理”[5-6]:如果“猜拳主人信道”的容量为 C,那么,对于任意传输率 $k/n\leqslant C$,都可以在译码错误概率任意小的情况下,通过某个 n 比特长的码字,成功地把 k 个比特传输到收信端。反过来,如果“猜拳主人信道”能够用 n 长码字,把 S 个比特无误差地传输到收端,那么,一定有 $S\leqslant nC$。把这段话翻译一下,便有如下定理:

定理 1(猜拳主人赢酒定理) 设由随机变量$(X;Z)$组成的“猜拳主人信道”的信道容量为 C。那么,在剔除掉“平局”的情况后有:(1)如果主人想罚客人 k 杯酒,那么,他一定有某种技巧(对应于仙农编码),使得他能够在 k/C 个回合中,以任意接近 1 的概率达到目的。反过来,(2)如果主人在 n 回合中,赢了 S 次,即,罚了客人 S 杯酒,那么,一定有 $S\leqslant nC$。

由该“猜拳主人赢酒定理”可知,只要求出“猜拳主人信道”的信道容量 C,那么,主人“赢酒”的“杯数”极限就确定了。下面就来求信道容量 C。

首先,(X,Z)的联合概率分布为:

$P_r(X=i,Z=j)=P_r(X=i,(Y+1)\bmod 4=j)=P_r(X=i,Y=(j-1)\bmod 4)=t_{i(j-1)\bmod 4}, i,j=0,1,2,3,4$

所以,“猜拳主人信道”$(X;Z)$的信道容量就是:

$C=\mathrm{Max}[\mathrm{I}(X,Z)]=\mathrm{Max}\{\sum_{0\leqslant i,j\leqslant 3}[t_{i(j-1)\bmod 4}]\log[t_{i(j-1)\bmod 4}](p_iq_j)\}$

这里的最大值 Max 是针对满足如下条件的实数而取的:$0<\mathrm{p}_i, t_{ij}<1, i,j=0,1,2,3; p_0+p_1+p_2+p_3=1; \sum_{0\leqslant i,j\leqslant 3}t_{ij}=1; p_x=\sum_{0\leqslant y\leqslant 3}t_{xy}$。所以,这个 C 实际上是满足条件 $q_0+q_1+q_2+q_3=1$ 和 $0<q_i<1, i=0,1,2,3$ 的正实数变量的函数,即,可以记为 $C(q_0,q_1,q_2,q_3)$,其中,$q_0+q_1+q_2+q_3=1$。

同理,可以分析“客人赢酒”的情况,此处不再复述了。

可见,“主人”赢酒的多少($C(q_0,q_1,q_2,q_3)$),其实取决于“客人”的习惯(q_0,q_1,q_2,q_3)。如果主客双方都固守他们的习惯,那么,他们的输赢已经“天定”了;如果“主人”或“客人”中有一方见机行事(即,调整自己的习惯),那么,当他调整到其信道容量大过对方时,他就能够整体上赢;如果“主人”和“客人”双方都在调整自己的习惯,那么,他们最终将达到动态平衡。

2 “划拳”赢酒

“划拳”比“猜拳”更复杂,它也是宴会上,主人和客人闹酒的另一个法宝。

该游戏是这样的:在每个回合中,主人(A)和客人(B)各自同时独立地,在手上亮出 0 到 5,这 6 种手势之一;并在嘴上吼出 0 到 10,这 11 个数之一。也就是说,每个回合中,“主人 A”是一个 2 维随机变量,即,$A=(X,Y)$,其中,$0\leqslant X\leqslant 5$ 是“主人”手上显示的数,而 $0\leqslant Y\leqslant 10$ 是“主人”嘴上吼出的数。同样,“客人 B”也是一个 2 维随机变量,即,$B=(F,G)$,其中,$0\leqslant F\leqslant 5$ 是“客人”手上显示的数,而 $0\leqslant G\leqslant 10$ 是“客人”嘴上吼出的数。

如果在某个回合中,“主人”和“客人”的 2 维数分别是(x,y)和(f,g),那么,“划拳”游戏的罚酒规则是:

如果,$x+f=y$,那么,“主人”赢,罚“客人”喝一杯酒;

如果,$x+f=g$,那么,“客人”赢,罚“主人”喝一杯酒;

