Research Article

Games Based Study of Nonblind Confrontation

Yixian Yang,^{1,2,3} Xinxin Niu,^{1,2,3} and Haipeng Peng^{2,3}

¹Guizhou Provincial Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China

²Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

³National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China

Correspondence should be addressed to Haipeng Peng; penghaipeng@bupt.edu.cn

Received 4 January 2017; Accepted 20 March 2017; Published 19 April 2017

Academic Editor: Liu Yuhong

Copyright © 2017 Yixian Yang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Security confrontation is the second cornerstone of the General Theory of Security. And it can be divided into two categories: blind confrontation and nonblind confrontation between attackers and defenders. In this paper, we study the nonblind confrontation by some well-known games. We show the probability of winning and losing between the attackers and defenders from the perspective of channel capacity. We establish channel models and find that the attacker or the defender winning one time is equivalent to one bit transmitted successfully in the channel. This paper also gives unified solutions for all the nonblind confrontations.

1. Introduction

The core of all security issues represented by cyberspace security [1], economic security, and territorial security is confrontation. Network confrontation [2], especially in big data era [3], has been widely studied in the field of cyberspace security. There are two strategies in network confrontation: blind confrontation and nonblind confrontation. The so-called “blind confrontation” is the confrontation in which both the attacker and defender are only aware of their self-assessment results and know nothing about the enemy’s assessment results after each round of confrontation. The superpower rivalry, battlefield fight, network attack and defense, espionage war, and other brutal confrontations, usually belong to the blind confrontation. The so-called “nonblind confrontation” is the confrontation in which both the attacker and defender know the consistent result after each round. The games studied in this paper are all belonging to the nonblind confrontation.

“Security meridian” is the first cornerstone of the General Theory of Security which has been well established [4, 5]. Security confrontation is the second cornerstone of the General Theory of Security, where we have studied the blind confrontation and gave the precise limitation of hacker attack

ability (hacker defense ability) [4, 5]. Comparing with the blind confrontation, the winning or losing rules of nonblind confrontation are more complex and not easy to study. In this paper, based on the Shannon Information Theory [6], we study several well-known games of the nonblind confrontation: “rock-paper-scissors” [7], “coin tossing” [8], “palm or back,” “draw boxing,” and “finger guessing” [9], from a novel point of view. The famous game, “rock-paper-scissors,” has been played for thousands of years. However, there are few related analyses on it. The interdisciplinary team of Zhejiang University, Chinese Academy of Sciences, and other institutions, in cooperation with more than three hundred volunteers, spent four years playing “rock-paper-scissors” and giving corresponding analysis of game. And the findings were awarded as “Best of 2014: MIT technology review.”

We obtain some significant results. The contributions of this paper are as follows:

- (i) Channel models of all the above three games are established.
- (ii) The conclusion that the attacker or the defender winning one time is equivalent to one bit transmitted successfully in the channel is found.

- (iii) Unified solutions for all the nonblind confrontations are given.

The rest of the paper is organized as follows. The model of rock-paper-scissors is introduced in Section 2, models of coin tossing and palm or back are introduced in Section 3, models of finger guessing and drawing boxing are introduced in Section 4, unified model of linear separable nonblind confrontation is introduced in Section 5, and Section 6 concludes this paper.

2. Model of Rock-Paper-Scissors

2.1. Channel Modeling. Suppose A and B play “rock-paper-scissors,” whose states can be, respectively, represented by random variables X and Y :

$X = 0$, $X = 1$, and $X = 2$ denote the “scissors,” “rock,” and “paper” of A , respectively;

$Y = 0$, $Y = 1$, and $Y = 2$ denote the “scissors,” “rock,” and “paper” of B , respectively.

Law of Large Numbers indicates that the limit of the frequency tends to probability; thus the choice habits of A and B can be represented as the probability distribution of random variables X and Y :

$\Pr(X = 0) = p$ means the probability of A for “scissors”;

$\Pr(X = 1) = q$ means the probability of A for “rock”;

$\Pr(X = 2) = 1 - p - q$ means the probability of A for “paper”, where $0 < p, q$ and $p + q < 1$;

$\Pr(Y = 0) = r$ means the probability of B for “scissors”;

$\Pr(Y = 1) = s$ means the probability of B for “rock”;

$\Pr(Y = 2) = 1 - r - s$ means the probability of B for “paper”, where $0 < r, s$ and $r + s < 1$.

Similarly, the joint probability distribution of two-dimensional random variables (X, Y) can be listed as follows:

$\Pr(X = 0, Y = 0) = a$ means the probability of A for “scissors” and B for “scissors”;

$\Pr(X = 0, Y = 1) = b$ means the probability of A for “scissors” and B for “rock”;

$\Pr(X = 0, Y = 2) = p - a - b$ means the probability of A for “scissors” and B for “paper”, where $0 < a, b$, and $a + b < p$;

$\Pr(X = 1, Y = 0) = e$ means the probability of A for “rock” and B for “scissors”;

$\Pr(X = 1, Y = 1) = f$ means the probability of A for “rock” and B for “rock”;

$\Pr(X = 1, Y = 2) = q - e - f$ means the probability of A for “rock” and B for “paper”, where $0 < e, f$, and $e + f < q$;

$\Pr(X = 2, Y = 0) = g$ means the probability of A for “paper” and B for “scissors”;

$\Pr(X = 2, Y = 1) = h$ means the probability of A for “paper” and B for “rock”;

$\Pr(X = 2, Y = 2) = 1 - p - q - g - h$ means the probability of A for “paper” and B for “paper”, where $0 < e, f$, and $e + f < 1 - p - q$.

Construct another random variable $Z = [2(1 + X + Y)] \bmod 3$ from X and Y . Because any two random variables can form a communication channel, we get a communication channel $(X; Z)$ with X as the input and Z as the output, which is called “Channel A,” which is shown in Figure 1.

FIGURE 1: Block diagram of the channel model.

If A wins, then there are only three cases.

Case 1. “ A chooses scissors, B chooses paper”; namely, “ $X = 0$, $Y = 2$.” This is also equivalent to “ $X = 0$, $Z = 0$ ”; namely, the input of “Channel A” is equal to the output.

Case 2. “ A chooses stone, B chooses scissors”; namely, “ $X = 1$, $Y = 0$.” This is also equivalent to “ $X = 1$, $Z = 1$ ”; namely, the input of “Channel A” is equal to the output.

Case 3. “ A chooses cloth, B chooses stone”; namely, “ $X = 2$, $Y = 1$.” This is also equivalent to “ $X = 2$, $Z = 2$ ”; namely, the input of “Channel A” is equal to the output.

In contrast, if “Channel A” sends one bit from the sender to the receiver successfully, then there are only three possible cases.

Case 1. The input and the output equal 0; namely, “ $X = 0$, $Z = 0$.” This is also equivalent to “ $X = 0$, $Y = 2$ ”; namely, “ A chooses scissors, B chooses paper”; A wins.

Case 2. The input and the output equal 1; namely, “ $X = 1$, $Z = 1$.” This is also equivalent to “ $X = 1$, $Y = 0$ ”; namely, “ A chooses rock, B chooses scissors”; A wins.

Case 3. The input and the output equal 2; namely, “ $X = 2$, $Z = 2$.” This is also equivalent to “ $X = 2$, $Y = 1$ ”; namely, “ A chooses paper, B chooses rock”; A wins.

Based on the above six cases, we get an important lemma.

Lemma 1. *A wins once if and only if “Channel A” sends one bit from the sender to the receiver successfully.*

Now we can construct another channel $(Y; Z)$ by using random variables Y and Z with Y as the input and Z as the output, which is called “Channel B.” Then similarly, we can get the following lemma.

