

## Card Problem

- Arrange the 16 face cards so that each Denomination ( Ace, King, Queen, Jack) and each suit (Club, Heart, Diamond, Spade) appears only once in each row and column

|    |    |    |    |
|----|----|----|----|
| ♠A | ♥A | ♦A | ♣A |
| ♠K | ♥K | ♦K | ♣K |
| ♠Q | ♥Q | ♦Q | ♣Q |
| ♠J | ♥J | ♦J | ♣J |

## Answer

|    |    |    |    |
|----|----|----|----|
| ♠A | ♥K | ♦Q | ♣J |
| ♦J | ♣Q | ♠K | ♥A |
| ♣K | ♦A | ♥J | ♠Q |
| ♥Q | ♠J | ♣A | ♦K |

# Latin Squares and Their Applications

Hong Zhou  
Department of Mathematics and Statistics  
Arkansas State University

MAA Seminar Series  
September 19, 2006

## Outline

- Introduction
- Latin Squares & Galois Field
- Applications of Latin Squares
- Summary

## History

- Latin squares have a long history. The earliest written reference is the solutions of the card problem published in 1723
- The systematic development of Latin squares started with Euler(1779). It was also called Euler Square
- In the 1930's, a big application area for Latin squares was opened by R.A.Fisher who used them in the design of statistical experiments

## Definition

- A **Latin square** is an  $s \times s$  square matrix whose entries consist of  $s$  letters such that each letter appears exactly once in each row and each column

|       |         |           |
|-------|---------|-----------|
| A B C | A B C D | A B C D E |
| B C A | B A D C | C D E A B |
| C A B | C D A B | E A B C D |
|       | D C B A | B C D E A |
|       |         | D E A B C |

## Orthogonal Latin Squares

- If we separate the denominations and the suits we obtain:

|                 |             |
|-----------------|-------------|
| ♠ ♥ ♦ ♣ A K Q J | ♠A ♥K ♦Q ♣J |
| ♦ ♣ ♠ ♥ J Q K A | ♦J ♣Q ♠K ♥A |
| ♣ ♦ ♥ ♠ K A J Q | ♣K ♦A ♥J ♠Q |
| ♥ ♠ ♣ ♦ Q J A K | ♥Q ♠J ♣A ♦K |

- The first two Latin squares are 4x4 Latin squares. If we superimpose one onto the other, *each card (a pair of suit and denomination)* exactly occurs once in the third square, therefore they are orthogonal to each other

## Orthogonality

- The property needed by the pair of Latin squares in the solution of the 16 card problem is called ***orthogonality***.
- Two Latin squares  $L_1 = [a_{ij}]$  and  $L_2 = [b_{ij}]$  on  $s$  numbers  $1, 2, \dots, s$  are said to be ***orthogonal*** if every ordered pair of numbers occurs exactly once among the  $s^2$  pairs  $(a_{ij}, b_{ij})$ ,  $i = 1, 2, \dots, s$ ;  $j = 1, 2, \dots, s$

## Graeco-Latin Squares

- $A B C$              $\alpha \beta \gamma$              $A_\alpha B_\beta C_\gamma$   
   $B C A$              $\gamma \alpha \beta$              $B_\gamma C_\alpha A_\beta$   
   $C A B$              $\beta \gamma \alpha$              $C_\beta A_\gamma B_\alpha$
- Graeco-Latin Squares of order  $s$  exist
  - When  $s$  is a prime or a power of a prime
  - When  $s$  is all other odd numbers
- Question: Do Graeco-Latin squares of order  $s$  always exist when  $s$  is an even number?

## 36 Officer Problem

- In a 1782 paper, Euler started by stating the problem of the 36 officers.
- This problem asks for an arrangement of 36 officers of 6 ranks and from 6 regiments into a square of size 6.
- Each column and each row of this square is to contain one and only one officer of each rank and one and only one officer from each regiment.

## Pair of Orthogonal Latin Squares

- Euler's Conjecture(1782):
  - If  $s \equiv 2 \pmod{4}$ , there did not exist a pair of orthogonal squares
- Tarry(1901):
  - verified this conjecture for the case  $s=6$
- Euler Spoilers: Bose, Shrikhande and Parker(1959,1960):
  - If  $s \equiv 2 \pmod{4}$  and  $s>6$ , a pair of orthogonal squares always exists

## Mutually Orthogonal Latin Squares

- A set of Latin squares of the same order, each of which is orthogonal to each other, is called a **set of mutually orthogonal Latin squares (MOLS)**

|   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | A | B | C | D | A | B | C | D |
| B | A | D | C | C | D | A | B | D | C | B | A |
| C | D | A | B | D | C | B | A | B | A | D | C |
| D | C | A | B | B | A | D | C | C | D | A | B |

## Q: How to find a set of orthogonal Latin Squares?

- Bose Methods (1938):
  - Galois Field/Finite Field
- What is Galois Field (GF)?