如果上述两种情况都不出现,那么,就算“平局”,主客双方互不罚酒,接着进行下一回合。仔细一点说:

双方嘴上吼的数一样(即,$g=y$)时,“平局”出现;双方虽然吼的数各不相同,但是,他们“手上显示的数之和”不等于“任何一方嘴上吼的数”时,“平局”也出现。

这个“划拳”游戏显然是一种“非盲对抗”。主人和客人到底会谁输,谁赢呢?最多会被罚多少杯酒呢?他们怎样才能让对方多喝,而自己少喝呢?下面就用《安全通论》的“信道容量法”,来回答这些问题。

由概率论中的大数定律,频率趋于概率,所以,根据“主人(A)”和“客人(B)”的习惯,即,过去他们“斗酒”的统计规律(如果他们是初次见面,那么,不妨让他们以“热身赛”的方式,先“斗酒”一阵子,然后,记下他们的习惯就行了),就可以分别给出 A 和 B 及其分量 X、Y、F、G 的概率分布,以及 4 个随机变量(X,Y,F,G)的联合概率分布:

“主人”手上显示 x 的概率:$0<P_r(X=x)=p_x<1$,$0\leqslant x\leqslant 5$;$x_0+x_1+x_2+x_3+x_4+x_5=1$;

“客人”手上显示 f 的概率:$0<P_r(F=f)=q_f<1$,$0\leqslant f\leqslant 5$;$f_0+f_1+f_2+f_3+f_4+f_5=1$;

“主人”嘴上吼 y 的概率:$0<P_r(Y=y)=r_y<1$,$0\leqslant y\leqslant 10$;$\sum_{0\leqslant y\leqslant 10}r_y=1$;

“客人”嘴上吼 g 的概率:$0<P_r(G=g)=s_g<1$,$0\leqslant g\leqslant 10$;$\sum_{0\leqslant g\leqslant 10}s_g=1$;

“主人”手上显示 x,嘴上吼 y 的概率:

$0<P_r[A=(x,y)]=P_r(X=x,Y=y)=b_{xy}<1$,$0\leqslant y\leqslant 10$,$0\leqslant x\leqslant 5$,$\sum_{0\leqslant y\leqslant 10,0\leqslant x\leqslant 5}b_{xy}=1$;

“客人”手上显示 f,嘴上吼 g 的概率:

$0<P_r[B=(f,g)]=P_r(F=f,G=g)=h_{fg}<1$,$0\leqslant g\leqslant 10$,$0\leqslant f\leqslant 5$,$\sum_{0\leqslant g\leqslant 10,0\leqslant f\leqslant 5}h_{fg}=1$;

“主人手上显示 x,嘴上吼 y;同时,客人手上显示 f,嘴上吼 g”的概率:

$0<P_r[A=(x,y),B=(f,g)]=P_r(X=x,Y=y,F=f,G=g)=t_{xyfg}<1$,这里,

$0\leqslant y,g\leqslant 10$,$0\leqslant x,f\leqslant 5$,$\sum_{0\leqslant y,g\leqslant 10,0\leqslant x,f\leqslant 5}t_{xyfg}=1$。

为了分析“主人”赢酒情况,我们构造一个 2 维随机变量

$$Z=(U,V)=(X\delta(G-Y),X+F),$$

这里的 δ 函数定义为:$\delta(0)=0$;$\delta(x)=1$,如果 $x\neq 0$。于是,

$P_r[Z=(u,v)]=\sum_{x+f=v,x\delta(g-y)=u}t_{xyfg}=:d_{uv}$,这里,$0\leqslant v\leqslant 10$,$0\leqslant u\leqslant 5$。

然后,再用随机变量 A 和 Z 构成一个信道(A;Z),称它为“划拳主人信道”,即,该信道以 A 为输入,以 Z 为输出。

下面来分析几个事件等式。如果某回合中,主人手上亮出的是 x(即,$X=x$,$0\leqslant x\leqslant 5$),主人嘴上吼的是 y(即,$Y=y$,$0\leqslant y\leqslant 10$);而客人手上亮出的是 f(即,$F=f$,$0\leqslant f\leqslant 5$),客人嘴上吼的是 g(即,$G=g$,$0\leqslant g\leqslant 10$)。那么,根据“划拳”的评判规则有:

如果本回合“主人”赢,那么,$x+f=y$ 同时 $y\neq g$。于是,$\delta(g-y)=1$,进一步就有:$Z=(u,v)=(x\delta(g-y),x+f)=(x,y)=A$,换句话说,此时,“划拳主人信道”的输出 Z 就始终等于输入 A,也就是说:一个“比特”被成功地从输入端 A,发送到了输出端 Z。

反过来,如果在“划拳主人信道”中,一个“比特”被成功地从输入端 A,发送到了输出端 Z;那么,此时就该“输出 $z=(u,v)=(x\delta(g-y),x+f)$ 始终等于输入 (x,y)”,也就有:$x\delta(g-y)=x$ 同时 $x+f=y$,即,$y\neq g$ 且 $x+f=y$,于是,根据“划拳”规则,就该判“主人赢”,即,客人罚酒一杯!

结合上述正反两种情况,我们便有:

引理 2　在“划拳”游戏中,“主人赢一次”就等价于“1 个“比特”被成功地从“划拳主人信道”(A;Z)的输入端,发送到了输出端”。

由引理 2,再结合仙农信息论的著名“信道编码定理”:如果“划拳主人信道”的容量为 D,那么,对于任意传输率 $k/n\leqslant D$,都可以在译码错误概率任意小的情况下,通过某个 n 比特长的码字,成功地把 k 个比特传输到收信端。反过来,如果“划拳主人信道”能够用 n 长码字,把 S 个比特无误差地传输到收端,那么,一定有 $S\leqslant nD$。把这段话翻译一下,便有如下定理:

定理 2(划拳主人赢酒定理)　设由随机变量(A;Z)组成的“划拳主人信道”的信道容量为 D。那么,在剔除掉“平局”的情况后有:(1)如果主人想罚客人 k 杯酒,那么,他一定有某种技巧(对应于仙农编码),使得他能够在 k/D 个回合中,以任意接近 1 的概率达到目的。反过来,(2)如果主人在 n 回合中,赢了 S 次,即,罚了客人 S 杯酒,那么,一定有 $S\leqslant nD$。

由该“划拳主人赢酒定理”可知,只要求出“划拳主人信道”的信道容量 D,那么,主人“赢酒”的“杯数”极限就确定了。下面就来求信道容量 D:

$$D=Max[I(A,Z)]$$

$$=\mathrm{Max}\{\sum_{a,z}P_r(a,z)\log[P_r(a,z)/[P_r(a)P_r(z)]]\}$$

$$=\mathrm{Max}\{\sum_{x,y,f,g}P_r(x,y,x\delta(g-y),x+f)\log[P_r(x,y,x\delta(g-y),x+f)/[P_r(x,y)P_r(x\delta(g-y),x+f)]]\}$$

$$=\mathrm{Max}\{\sum_{x,y,f,g}t_{x,y,x\delta(g-y),x+f}\log[t_{x,y,x\delta(g-y),x+f}/[b_{xy}d_{x\delta(g-y),x+f}]]\}$$

这里的最大值是针对满足如下条件的正实数而取的:

$0\leqslant y\leqslant 10$;$\sum_{0\leqslant y\leqslant 10}r_y=1$;

$0\leqslant y\leqslant 10, 0\leqslant x\leqslant 5, \sum_{0\leqslant y\leqslant 10, 0\leqslant x\leqslant 5} b_{xy}=1$;

$0\leqslant g\leqslant 10, 0\leqslant f\leqslant 5, \sum_{0\leqslant g\leqslant 10, 0\leqslant f\leqslant 5} h_{fg}=1$。

所以,实际上,“划拳主人信道”的容量 D 其实是满足条件 $0\leqslant f\leqslant 5; f_0+f_1+f_2+f_3+f_4+f_5=1; 0\leqslant g\leqslant 10; \sum_{0\leqslant g\leqslant 10} s_g=1$ 的 f_i, g_j 的函数,$0\leqslant i\leqslant 5, 0\leqslant j\leqslant 10$。

同理,可以分析“客人赢酒”的情况,此处不再复述了。

可见,“划拳主人”赢酒的多少($D(g_j, f_i)$),其实取决于“客人”的习惯(g_j, f_i)。如果主客双方都固守他们的习惯,那么,他们的输赢已经“天定”了;如果“主人”或“客人”中有一方见机行事(即,调整自己的习惯),那么,当他调整到其信道容量大过对方时,他就能够整体上赢;如果“主人”和“客人”双方都在调整自己的习惯,那么,他们最终将达到动态平衡。