Lemma 2. *B wins once if and only if “Channel B” sends one bit from the sender to the receiver successfully.*

Thus, the winning and losing problem of “rock-paper-scissors” played by A and B converts to the problem of whether the information bits can be transmitted successfully by “Channel A” and “Channel B.” According to Shannon’s second theorem [3], we know that channel capacity is equal to the maximal number of bits that the channel can transmit

successfully. Therefore, the problem is transformed into the channel capacity problem. More accurately, we have the following theorem.

Theorem 3 (“rock-paper-scissors” theorem). *If one does not consider the case that both A and B have the same state; then*

- (1) *for A, there must be some skills (corresponding to the Shannon coding) for any $k/n \leq C$, such that A wins k times in nC rounds of the game; if A wins u times in m rounds of the game, then $u \leq mC$, where C is the capacity of “Channel A”;*
- (2) *for B, there must be some skills (corresponding to the Shannon coding) for any $k/n \leq D$, such that B wins k times in nD rounds of the game; if B wins u times in m rounds of the game, then $u \leq mD$, where D is the capacity of “Channel B”;*
- (3) *statistically, if $C < D$, B will win; if $C > D$, A will win; if $C = D$, A and B are evenly matched.*

Here, we calculate the channel capacity of “Channel A” and “Channel B” as follows.

For channel $(X; Z)$ of A: P denotes its transition probability matrix with 3×3 order,

$$\begin{aligned}
 P(0, 0) &= \Pr(Z = 0 | X = 0) = \frac{(p - a - b)}{p}, \\
 P(0, 1) &= \Pr(Z = 1 | X = 0) = \frac{b}{p}, \\
 P(0, 2) &= \Pr(Z = 2 | X = 0) = \frac{a}{p}, \\
 P(1, 0) &= \Pr(Z = 0 | X = 1) = \frac{f}{q}, \\
 P(1, 1) &= \Pr(Z = 1 | X = 1) = \frac{e}{q}, \\
 P(1, 2) &= \Pr(Z = 2 | X = 1) = \frac{(q - e - f)}{q}, \\
 P(2, 0) &= \Pr(Z = 0 | X = 2) = \frac{g}{(1 - p - q)}, \\
 P(2, 1) &= \Pr(Z = 1 | X = 2) = \frac{(1 - p - q - g - h)}{(1 - p - q)}, \\
 P(2, 2) &= \Pr(Z = 2 | X = 2) = \frac{h}{(1 - p - q)}.
 \end{aligned} \tag{1}$$

The channel transfer probability matrix is used to calculate the channel capacity: solve the equations $Pm = n$, where m is the column vector:

$$\begin{aligned}
 m &= (m_0, m_1, m_2)^T, \\
 n &= \left(\sum_{j=0}^2 P(0, j) \log_2 P(0, j), \sum_{j=0}^2 P(1, j) \log_2 P(1, j), \right. \\
 &\quad \left. \sum_{j=0}^2 P(2, j) \log_2 P(2, j) \right).
 \end{aligned} \tag{2}$$

Consider the transition probability matrix P .

(1) If P is reversible, there is a unique solution; that is, $m = P^{-1}n$; then $C = \log_2(\sum_{j=0}^2 2^{m_j})$.

According to the formula $P_z(j) = 2^{m_j - C}$, $P_z(j) = \sum_{i=0}^2 P_x(i)P(i, j)$, $i, j = 0, 1, 2$, where $P_z(j)$ is the probability distribution of Z .

And the probability distribution of X is obtained. If $P_X(i) \geq 0$, $i = 0, 1, 2$, the channel capacity can be confirmed as C .

(2) If P is irreversible, the equation has multiple solutions. Repeat the above steps; then we can get multiple C and the corresponding $P_X(i)$. If $P_X(i)$ does not satisfy $P_X(i) \geq 0$, $i = 0, 1, 2$, we delete the corresponding C .

For channel $(Y; Z)$ of B: Q denotes its transition probability matrix with 3×3 order,

$$\begin{aligned}
 Q(0, 0) &= \Pr(Z = 0 | Y = 0) = \frac{g}{r}, \\
 Q(0, 1) &= \Pr(Z = 1 | Y = 0) = \frac{e}{r}, \\
 Q(0, 2) &= \Pr(Z = 2 | Y = 0) = \frac{(r - g - e)}{r}, \\
 Q(1, 0) &= \Pr(Z = 0 | Y = 1) = \frac{f}{s}, \\
 Q(1, 1) &= \Pr(Z = 1 | Y = 1) = \frac{b}{s}, \\
 Q(1, 2) &= \Pr(Z = 2 | Y = 1) = \frac{(s - f - b)}{s}, \\
 Q(2, 0) &= \Pr(Z = 0 | Y = 2) = \frac{(1 - a - b)}{(1 - r - s)}, \\
 Q(2, 1) &= \Pr(Z = 1 | Y = 2) = \frac{(1 - g - h)}{(1 - r - s)}, \\
 Q(2, 2) &= \Pr(Z = 2 | Y = 2) = \frac{(1 - e - f)}{(1 - r - s)}.
 \end{aligned} \tag{3}$$

The channel transfer probability matrix Q is used to calculate the channel capacity B .

Solution equation group $Qw = u$, where w, u are the column vector:

$$\begin{aligned}
 w &= (w_0, w_1, w_2)^T, \\
 u &= \left(\sum_{j=0}^2 Q(0, j) \log_2 Q(0, j), \sum_{j=0}^2 Q(1, j) \log_2 Q(1, j), \right. \\
 &\quad \left. \sum_{j=0}^2 Q(2, j) \log_2 Q(2, j) \right).
 \end{aligned} \tag{4}$$

Consider the transition probability matrix Q .

(1) If Q is reversible, there is a unique solution; that is, $w = Q^{-1}u$; then $D = \log_2(\sum_{j=0}^2 2^{w_j})$.

According to the formula $Q_z(j) = 2^{w_j - D}$, $Q_z(j) = \sum_{i=0}^2 Q_y(i)Q(i, j)$, $i, j = 0, 1, 2$.

And the probability distribution of Y is obtained. If $Q_Y(i) \geq 0$, $i = 0, 1, 2$, the channel capacity can be confirmed as D .

(2) If Q is irreversible, the equation has multiple solutions. Repeat the above steps, then we can get multiple D and the corresponding $Q_Y(i)$. If $Q_Y(i)$ does not satisfy $Q_Y(i) \geq 0$, $i = 0, 1, 2$, we delete the corresponding D .

In the above analysis, the problem of “rock-paper-scissors” game has been solved perfectly, but the corresponding analysis is complex. Here, we give a more abstract and simple solution.

Law of Large Numbers indicates that the limit of the frequency tends to probability; thus the choice habits of A and B can be represented as the probability distribution of random variables X and Y :

$$\begin{aligned} 0 < \Pr(X = x) = p_x < 1, \\ x = 0, 1, 2, \quad p_0 + p_1 + p_2 = 1; \\ 0 < \Pr(Y = y) = q_y < 1, \\ y = 0, 1, 2, \quad q_0 + q_1 + q_2 = 1; \\ 0 < \Pr(X = x, Y = y) = t_{xy} < 1, \\ x, y = 0, 1, 2, \quad \sum_{0 \leq x, y \leq 2} t_{xy} = 1; \end{aligned} \quad (5)$$

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

$$q_y = \sum_{0 \leq x \leq 2} t_{xy}, \quad y = 0, 1, 2.$$

The winning and losing rule of the game is if $X = x$, $Y = y$, then the necessary and sufficient condition of the winning of $A(X)$ is $(y - x) \bmod 3 = 2$.

Now construct another random variable $F = (Y - 2) \bmod 3$. Considering a channel $(X; F)$ consisting of X and F , that is, a channel with X as an input and F as an output, then, there are the following event equations.