## Galois Field / Finite Field

- Galois field: A field  $F$  is a set of more than one element for which there are defined operations of additions and multiplications which satisfy following laws:
- Commutative law:  $a+b=b+a$ ,  $ab=ba$
- Associative Law:  $a+(b+c)=(a+b)+c$ ,  $a(bc)=(ab)c$
- Distributive Law:  $a(b+c)=ab+ac$
- Law of Inverse existence:
  - For every pair  $a,b$ , there exists an  $x$  such that  $x+a=b$
  - For every pair  $a,b$  satisfying the condition  $a \neq 0$ , there exists an  $y$  such that  $ya=b$

## Construction of Galois Field

- Galois Field
  - Denoted by  $GF(s)$ ,  $s=p^n$ ,  $n \geq 1$ ,  $p$  is a prime
  - Constructed when  $s$  is a prime or a power of prime
- Elements of  $GF(S)$ :
  - $\alpha_0=0, \alpha_1=1, \alpha_2=x, \alpha_3=x^2, \alpha_4=x^3, \dots, \alpha_{s-1}=x^{s-2}$
  - where  $x$  is a primitive element of the field, i.e.,  $x$  is an element such that  $x^{s-1}=1 \pmod{p}$  and there is no other power  $q$ ,  $x^q=1 \pmod{p}$ ,  $0 < q < s$ .
- Cyclotomic Equation:  $x^{s-1}=1 \pmod{p}$

## Example1: Construction of $GF(3)$

- Solve Cyclotomic Equation:  $x^{s-1}=1 \pmod{p}$ 
  - $n=1, p=3, s=p^n=3^1=3$  (*prime*)
  - $x^{3-1}=1 \pmod{3}$
  - $x=2$  (*primitive root of  $GF(3)$* )
- Elements of  $GF(3)$ 
  - $\alpha_0=0, \alpha_1=1, \alpha_2=2$

## Addition Table of GF(3)

|   |   |   |   |
|---|---|---|---|
|   | 0 | 1 | 2 |
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

• Associate each of the letters with an element of the Galois field, GF(3), in a one-to-one correspondence  
That is  $A \rightarrow 0$ ,  $B \rightarrow 1$ ,  $C \rightarrow 2$

$L_1$  comes directly from addition table

•  $L_2$  is obtained by rotating the second and third row of  $L_1$

|   |       |       |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |    |    |    |    |    |    |    |    |    |
|---|-------|-------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|--|----|----|----|----|----|----|----|----|----|
| $L_1$   | $L_2$ | $L_3$ |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |    |    |    |    |    |    |    |    |    |
| <table style="border-collapse: collapse; text-align: center;"> <tr><td>A</td><td>B</td><td>C</td></tr> <tr><td>B</td><td>C</td><td>A</td></tr> <tr><td>C</td><td>A</td><td>B</td></tr> </table> | A     | B     | C | B | C | A | C | A | B | <table style="border-collapse: collapse; text-align: center;"> <tr><td>A</td><td>B</td><td>C</td></tr> <tr><td>C</td><td>A</td><td>B</td></tr> <tr><td>B</td><td>C</td><td>A</td></tr> </table> | A | B | C | C | A | B | B | C | A | <table style="border-collapse: collapse; text-align: center;"> <tr><td>AA</td><td>BB</td><td>CC</td></tr> <tr><td>BC</td><td>CA</td><td>AB</td></tr> <tr><td>CB</td><td>AC</td><td>BA</td></tr> </table> | AA | BB | CC | BC | CA | AB | CB | AC | BA |
| A   | B     | C     |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |    |    |    |    |    |    |    |    |    |
| B   | C     | A     |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |    |    |    |    |    |    |    |    |    |
| C   | A     | B     |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |    |    |    |    |    |    |    |    |    |
| A   | B     | C     |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |    |    |    |    |    |    |    |    |    |
| C   | A     | B     |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |    |    |    |    |    |    |    |    |    |
| B   | C     | A     |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |    |    |    |    |    |    |    |    |    |
| AA  | BB    | CC    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |    |    |    |    |    |    |    |    |    |
| BC  | CA    | AB    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |    |    |    |    |    |    |    |    |    |
| CB  | AC    | BA    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |    |    |    |    |    |    |    |    |    |