3 线性可分“非盲对抗”的抽象模型

设黑客(X)共有 n 招来发动攻击,即,随机变量 X 的取值共有 n 个,不妨记为 $\{x_0, x_1, \cdots, x_{n-1}\}=\{0,1,2,\cdots,n-1\}$,这也是黑客的全部“武器库”。

设红客(Y)共有 m 招来抵抗攻击,即,随机变量 Y 的取值共有 m 个,不妨记为 $\{y_0, y_1, \cdots, y_{m-1}\}=\{0,1,2,\cdots,m-1\}$,这也是红客的全部“武器库”。

注意:在下面推导中,我们将根据需要在“招 x_i, y_j”和“数 i, j”之间等价地变换,即,$x_i=i, y_j=j$,其目的在于,既把问题说清楚,又在形式上简化。

在非盲对抗中,每个黑客武器 $x_i(j=0,1,\cdots,m-1)$ 和每个红客武器 $y_j(j=0,1,\cdots,m-1)$ 之间,存在着一个红黑双方公认的输赢规则,于是,一定存在 2 维数集 $\{(i,j), 0\leqslant i\leqslant n-1, 0\leqslant j\leqslant m-1\}$ 的某个子集 H,使得“x_i 胜 y_j”当且仅当 $(i,j)\in H$。如果这个子集 H 的结构比较简单,那么,我们就能够构造某个信道,使得“黑客赢一次”等价于“1 比特信息被成功地从该通信信道的发端传输到了收端”,然后,再利用著名的仙农信道编码定理就行了。比如:

在“石头剪刀布”游戏中,$H=\{(i,j): 0\leqslant i,j\leqslant 2, (j-i) \bmod 3=2\}$;

在“猜正反面”游戏中,$H=\{(i,j): 0\leqslant i=j\leqslant 1\}$;

在“手心手背”游戏中,$H=\{(i,j,k): 0\leqslant i\neq j=k\leqslant 1\}$;

在“猜拳”游戏中,$H=\{(i,j): 0\leqslant i,j\leqslant 3, (i-j) \bmod 4=1\}$;

在“划拳”游戏中,$H=\{(x,y,f,g): 0\leqslant x,f\leqslant 5; 0\leqslant g\neq y\leqslant 10; x+f=y\}$。

我们已经在文献[3-4]和本文中,针对以上各 H 构造出了相应的通信信道。但是,对一般的 H,却很难构造出这样的通信信道,不过,有一种特殊情况还是可以有所作为的,即,如果上面的集合 H,可以分解为 $H=\{(i,j): i=f(j), 0\leqslant i\leqslant n-1, 0\leqslant j\leqslant m-1\}$(即,$H$ 中第一个分量 j 是其第二个分量的某种函数),那么,我们就可以构造一个随机变量 $Z=f(Y)$。然后,考虑信道 $(X;Z)$,于是便有如下事件等式:

如果在某个回合中,黑客出击的招是 x_i,而红客应对的招是 y_j,那么:

如果“黑客赢”,那么,就有 $i=f(j)$,也就是说,所以,此时信道 $(X;Z)$ 的输出便是 $Z=f(y_j)=f(j)=i=x_i$,即,此时信道的输出与输入相同,即 1 个比特被成功地从信道 $(X;Z)$ 的输入端发送到了输出端。

反过来,如果“1 个比特被成功地从信道 $(X;Z)$ 的输入端发送到了输出端”,那么,此时就该有“输入=输出”,即“$i=f(j)$”,这也就意味着“黑客赢”。

结合上述正反两个方面,我们得到如下定理:

定理 3(线性非盲对抗极限定理) 在“非盲对抗”中,设黑客 X 共有 n 种攻击法 $\{x_0, x_1, \cdots x_{n-1}\}=\{0,1,2,\cdots,n-1\}$;设红客 Y 共有 m 种防御法 $\{y_0, y_1, \cdots y_{m-1}\}=\{0,1,2,\cdots,m-1\}$,又设红黑双方约定的输赢规则是:“$x_i$ 胜 y_j”当且仅当 $(i,j)\in H$。这里 H 是矩形集合 $\{(i,j), 0\leqslant i\leqslant n-1, 0\leqslant j\leqslant m-1\}$ 的某个子集。