If $A(X)$ wins in a certain round, then $(Y - X) \bmod 3 = 2$, so $F = (Y - 2) \bmod 3 = [(2 + X) - X] \bmod 3 = X$. That is, the input (X) of the channel $(X; F)$ always equals its output (F). In other words, one bit is successfully transmitted from the sender to the receiver in the channel.

Conversely, if “one bit is successfully transmitted from the sender to the receiver in the channel,” it means that the input (X) of the channel $(X; F)$ always equals its output (F). That is, $F = (Y - 2) \bmod 3 = X$, which is exactly the necessary and sufficient conditions for X winning.

Based on the above discussions, $A(X)$ winning once means that the channel $(X; F)$ sends one bit from the sender to the receiver successfully and vice versa. Therefore, the channel $(X; F)$ can also play the role of “Channel A ” in the third section.

Similarly, if the random variable $G = (X - 2) \bmod 3$, then the channel $(Y; G)$ can play the role of the above “Channel B .”

And now the form of channel capacity for channel $(X; F)$ and channel $(Y; G)$ will be simpler. We have

$C(X; F) = \max_X [I(X, F)] = \max_X [I(X, (Y - 2) \bmod 3)] = \max_X [I(X, Y)] = \max_X [\sum t_{xy} \log(t_{xy}/(p_x q_y))]$. The maximal value here is taken for all possible t_{xy} and p_x . So, $C(X; F)$ is actually the function of q_0, q_1 , and q_2 .

Similarly, $C(Y; G) = \max_Y [I(Y, G)] = \max_Y [I(Y, (X - 2) \bmod 3)] = \max_Y [I(X, Y)] = \max_Y [\sum t_{xy} \log(t_{xy}/(p_x q_y))]$. The maximal value here is taken for all possible t_{xy} and q_y . So, $C(Y; G)$ is actually the function of p_0, p_1 , and p_2 .

2.2. The Strategy of Win. According to Theorem 3, if the probability of a specific action is determined, the victory of both parties in the “rock-paper-scissors” game is determined as well. In order to obtain the victory with higher probability, one must adjust his strategy.

2.2.1. The Game between Two Fools. The so-called “two fools” means that A and B entrench their habits; that is, they choose their actions in accordance with the established habits no matter who won in the past. According to Theorem 3, statistically, if $C < D$, A will lose; if $C > D$, then A will win; and if $C = D$, then both parties are well-matched in strength.

2.2.2. The Game between a Fool and a Sage. If A is a fool, he still insists on his inherent habit; then after confronting a sufficient number of times, B can calculate the distribution probabilities p and q of random variable X corresponding to A . And B can get the channel capacity of A by some related conditional probability distribution at last, and then by adjusting their own habits (i.e., the probability distribution of the random variable Y and the corresponding conditional probability distribution, etc.); then B enlarges his own channel capacity to make the rest of game more beneficial to himself; moreover, the channel capacity of B is larger enough, $C(B) > C(A)$; then B win the success at last.

2.2.3. The Game between Two Sages. If both A and B get used to summarizing the habits of each other at any time, and adjust their habits, enlarge their channel capacity. At last, the two parties can get the equal value of channel capacities; that is, the competition between them will tend to a balance, a dynamically stable state.

3. Models of “Coin Tossing” and “Palm or Back”

3.1. The Channel Capacity of “Coin Tossing” Game. “Coin tossing” game: “banker” covers a coin under his hand on the table, and “player” guesses the head or tail of the coin. The “player” will win when he guesses correctly.

Obviously, this game is a kind of “nonblind confrontation.” We will use the method of channel capacity to analyze the winning or losing of the game.

Based on the Law of Large Numbers in the probability theory, the frequency tends to probability. Thus, according to the habits of “banker” and “player,” that is, the statistical regularities of their actions in the past, we can give the probability distribution of their actions.

We use the random variable X to denote the state of the “banker.” $X = 0$ ($X = 1$) means the coin is head (tail). So the habit of “banker” can be described by the probability distribution of X ; that is, $\Pr(X = 0) = p$, $\Pr(X = 1) = 1 - p$, where $0 \leq p \leq 1$.

We use the random variable Y to denote the state of the “player.” $Y = 0$ ($Y = 1$) means that he guesses head (tail).

So the habit of “player” can be described by the probability distribution of Y ; that is, $\Pr(Y = 0) = q$, $\Pr(Y = 1) = 1 - q$, where $0 \leq q \leq 1$. Similarly, according to the past states of “banker” and “player,” we have the joint probability distribution of random variables (X, Y) ; namely,

$$\begin{aligned}\Pr(X = 0, Y = 0) &= a; \\ \Pr(X = 0, Y = 1) &= b; \\ \Pr(X = 1, Y = 0) &= c; \\ \Pr(X = 1, Y = 1) &= d,\end{aligned}\tag{6}$$

where $0 \leq p, q, a, b, c, d \leq 1$ and

$$\begin{aligned}a + b + c + d &= 1; \\ p &= \Pr(X = 0) \\ &= \Pr(X = 0, Y = 0) + \Pr(X = 0, Y = 1) \\ &= a + b; \\ q &= \Pr(Y = 0) \\ &= \Pr(X = 0, Y = 0) + \Pr(X = 1, Y = 0) \\ &= a + c.\end{aligned}\tag{7}$$

Taking X as the input and Y as the output, we obtain the channel $(X; Y)$ which is called “Channel X ” in this paper.

Because Y guesses correctly = $\{X = 0, Y = 0\} \cup \{X = 1, Y = 1\}$ = one bit is successfully transmitted from the sender X to the receiver Y in “Channel X ,” “ Y wins one time” is equivalent to transmitting one bit of information successfully in “Channel X .”

Based on the channel coding theorem of Shannon’s Information Theory, if the capacity of “Channel X ” is C , for any transmission rate $k/n \leq C$, we can receive k bits successfully by sending n bits with an arbitrarily small probability of decoding error. Conversely, if “Channel X ” can transmit s bits to the receiver by sending n bits without error, there must be $S \leq nC$. In a word, we have the following theorem.

Theorem 4 (banker theorem). *Suppose that the channel capacity of “Channel X ” composed of the random variable $(X; Y)$ is C . Then one has the following: (1) if Y wants to win k times, he must have a certain skill (corresponding to the Shannon coding) to achieve the goal by any probability close to 1 in the k/C rounds; conversely, (2) if Y wins S times in n rounds, there must be $S \leq nC$.*

According to Theorem 3, we only need to figure out the channel capacity C of “Channel X ”; then the limitation of times that “ Y wins” is determined. So we can calculate the transition probability matrix $A = [A(i, j)]$, $i, j = 0, 1$ of “Channel X ”:

$$\begin{aligned}A(0, 0) &= \Pr(Y = 0 | X = 0) = \frac{\Pr(Y = 0, X = 0)}{\Pr(X = 0)} \\ &= \frac{a}{p};\end{aligned}$$

$$\begin{aligned}A(0, 1) &= \Pr(Y = 1 | X = 0) = \frac{\Pr(Y = 1, X = 0)}{\Pr(X = 0)} \\ &= \frac{b}{p} = 1 - \frac{a}{p};\end{aligned}$$

$$\begin{aligned}A(1, 0) &= \Pr(Y = 0 | X = 1) = \frac{\Pr(Y = 0, X = 1)}{\Pr(X = 1)} \\ &= \frac{c}{(1-p)} = \frac{(q-a)}{(1-p)};\end{aligned}$$

$$\begin{aligned}A(1, 1) &= \Pr(Y = 1 | X = 1) = \frac{\Pr(Y = 1, X = 1)}{\Pr(X = 1)} \\ &= \frac{d}{(1-p)} = 1 - \frac{(q-a)}{(1-p)}.\end{aligned}\tag{8}$$