## Construction of Mutually Orthogonal Latin Squares

- Bose Method (1938):
  - Elements of GF(s)
    - ordered by  $\alpha_0=0$ ,  $\alpha_1=1$ ,  $\alpha_2=x$ ,  $\alpha_3=x^2$ ,  $\alpha_4=x^3$ , ...,  $\alpha_{s-1}=x^{s-2}$
    - where  $x$  is a primitive element of the field
    - $x$  is an element such that  $x^{s-1}=1 \pmod{p}$  and there is no other power  $q$ ,  $x^q=1$ ,  $0 < q < s$ .
  - Addition table forms a Latin square
  - Other squares can be obtained by rotating cyclically all the rows except the first

## Example2: Construction of GF(2<sup>2</sup>)

- Now, **s is a power of a prime**
- Solve Cyclotomic Equation:  $x^{s-1} = 1 \pmod{2}$ 
  - $p=2, n=2, s=2^2=4$
  - $x^{4-1} = 1 \pmod{2}$ , i.e.  $x^3 = 1 \pmod{2}$
  - $x^2 = x+1$  (minimum function for GF(2<sup>2</sup>))
- Elements of GF(2<sup>2</sup>)
  - $\alpha_0=0, \alpha_1=1, \alpha_2=x, \alpha_3=x^2=x+1$

## Addition Table of GF(2<sup>2</sup>)

|     |     |     |     |     |
|-----|-----|-----|-----|-----|
|     | 0   | 1   | X   | X+1 |
| 0   | 0   | 1   | X   | X+1 |
| 1   | 1   | 0   | X+1 | X   |
| X   | X   | X+1 | 0   | 1   |
| X+1 | X+1 | X   | 1   | 0   |

L<sub>1</sub>                      L<sub>2</sub>                      L<sub>3</sub>

|      |      |      |
|------|------|------|
| ABCD | ABCD | ABCD |
| BADC | CDAB | DCBA |
| CDAB | DCBA | BADC |
| DCBA | BADC | CDAB |

- Associate each of the letters with an element of the Galois field, GF(2<sup>2</sup>), i.e. A→0, B→1, C→x, D→x+1
- L<sub>1</sub> comes directly from addition table
- L<sub>2</sub> is obtained by rotating the 2<sup>nd</sup> to 4<sup>th</sup>; the 3<sup>rd</sup> to 2<sup>nd</sup>; the 4<sup>th</sup> to 3<sup>rd</sup> row of L<sub>1</sub>
- L<sub>3</sub> is obtained by rotating rows of L<sub>2</sub> in the same manner

## Complete Sets of MOLS

- A set of MOLS of order  $s$  containing  $s-1$  squares is called a **complete set**
- Existence of complete sets of MOLS exist
  - For  $s=2$ , complete sets exist for order 2 (only one square is needed)
  - $s=3$  and 4, complete sets of MOLS exist
  - Using finite fields, complete sets of MOLS for any order which is a prime or power of a prime can be constructed
  - no complete set exists for orders 6 and 10
- However, it is an open research question:
  - Whether or not a complete set of MOLS exists for any composite order.

## Application of Latin Squares

- Let us consider an experiment in automobile company, an engineer wants to examine the rate of consumption in miles per gallon for cars.
- Which gasoline gives us a good mileage? Is there any difference among three gasoline in terms of mileage?
- Response: miles per gallon
- Factor: type of gasoline, 83,89,or 93?
- Two nuisance factors: *car* and *day*
  - Performance of each car might be different: car-to-car variation
  - Weather of each day might be different: warmer or drier, day-to-day variation
  - Constrains: each car can only test one gasoline per day;

## 3x3 Latin Square

- Letters represent three different type of gasoline, A=83, B=89, C=93
- Rows=days, columns=cars

|      | Car1 | Car2 | Car3 |
|------|------|------|------|
| Day1 | A    | B    | C    |
| Day2 | B    | C    | A    |
| Day3 | C    | A    | B    |

## Using Latin Square

- Purpose of using Latin Square design is to improve the precision of the gasoline comparisons by eliminating the car and day effects
- Latin square design is only used in the situation where there is no interactions between factors

## Summary

- Euler's conjecture(1782)
  - If  $s \equiv 2 \pmod{4}$ , there did not exist a pair of orthogonal squares
- Euler spoilers:
  - Bose, Shrikhande and Parker(1959,1960): If  $s \equiv 2 \pmod{4}$  and  $s > 6$ , a pair of orthogonal squares always exists
- Graeco-Latin squares of order  $s$  exist
  - When  $s$  is a prime or a power of prime
  - Construction: using Galois field or Bose method
- Application: Design of Experiments

## Open Research Question

- Whether or not a complete set of Mutually Orthogonal Latin Square exists for any composite order?
- *Instant fame will go to any mathematician who can settle this question.*

**THANK YOU!**