如果 H 关于黑客 X 是线性的,即,H 可以表示为 $H=\{(i,j): i=f(j), 0\leqslant i\leqslant n-1, 0\leqslant j\leqslant m-1\}$(即,$H$ 中第一个分量 i 是其第二个分量 j 的某种函数 $f(.)$),那么,便可以构造一个信道 $(X;Z)$,其中 $Z=f(Y)$,使得:若 C 是信道 $(X;Z)$ 的信道容量,

(1)如果黑客想赢 k 次,那么,他一定有某种技巧(对应于仙农编码),使得他能够在 k/C 个回合中,以任意接近 1 的概率达到目的。

(2)如果黑客在 n 个回合中,赢了 S 次,那么,一定有 $S\leqslant nC$。

如果 H 关于红客 Y 是线性的,即,H 可以表示为 $H=\{(i,j): j=g(i), 0\leqslant i\leqslant n-1, 0\leqslant j\leqslant m-1\}$(即,$H$ 中第二个分量 j 是其第一个分量 i 的某种函数 $g(.)$),那么,便可以构造一个信道 $(Y;G)$,其中 $G=g(X)$,使得:若 D 是信道 $(Y;G)$ 的信道容量,那么有:

(1)如果红客想赢 k 次,那么,他一定有某种技巧(对应于仙农编码),使得他能够在 k/D 个回合中,以任意接近 1 的概率达到目的。

(2)如果红客在 n 个回合中,赢了 S 次,那么,一定有 $S\leqslant nD$。

4 结束语

“石头剪刀布”、“手心手背”、“猜正反面”、“猜

拳”和“划拳”等游戏,其实他们的输赢规则集 H 都是线性可分的,因此,它们全是本文定理 3(线性非盲对抗极限定理)的特例而已。至于 H 为不可分情况,相应的信道构造就无从下手了,这个问题就作为公开问题,留待今后解决吧。

为了加深大家的印象,我们对“盲对抗”和“非盲对抗”,再做一些形象的描述:

所谓“盲对抗”,就是在每个攻防回合后,攻防双方都只知道自己的“自评结果”,而对敌方的“他评结果”一无所知。像大国斗智、战场搏杀、网络攻防、谍报战等比较惨烈的对抗,通常都属于“盲对抗”。这里的“盲”,与是否面对面无关,比如,“两泼妇互相骂街”就是典型的,面对面的“盲对抗”,因为,“攻方”是否骂到了“守方”的痛处,只有“守方”自己才知道,而且,被骂者通常还要极力掩盖其痛处,不让“攻方”知道自己的弱点在哪。当然,“一群泼妇互相乱骂”,更是盲对抗了。

所谓“非盲对抗”,就是在每个攻防回合后,双方都知道本回合的,一致的“胜败结果”。比如,像古老的“石头剪刀布”游戏中,一旦双方的手势亮出后,本回合的胜败结果就一目了然:石头胜剪刀,剪刀胜布,布胜石头。像许多赌博游戏、体育竞技等项目都属于“非盲对抗”。家喻户晓的童趣游戏“猜正反面游戏”、“手心手背游戏”和本文中的“划拳”和“划拳”等,也都是“非盲对抗”,只不过,在“手心手背游戏”中彼此对抗的人,不再是两个,而是 3 个。

更加形象地说,“泼妇骂架”是“盲对抗”,但是,“两流氓打架”却是“非盲对抗”了。因为,人的身体结构都相似,被打的痛处在哪,谁都知道,而且结论也基本一致的,所以,“打架”是“非盲的”,当然,“打群架”也是“非盲对抗”。但是,人的心理结构却千差万别,被骂的痛点会完全不同,所以,“骂架”是“盲的”。

《安全通论》的第三篇(黑客篇),努力提示黑客的本质!

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” 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”,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”,http://blog. sciencenet. cn/blog-453322-949155. html,2016-01-09.

[5] 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.

[6] Shu Lin,Daniel J, Costello,Jr. 差错控制码[M]. 晏坚,何元智,潘亚汉,等译. 北京:机械工程出版社,2007.