Thus, the mutual information $I(X, Y)$ of X and Y equals

$$\begin{aligned}I(X, Y) &= \sum_X \sum_Y p(X, Y) \log \left(\frac{p(X, Y)}{[p(X)p(Y)]} \right) \\ &= a \log \left[\frac{a}{(pq)} \right] + b \log \left[\frac{b}{[p(1-q)]} \right] \\ &\quad + c \log \left[\frac{c}{[(1-p)q]} \right] \\ &\quad + d \log \left[\frac{d}{[(1-p)(1-q)]} \right] \\ &= a \log \left[\frac{a}{(pq)} \right] + (p-a) \log \left[\frac{(p-a)}{[p(1-q)]} \right] \\ &\quad + (q-a) \log \left[\frac{(q-a)}{[(1-p)q]} \right] \\ &\quad + (1+a-p-q) \log \left[\frac{(1+a-p-q)}{[(1-p)(1-q)]} \right].\end{aligned}\tag{9}$$

Thus, the channel capacity C of “Channel X ” is equal to $\max[I(X, Y)]$ (the maximal value here is taken from all possible binary random variables X). In a word, $C = \max[I(X, Y)]$ $0 < a, p < 1$ (where $I(X, Y)$ is the mutual information above). Thus, the channel capacity C of “Channel X ” is a function of q , which is defined as $C(q)$.

Suppose the random variable $Z = (X + 1) \bmod 2$. Taking Y as the input and Z as the output, we obtain the channel $(Y; Z)$ which is called “Channel Y ” in this paper.

Because $\{X \text{ wins}\} = \{Y = 0, X = 1\} \cup \{Y = 1, X = 0\} = \{Y = 0, Z = 0\} \cup \{Y = 1, Z = 1\} = \{\text{one bit is successfully transmitted from the sender } Y \text{ to the receiver } Z \text{ in the “Channel } Y\}\}$, “ X wins one time” is equivalent to transmitting one bit of information successfully in “Channel Y .”

Based on the Channel coding theorem of Shannon’s Information Theory, if the capacity of “Channel Y ” is D , for any transmission rate $k/n \leq D$, we can receive k bits successfully by sending n bits with an arbitrarily small probability of

decoding error. Conversely, if “Channel Y” can transmit s bits to the receiver by sending n bits without error, there must be $S \leq nD$. In a word, we have the following theorem.

Theorem 5 (player theorem). *Suppose that the channel capacity of “Channel Y” composed of the random variable $(Y; Z)$ is D . Then one has the following: (1) if X wants to win k times, he must have a certain skill (corresponding to the Shannon coding) to achieve the goal by any probability close to 1 in the k/C rounds; conversely, (2) if X wins S times in the n rounds, there must be $S \leq nD$.*

According to Theorem 4, we can determine the winning limitation of X as long as we know the channel capacity D of “Channel Y.”

Similarly, we can get the channel capacity $D = \max [I(Y, Z)]$, $0 < a, q < 1$, of “Channel Y.” Thus, the channel capacity D of “Channel Y” is a function of p , which is denoted as $D(p)$.

$$\begin{aligned} I(Y, Z) &= \sum_Y \sum_Z p(Y, Z) \log \left(\frac{p(Y, Z)}{[p(Y) p(Z)]} \right) \\ &= a \log \left[\frac{a}{(pq)} \right] + (p-a) \log \left[\frac{(p-a)}{[p(1-q)]} \right] \\ &\quad + (q-a) \log \left[\frac{(q-a)}{[(1-p)q]} \right] \\ &\quad + (1+a-p-q) \log \left[\frac{(1+a-p-q)}{[(1-p)(1-q)]} \right]. \end{aligned} \quad (10)$$

From Theorems 3 and 4, we can obtain the quantitative results of “the statistical results of winning and losing” and “the game skills of banker and player.”

Theorem 6 (strength theorem). *In the game of “coin tossing,” if the channel capacities of “Channel X” and “Channel Y” are $C(q)$ and $D(p)$, respectively, one has the following.*

Case 1. If both X and Y do not try to adjust their habits in the process of game, that is, p and q are constant, statistically, if $C(q) > D(p)$, Y will win; if $C(q) < D(p)$, X will win; and if $C(q) = D(p)$, the final result of the game is a “draw.”

Case 2. If X implicitly adjusts his habit and Y does not, that is, change the probability distribution p of the random variable X to enlarge the $D(p)$ of “Channel Y” such that $D(p) > C(p)$, statistically, X will win. On the contrary, if Y implicitly adjusts his habit and X does not, that is, $D(p) < C(p)$, Y will win.

Case 3. If both X and Y continuously adjust their habits and make $C(q)$ and $D(p)$ grow simultaneously, they will achieve a dynamic balance when $p = q = 0.5$, and there is no winner or loser in this case.

3.2. The Channel Capacity of “Palm or Back” Game. The “palm or back” game: three participants (A , B , and C) choose their actions of “palm” or “back” at the same time; if one of the participants choose the opposite action to the others (e.g., the

others choose “palm” when he chooses “back”), he will win this round.

Obviously, this game is also a kind of “nonblind confrontation.” We will use the method of channel capacity to analyze the winning or losing of the game.

Based on the Law of Large Numbers in the probability theory, the frequency tends to probability. Thus, according to the habits of A , B , and C , that is, the statistical regularities of their actions in the past, we have the probability distribution of their actions.

We use the random variable X to denote the state of A . $X = 0$ ($Y = 1$) means that he chooses “palm (back).” Thus, the habit of A can be described as the probability distribution of X ; that is, $\Pr(X = 0) = p$, $\Pr(X = 1) = 1 - p$, where $0 \leq p \leq 1$.

We use random variable Y to denote the state of B . $Y = 0$ ($Y = 1$) means that he chooses “palm (back).” Thus, the habit of B can be described as the probability distribution of Y , that is, $\Pr(Y = 0) = q$, $\Pr(Y = 1) = 1 - q$, where $0 \leq q \leq 1$.

We use the random variable Z to denote the state of C . $Z = 0$ ($Z = 1$) means that he chooses “palm (back).” Thus, the habit of C can be described as the probability distribution of Z ; that is, $\Pr(Z = 0) = r$, $\Pr(Z = 1) = 1 - r$, where $0 \leq r \leq 1$.

Similarly, according to the Law of Large Numbers, we can obtain the joint probability distributions of the random variables (X, Y, Z) from the records of their game results after some rounds; namely,

$$\begin{aligned} &\Pr(A \text{ for palm}, B \text{ for palm}, C \text{ for palm}) \\ &= \Pr(X = 0, Y = 0, Z = 0) = a; \\ &\Pr(A \text{ for palm}, B \text{ for palm}, C \text{ for back}) \\ &= \Pr(X = 0, Y = 0, Z = 1) = b; \\ &\Pr(A \text{ for palm}, B \text{ for back}, C \text{ for palm}) \\ &= \Pr(X = 0, Y = 1, Z = 0) = c; \\ &\Pr(A \text{ for palm}, B \text{ for back}, C \text{ for back}) \\ &= \Pr(X = 0, Y = 1, Z = 1) = d; \\ &\Pr(A \text{ for back}, B \text{ for palm}, C \text{ for palm}) \\ &= \Pr(X = 1, Y = 0, Z = 0) = e; \\ &\Pr(A \text{ for back}, B \text{ for palm}, C \text{ for back}) \\ &= \Pr(X = 1, Y = 0, Z = 1) = f; \\ &\Pr(A \text{ for back}, B \text{ for back}, C \text{ for palm}) \\ &= \Pr(X = 1, Y = 1, Z = 0) = g; \\ &\Pr(A \text{ for back}, B \text{ for back}, C \text{ for back}) \\ &= \Pr(X = 1, Y = 1, Z = 1) = h, \end{aligned} \quad (11)$$

where $0 \leq p, q, r, a, b, c, d, e, f, g, h \leq 1$ and

$$\begin{aligned} &a + b + c + d + e + f + g + h = 1; \\ &p = \Pr(A \text{ for palm}) = \Pr(X = 0) = a + b + c + d; \\ &q = \Pr(B \text{ for palm}) = \Pr(Y = 0) = a + b + e + f; \\ &r = \Pr(C \text{ for palm}) = \Pr(Z = 0) = a + c + e + g. \end{aligned} \quad (12)$$

Suppose the random variable $M = (X + Y + Z) \bmod 2$; then the probability distribution of M is

$$\begin{aligned}
 \Pr(M = 0) &= \Pr(X = 0, Y = 0, Z = 0) \\
 &\quad + \Pr(X = 0, Y = 1, Z = 1) \\
 &\quad + \Pr(X = 1, Y = 1, Z = 0) \\
 &\quad + \Pr(X = 1, Y = 0, Z = 1) \\
 &= a + d + g + f, \\
 \Pr(M = 1) &= \Pr(X = 0, Y = 0, Z = 1) \\
 &\quad + \Pr(X = 0, Y = 1, Z = 0) \\
 &\quad + \Pr(X = 1, Y = 0, Z = 0) \\
 &\quad + \Pr(X = 1, Y = 1, Z = 1) \\
 &= b + c + e + h.
 \end{aligned} \tag{13}$$

Taking X as the input and M as the output, we obtain the channel $(X; M)$ which is called “Channel A” in this paper.

After removing the situations in which three participants choose the same actions, we have the following equation:

$\{A \text{ wins}\} = \{A \text{ for palm}, B \text{ for back}, C \text{ for back}\} \cup \{A \text{ for back}, B \text{ for palm}, C \text{ for palm}\} = \{X = 0, Y = 1, Z = 1\} \cup \{X = 1, Y = 0, Z = 0\} = \{X = 0, M = 0\} \cup \{X = 1, M = 1\} = \{\text{one bit is successfully transmitted from the sender } (X) \text{ to the receiver } (M) \text{ in the “Channel A”}\}.$

Conversely, after removing the situations that three participants choose the same actions, if $\{\text{one bit is successfully transmitted from sender } (X) \text{ to the receiver } (M) \text{ in the “Channel A”}\}$, there is $\{X = 0, M = 0\} \cup \{X = 1, M = 1\} = \{X = 0, Y = 1, Z = 1\} \cup \{X = 1, Y = 0, Z = 0\} = \{A \text{ for palm}, B \text{ for back}, C \text{ for back}\} \cup \{A \text{ for back}, B \text{ for palm}, C \text{ for palm}\} = \{A \text{ wins}\}$. Thus, “A wins one time” is equivalent to transmitting one bit successfully from the sender X to the receiver M in the “Channel A.” From the channel coding theorem of Shannon’s Information Theory, if the capacity of the “Channel A” is E , for any transmission rate $k/n \leq E$, we can receive k bits successfully by sending n bits with an arbitrarily small probability of decoding error. Conversely, if the “Channel A” can transmit s bits to the receiver by sending n bits without error, there must be $S \leq nE$. In a word, we have the following theorem.

Theorem 7. Suppose that the channel capacity of the “Channel A” composed of the random variable $(X; M)$ is E . Then, after removing the situations in which three participants choose the same actions, one has the following: (1) if A wants to win k times, he must have a certain skill (corresponding to the Shannon coding theory) to achieve the goal by any probability close to 1 in the k/E rounds; conversely, (2) if A wins S times in the n rounds, there must be $S \leq nE$.

In order to calculate the channel capacity of the channel $(X; M)$, we should first calculate the joint probability distribution of the random variable (X, M) :

$$\begin{aligned}
 \Pr(X = 0, M = 0) &= \Pr(X = 0, Y = 0, Z = 0) \\
 &\quad + \Pr(X = 0, Y = 1, Z = 1) \\
 &= a + d;
 \end{aligned}$$

$$\begin{aligned}
 \Pr(X = 0, M = 1) &= \Pr(X = 0, Y = 1, Z = 0) \\
 &\quad + \Pr(X = 0, Y = 0, Z = 1) \\
 &= c + b;
 \end{aligned}$$

$$\begin{aligned}
 \Pr(X = 1, M = 0) &= \Pr(X = 1, Y = 1, Z = 0) \\
 &\quad + \Pr(X = 1, Y = 0, Z = 1) \\
 &= g + f;
 \end{aligned}$$

$$\begin{aligned}
 \Pr(X = 1, M = 1) &= \Pr(X = 1, Y = 0, Z = 0) \\
 &\quad + \Pr(X = 1, Y = 1, Z = 1) \\
 &= e + h.
 \end{aligned}$$

(14)

Therefore, the mutual information between X and M equals

$$\begin{aligned}
 I(X, M) &= (a + d) \log \left[\frac{(a + d)}{[p(a + d + g + f)]} \right] \\
 &\quad + (g + f) \log \left[\frac{(g + f)}{[(1 - p)(a + d + g + f)]} \right] \\
 &\quad + (c + b) \log \left[\frac{(c + b)}{[p(b + c + e + h)]} \right] + (e + h) \\
 &\quad \cdot \log \left[\frac{(e + h)}{[(1 - p)(b + c + e + h)]} \right] = (a + d) \\
 &\quad \cdot \log \left[\frac{(a + d)}{[p(a + d + g + f)]} \right] + (g + f) \\
 &\quad \cdot \log \left[\frac{(g + f)}{[(1 - p)(a + d + g + f)]} \right] + (p - a - d) \\
 &\quad \cdot \log \left[\frac{(p - a - d)}{[p(1 - (a + d + f + g))]} \right] \\
 &\quad + (1 - (p + f + g)) \\
 &\quad \cdot \log \left[\frac{(1 - (p + f + g))}{[(1 - p)(1 - (a + d + f + g))]} \right].
 \end{aligned} \tag{15}$$

Thus, the channel capacity of “channel A” is equal to $E = \max[I(X, M)]$ and it is a function of q and r , which is defined as $E(q, r)$.

Taking Y as the input and M as the output, we obtain the channel (Y, M) which is called “Channel B.” Similarly, we have the following.

Theorem 8. Suppose that the channel capacity of the “Channel B” composed of the random variable $(Y; M)$ is F . Then, after removing the situation in which the three participants choose the same action, one has the following: (1) if B wants to win k times, he must have a certain skill (corresponding to the Shannon coding) to achieve the goal by any probability close

to 1 in the k/F rounds; conversely, (2) if B wins S times in the n rounds, there must be $S \leq nF$.

The channel capacity F can be calculated as the same way of calculating E . Here, the capacity of "Channel B " is a function of p and r , which can be defined as $F(p, r)$.

Similarly, taking Z as the input and M as the output, we obtain the channel (Z, M) which is called "Channel C ." So we have the following.

Theorem 9. Suppose that the channel capacity of the "Channel C " composed of the random variable $(Z; M)$ is G . Then, after removing the situations in which three participants choose the same actions, one has the following: (1) if C wants to win k times, he must have a certain skill (corresponding to the Shannon coding theory) to achieve the goal by any probability close to 1 in the k/F rounds; conversely, (2) if C wins S times in the n rounds, there must be $S \leq nG$.

The channel capacity G can be calculated by the same way of calculating E . Now the capacity of "Channel C " is a function of p and q , which can be defined as $G(p, q)$.

From Theorems 6, 7, and 8, we can qualitatively describe the winning or losing situations of A , B , and C in the palm or back game.

Theorem 10. If the channel capacities of "Channel A ," "Channel B ," and "Channel C " are E , F , and G , respectively, the statistical results of winning or losing depend on the values of E , F , and G . The one who has the largest channel capacity will gain the priority. We can know that the three channel capacities cannot be adjusted only by one participant individually. It is difficult to change the final results by adjusting one's habit (namely, only change one of the p , q , and r separately), unless two of them cooperate secretly.

4. Models of "Finger Guessing" and "Draw Boxing"

4.1. Model of "Finger Guessing." "Finger guessing" is a game between the host and guest in the banquet. The rules of the game are the following. The host and the guest, respectively, choose one of the following four gestures at the same time in a round: bug, rooster, tiger, and stick. Then they decide the winner by the following regulations: "Bug" is inferior to "rooster"; "rooster" is inferior to "tiger"; "tiger" is inferior to "stick"; and "stick" is inferior to "bug". Beyond that, the game is ended in a draw and nobody will be punished.

The "host A " and "guest B " will play the "finger guessing game" again after the complete end of this round. The mathematical expression of "finger guessing game" is as follows: suppose A and B are denoted by random variables X and Y , respectively; there are 4 possible values of them. Specifically,

- $X = 0$ (or $Y = 0$) when A (or B) shows "bug";
- $X = 1$ (or $Y = 1$) when A (or B) shows "cock";
- $X = 2$ (or $Y = 2$) when A (or B) shows "tiger";
- $X = 3$ (or $Y = 3$) when A (or B) shows "stick".

If A shows x (namely, $X = x$, $0 \leq x \leq 3$) and B shows y (namely, $Y = y$, $0 \leq y \leq 3$) in a round, the necessary and

sufficient condition of A wins in this round is $(x - y) \bmod 4 = 1$. The necessary and sufficient condition of B wins in this round is $(y - x) \bmod 4 = 1$. Otherwise, this round ends in a draw and proceeds to the next round of the game.

Obviously, the "finger guessing" game is a kind of "non-blind confrontation." Who is the winner and how many times the winner wins? How can they make themselves win more? We will use the "channel capacity method" of the "General Theory of Security" to answer these questions.

Based on the Law of Large Numbers in the probability theory, the frequency tends to probability. Thus, according to the habits of "host (X)" and "guest (Y)," that is, the statistical regularities of their actions in the past (if they meet for the first time, we can require them to play a "warm-up game" and record their habits), we can give the probability distribution of X , Y and the joint probability distribution of (X, Y) , respectively:

$$\begin{aligned} 0 < \Pr(X = i) &= p_i < 1, \\ i &= 0, 1, 2, 3; \quad p_0 + p_1 + p_2 + p_3 = 1; \\ 0 < \Pr(Y = i) &= q_i < 1, \\ i &= 0, 1, 2, 3; \quad q_0 + q_1 + q_2 + q_3 = 1; \\ 0 < \Pr(X = i, Y = j) &= t_{ij} < 1, \\ i, j &= 0, 1, 2, 3; \quad \sum_{0 \leq i, j \leq 3} t_{ij} = 1. \end{aligned} \quad (16)$$

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

$$q_y = \sum_{0 \leq x \leq 3} t_{xy}, \quad y = 0, 1, 2, 3.$$

In order to analyze the winning situation of A , we construct a random variable $Z = (Y + 1) \bmod 4$. Then we use the random variables X and Z to form a channel $(X; Z)$, which is called "channel A "; namely, the channel takes X as the input and Z as the output. Then we analyze some equations of the events. If A shows x (namely, $X = x$, $0 \leq x \leq 3$) and B shows y (namely, $Y = y$, $0 \leq y \leq 3$) in a round, one has the following.

If A wins in this round, there is $(x - y) \bmod 4 = 1$; that is, $y = (x - 1) \bmod 4$, so we have $z = (y + 1) \bmod 4 = [(x - 1) + 1] \bmod 4 = x \bmod 4 = x$. In other words, the output Z is always equal to the input X in the channel A at this time. That is, a "bit" is successfully transmitted from the input X to its output Z .

In contrast, if a "bit" is successfully transmitted from the input X to the output Z in the "channel A ," "the output z is always equal to its input x ; namely, $z = x$ " is true at this time. Then there is $(x - y) \bmod 4 = (z - y) \bmod 4 = [(y + 1) - y] \bmod 4 = 1 \bmod 4 = 1$. Hence, we can judge that "A wins" according to the rules of this game.

Combining with the situations above, one has the following.

Lemma 11. In the "finger guessing" game, "A wins one time" is equivalent to "a 'bit' is successfully transmitted from the input to its output in the 'channel A .'" Combine Lemma 1 with the "channel coding theorem" of Shannon's Information Theory; if the capacity of the "channel A " is C , for any transmission rate $k/n \leq C$, we can receive k bits successfully by sending n bits with

an arbitrarily small probability of decoding error. Conversely, if the “channel A” can transmit s bits to the receiver by sending n bits without error, there must be $S \leq nC$. In a word, we have the following theorem.

Theorem 12. Suppose that the channel capacity of the “channel A” composed of the random variable $(X; Z)$ is C . Then after removing the situation of “draw,” one has the following: (1) if A wants to win k times, he must have a certain skill (corresponding to the Shannon coding) to achieve the goal by any probability close to 1 in the k/C rounds; conversely, (2) if A wins S times in the n rounds, there must be $S \leq nC$.

According to Theorem 12, we only need to figure out the channel capacity C of the “channel A,” then the limitation of the times of “A wins” is determined. So we can calculate the channel capacity C : first, the joint probability distribution of (X, Z) is $\Pr(X = i, Z = j) = \Pr(X = i, (Y + 1) \bmod 4 = j) = \Pr(X = i, Y = (j - 1) \bmod 4) = t_{i(j-1) \bmod 4}$, $i, j = 0, 1, 2, 3, 4$.

Therefore, the channel capacity of the channel $A(X; Z)$ is

$$C = \max [I(X, Z)] \\ = \max \left\{ \sum_{0 \leq i, j \leq 3} [t_{i(j-1) \bmod 4}] \frac{\log [t_{i(j-1) \bmod 4}]}{(p_i q_j)} \right\}. \quad (17)$$

The max in the equation is the maximal value taken from the real numbers which satisfy the following conditions: $0 < p_i$, $t_{ij} < 1$, $i, j = 0, 1, 2, 3$; $p_0 + p_1 + p_2 + p_3 = 1$; $\sum_{0 \leq i, j \leq 3} t_{ij} = 1$; $p_x = \sum_{0 \leq y \leq 3} t_{xy}$. Thus, the capacity C is actually the function of the positive real variables which satisfy the following conditions $q_0 + q_1 + q_2 + q_3 = 1$ and $0 < q_i < 1$, $i = 0, 1, 2, 3$; namely, it can be written as $C(q_0, q_1, q_2, q_3)$, where $q_0 + q_1 + q_2 + q_3 = 1$.

Similarly, we can analyze the situation of “B wins.” We can see that the times of “A wins” ($C(q_0, q_1, q_2, q_3)$) depend on the habit of $B(q_0, q_1, q_2, q_3)$. If both A and B stick to their habits, their winning or losing situation is determined; if either A or B adjusts his habit, he can win statistically when his channel capacity is larger; if both A and B adjust their habits, their situations will eventually reach a dynamic balance.

4.2. Model of “Draw Boxing.” “Draw boxing” is more complicated than “finger guessing,” and it is also a game between the host and guest in the banquet. The rule of the game is that the host (A) and the guest (B) independently show one of the six gestures from 0 to 5 and shout one of eleven numbers from 0 to 10. That is, in each round, “host A” is a two-dimensional random variable $A = (X, Y)$, where $0 \leq X \leq 5$ is the gesture showed by the “host” and $0 \leq Y \leq 10$ is the number shouted by him. Similarly, “guest B” is also a two-dimensional random variable $B = (F, G)$, where $0 \leq F \leq 5$ is the gesture showed by the “guest” and $0 \leq G \leq 10$ is the number shouted by him. If A and B are denoted by (x, y) and (f, g) in a certain round, respectively, the rules of the “draw boxing” game are

If $x + f = y$, A wins;

If $x + f = g$, B wins.

If the above two cases do not occur, the result of this round is a “draw,” and A and B continue the next round. Specifically, when the numbers shouted by both sides are the same

(namely, $g = y$), the result of this round is a “draw.” However, the numbers shouted by both sides are different and the gestures showed by them are not equal to “the number shouted by any side”; the result of this round also comes to a “draw.”

Obviously, the “draw boxing” game is a kind of “nonblind confrontation.” Who is the winner and how many times the winner wins? How can they make themselves win more? We will use the channel capacity method of the “General Theory of Security” to answer these questions.

Based on the Law of Large Numbers in the probability theory, the frequency tends to probability. Thus, according to the habits of “host (A)” and “guest (B),” that is the statistical regularities of their actions in the past (if they meet for the first time, we can require them to play a “warm-up game” and record their habits), we can give the probability distribution of A, B and their components X, Y, F, and G, and the joint probability distribution of (X, Y, F, G) , respectively.

The probability of “A shows x ”:

$$0 < \Pr(X = x) = p_x < 1, 0 \leq x \leq 5; x_0 + x_1 + x_2 + x_3 + x_4 + x_5 = 1;$$

The probability of “B shows f ”:

$$0 < \Pr(F = f) = q_f < 1, 0 \leq f \leq 5; f_0 + f_1 + f_2 + f_3 + f_4 + f_5 = 1;$$

The probability of “A shouts y ”:

$$0 < \Pr(Y = y) = r_y < 1, 0 \leq y \leq 10; \sum_{0 \leq y \leq 10} r_y = 1;$$

The probability of “B shouts g ”:

$$0 < \Pr(G = g) = s_g < 1, 0 \leq g \leq 10; \sum_{0 \leq g \leq 10} s_g = 1;$$

The probability of “A shows x and shouts y ”:

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

The probability of “B shows f and shouts g ”:

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

The probability of “A shows x and shouts y ” and “B shows f and shouts g ” at the same time:

$$0 < \Pr[A = (x, y), B = (f, g)] = \Pr(X = x, Y = y, F = f, G = g) = t_{xyfg} < 1, \text{ where } 0 \leq y, g \leq 10, \\ 0 \leq x, f \leq 5, \sum_{0 \leq y, g \leq 10, 0 \leq x, f \leq 5} t_{xyfg} = 1.$$

In order to analyze the situation of A wins, we construct a two-dimensional random variable

$$Z = (U, V) = (X\delta(G - Y), X + F). \quad (18)$$

The function δ is defined as $\delta(0) = 0$; $\delta(x) = 1$ when $x \neq 0$. Therefore,

$$\Pr[Z = (u, v)] = \sum_{x+f=v, x\delta(g-y)=u} t_{xyfg} =: d_{uv}, \quad (19) \\ \text{where } 0 \leq v \leq 10, 0 \leq u \leq 5.$$

Then, we use the random variables A and Z to form a channel $(A; Z)$, which is called “channel A” and takes A as the input and Z as the output.

Then we analyze some equations. In a certain round, A shows x (i.e., $X = x$, $0 \leq x \leq 5$) and shouts y (i.e., $Y = y$, $0 \leq y \leq 10$); meanwhile, B shows f (i.e., $F = f$, $0 \leq f \leq 5$) and

shouts g (i.e., $G = g, 0 \leq g \leq 10$). According to the evaluation rules, we have the following: if A wins in this around, we have $x + f = y$ and $y \neq g$. Thus, $\delta(g - y) = 1$ and $Z = (u, v) = (x\delta(g - y), x + f) = (x, y) = A$. In other words, the output Z of the “channel A ” is always equal to its input A at this time; that is to say, a “bit” is sent successfully from the input A to its output Z .

In contrast, if one bit is successfully sent from the input A to the output Z in the “channel A ,” “the output $z = (u, v) = (x\delta(g - y)x + f)$ ” is always equal to the “input (x, y) ” at this time; also there is $x\delta(g - y) = x$ when $x + f = y$; that is, $y \neq g$ and $x + f = y$. Thus, A wins this round according to the evaluation rules.

Combining with the cases above, we have the following.

Lemma 13. *In a “draw boxing” game, “A wins one time” is equivalent to one bit is successfully sent from the input of “channel A ” to its output.*

Combining Lemma 13 with the “channel coding theorem” of Shannon’s Information Theory, if the capacity of the “channel A ” is D , for any transmission rate $k/n \leq D$, we can receive k bits successfully by sending n bits with an arbitrarily small probability of decoding error. Conversely, if the “channel A ” can transmit s bits to the receiver by sending n bits without error, there must be $S \leq nD$. In a word, we have the following theorem.

Theorem 14. *Suppose that the channel capacity of the “channel A ” composed of the random variable $(A; Z)$ is D . Then after removing the situation of “draw,” one has the following: (1) if A wants to win k times, he must have a certain skill (corresponding to the Shannon coding) to achieve the goal by any probability close to 1 in the k/D rounds; conversely, (2) if A wins S times in the n rounds, there must be $S \leq nD$.*

According to Theorem 4, we only need to figure out the channel capacity D of the “channel A ”; then the limitation of times that “ A wins” is determined. So we can calculate the channel capacity D :

$$\begin{aligned}
 D &= \max [I(A, Z)] = \max \left\{ \sum_{a,z} \Pr(a, z) \right. \\
 &\quad \cdot \log \left[\frac{\Pr(a, z)}{[\Pr(a) \Pr(z)]} \right] \Bigg\} \\
 &= \max \left\{ \sum_{x,y,f,g} \Pr(x, y, x\delta(g - y), x + f) \right. \\
 &\quad \cdot \log \left[\frac{\Pr(x, y, x\delta(g - y), x + f)}{[\Pr(x, y) \Pr(x\delta(g - y), x + f)]} \right] \Bigg\} \quad (20) \\
 &= \max \left\{ \sum_{x,y,f,g} t_{x,y,x\delta(g-y),x+f} \right. \\
 &\quad \cdot \log \left[\frac{t_{x,y,x\delta(g-y),x+f}}{[b_{xy} d_{x\delta(g-y),x+f}]} \right] \Bigg\}.
 \end{aligned}$$

The maximal value in the equation is a real number which satisfies the following conditions:

$$\begin{aligned}
 \sum_{0 \leq y \leq 10} r_y &= 1; \quad 0 \leq y \leq 10; \\
 \sum_{0 \leq y \leq 10, 0 \leq x \leq 5} b_{xy} &= 1; \quad 0 \leq y \leq 10, \quad 0 \leq x \leq 5, \\
 \sum_{0 \leq g \leq 10, 0 \leq f \leq 5} h_{fg} &= 1; \quad 0 \leq g \leq 10, \quad 0 \leq f \leq 5.
 \end{aligned} \quad (21)$$

Thus, the capacity D is actually the function of f_i, g_j , which satisfies the following conditions: $0 \leq f \leq 5; f_0 + f_1 + f_2 + f_3 + f_4 + f_5 = 1; 0 \leq g \leq 10; \sum_{0 \leq g \leq 10} s_g = 1$, where $0 \leq i \leq 5$ and $0 \leq j \leq 10$.

Similarly, we can analyze the situation of “ B wins.” We can see that the times of “ A wins” ($D(g_j, f_i)$) depend on the habit of $B(g_j, f_i)$. If both A and B stick to their habits, their winning or losing is determined; if either A or B adjusts his habit, he can win statistically when his channel capacity is larger; if both A and B adjust their habits, their situations will eventually reach a dynamic balance.

5. Unified Model of Linear Separable “Nonblind Confrontation”

Suppose that the hacker (X) has n methods of attack; that is, the random variable X has n values which can be denoted as $\{x_0, x_1, \dots, x_{n-1}\} = \{0, 1, 2, \dots, n-1\}$. These n methods make up the entire “arsenal” of the hacker.

Suppose that the honker (Y) has m methods of defense; that is, the random variable Y has m values, which can be denoted as $\{y_0, y_1, y_{m-1}\} = \{0, 1, 2, \dots, m-1\}$. These m methods make up the entire “arsenal” of the honker.

Remark 15. In the following, we will equivalently transform between “the methods x_i, y_j ” and “the numbers i, j ” as needed; that is, $x_i = i$ and $y_j = j$. By the transformation, we can make the problem clear in the interpretation and simple in the form.

In the nonblind confrontation, there is a rule of winning or losing between each hacker’s method x_i ($i = 0, 1, \dots, n-1$) and each honker’s method y_j ($j = 0, 1, \dots, m-1$). So there must exist a subset of the two-dimensional number set $\{(i, j), 0 \leq i \leq n-1, 0 \leq j \leq m-1\}$, which makes “ x_i is superior to y_j ” true if and only if $(i, j) \in H$. If the structure of the subset H is simple, we can construct a certain channel to make “the hacker wins one time” equivalent to “one bit is successfully transmitted from the sender to the receiver.” Then, we analyze it using Shannon’s “channel coding theorem.” For example,

in the game of “rock-paper-scissors,” $H = (i, j) : 0 \leq i, j \leq 2(j - i) \bmod 3 = 2$;

in the game of “coin tossing,” $H = (i, j) : 0 \leq i = j \leq 1$;

in the game of “palm or back,” $H = (i, j, k) : 0 \leq i \neq j = k \leq 1$;

in the game of “finger guessing,” $H = (i, j) : 0 \leq i, j \leq 3(i - j) \bmod 4 = 1$;

in the game of “draw boxing,” $H = (x, y, f, g) : 0 \leq x, f \leq 50 \leq g \neq y \leq 10x + f = y$.

We have constructed corresponding communication channels for each H above in this paper. However, it is difficult to construct such a communication channel for a general H . But if the above set H can be decomposed into $H = \{(i, j) : i = f(j), 0 \leq i \leq n - 1, 0 \leq j \leq m - 1\}$ (namely, the first component j of H is a function of its second component), we can construct a random variable $Z = f(Y)$. Then considering the channel $(X; Z)$, we can give the following equations.

If the “hacker X ” attacks with the method x_i , and “honker Y ” defends with the method y_j in a certain round, then if “ X wins,” that is, $i = f(j)$, the output of the channel $(X; Z)$ is $Z = f(y_j) = f(j) = i = x_i$. So the output of the channel is the same as its input now; that is, one bit is successfully transmitted from the input of the channel $(X; Z)$ to its output. Conversely, if “one bit is successfully transmitted from the input of the channel $(X; Z)$ to its output,” there is “input = output”; that is, “ $i = f(j)$,” which means “ X wins.”

Combining the cases above, we obtain the following theorem.

Theorem 16 (the limitation theorem of linear nonblind confrontation). *In the “nonblind confrontation”, suppose the hacker X has n attack methods $\{x_0, x_1, \dots, x_{n-1}\} = \{0, 1, 2, \dots, n - 1\}$ and the honker Y has m defense methods $\{y_0, y_1, y_{m-1}\} = \{0, 1, 2, \dots, m - 1\}$, and both sides comply with the rule of winning or losing: “ x_i is superior to y_j ” if and only if $(i, j) \in H$, where H is a subset of the rectangular set $\{(i, j), 0 \leq i \leq n - 1, 0 \leq j \leq m - 1\}$.*

For X , if H is linear and can be written as $H = \{(i, j) : i = f(j), 0 \leq i \leq n - 1, 0 \leq j \leq m - 1\}$ (i.e., the first component i of H is a certain function $f(\cdot)$ of its second component j), we can construct a channel $(X; Z)$ with $Z = f(Y)$ to get that, if C is the channel capacity of channel $(X; Z)$, we have the following.

(1) If X wants to win k times, he must have a certain skill (corresponding to the Shannon coding) to achieve the goal by any probability close to 1 in the k/C rounds.

(2) If X wins S times in n rounds, there must exist $S \leq nC$.

For Y , if H is linear and can be written as $H = \{(i, j) : j = g(i), 0 \leq i \leq n - 1, 0 \leq j \leq m - 1\}$ (i.e., the second component j of H is a certain function $g(\cdot)$ of its first component i), we can construct a channel $(Y; G)$ with $G = g(X)$ to get that, if D is the channel capacity of channel $(Y; G)$, we have the following.

(3) If Y wants to win k times, he must have a certain skill (corresponding to the Shannon coding) to achieve the goal by any probability close to 1 in the k/D rounds.

(4) If Y wins S times in n rounds, there must exist $S \leq nD$.

6. Conclusion

It seems that these games of nonblind confrontation are different. However, we use an unified method to get the

distinctive conclusion; that is, we establish a channel model which can transform “the attacker or the defender wins one time” to “one bit is transmitted successfully in the channel.” Thus, “the confrontation between attacker and defender” is transformed to “the calculation of channel capacities” by the Shannon coding theorem [6]. We find that the winning or losing rules sets of these games are linearly separable. For linearly inseparable case, it is still an open problem. These winning or losing strategies can be applied in big data field, which provides a new perspective for the study of the big data privacy protection.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This paper is supported by the National Key Research and Development Program of China (Grant nos. 2016YFB0800602, 2016YFB0800604), the National Natural Science Foundation of China (Grant nos. 61573067, 61472045), the Beijing City Board of Education Science and technology project (Grant no. KM201510015009), and the Beijing City Board of Education Science and Technology Key Project (Grant no. KZ201510015015).

References

- [1] R. J. Deibert and R. Rohozinski, “Risking security: policies and paradoxes of cyberspace security,” *International Political Sociology*, vol. 4, no. 1, pp. 15–32, 2010.
- [2] L. Shi, C. Jia, and S. Lv, “Research on end hopping for active network confrontation,” *Journal of China Institute of Communications*, vol. 29, no. 2, p. 106, 2008.
- [3] H. Demirkan and D. Delen, “Leveraging the capabilities of service-oriented decision support systems: putting analytics and big data in cloud,” *Decision Support Systems*, vol. 55, no. 1, pp. 412–421, 2013.
- [4] Y. Yang, H. Peng, L. Li, and X. Niu, “General theory of security and a study case in internet of things,” *IEEE Internet of Things Journal*, 2016.
- [5] Y. Yang, X. Niu, L. Li, H. Peng, J. Ren, and H. Qi, “General theory of security and a study of hacker’s behavior in big data era,” *Peer-to-Peer Networking and Applications*, 2016.
- [6] C. E. Shannon, “Coding theorems for a discrete source with a fidelity criterion,” *IRE National Convention Record*, vol. 4, pp. 142–163, 1959.
- [7] B. Kerr, M. A. Riley, M. W. Feldman, and B. J. M. Bohannan, “Local dispersal promotes biodiversity in a real-life game of rock-paper-scissors,” *Nature*, vol. 418, no. 6894, pp. 171–174, 2002.
- [8] K. L. Chung and W. Feller, “On fluctuations in coin-tossing,” *Proceedings of the National Academy of Sciences of the United States of America*, vol. 35, pp. 605–608, 1949.
- [9] K.-T. Tseng, W.-F. Huang, and C.-H. Wu, “Vision-based finger guessing game in human machine interaction,” in *Proceedings of the IEEE International Conference on Robotics and Biomimetics (ROBIO ’06)*, pp. 619–624, December 2006.

Hindawi

Submit your manuscripts at
<https://www.hindawi.com>