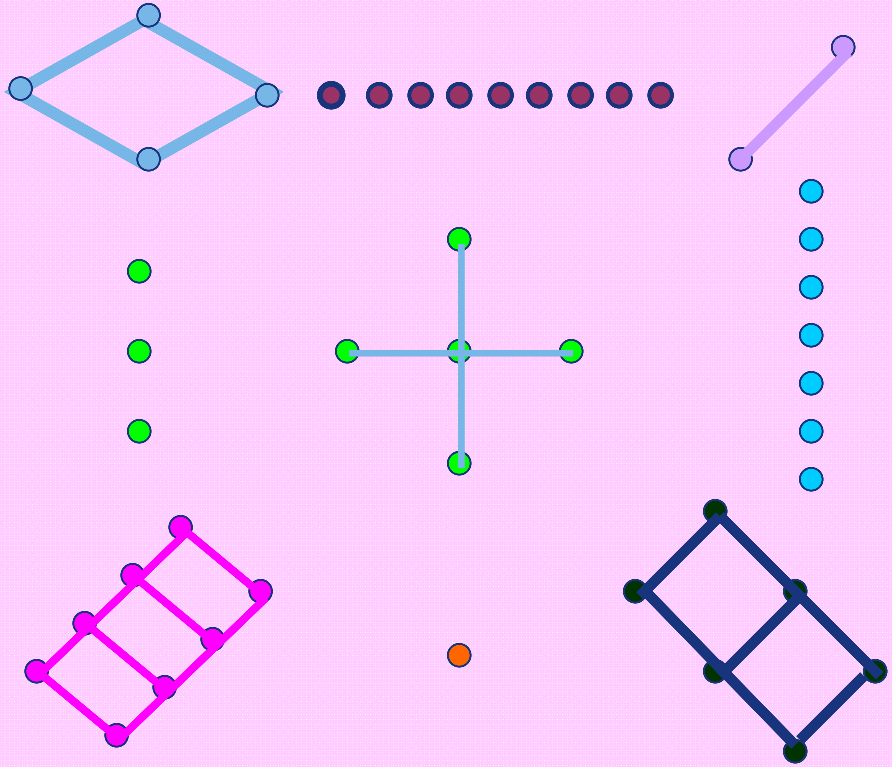
前景广阔的古老组合学分支

— 组合设计漫谈 —

1. Combinatorics and designs
2. Topics of Combinatorial designs
3. Applications of design theory



2000BC

神农幻方

4	9	2
3	5	7
8	1	6

1	15	14	4
12	6	7	9
8	10	11	5
13	3	2	16

Magic square

加乘幻方

幻和数= 840

幻积数= 205806823185600

$= 2^7 3^8 5^3 7^1 13^1 17^1 19^1 23^1 29^1$

Walter W. Horner, 1955

46	81	117	102	15	76	200	203
19	60	232	175	54	69	153	78
216	161	17	52	171	90	58	75
135	114	50	87	184	189	13	68
150	261	45	38	91	136	92	27
119	104	108	23	174	225	57	30
116	25	133	120	51	26	162	207
39	34	138	243	100	29	105	152

$2*23$	3^4	3^2*13	$2*3*17$	$3*5$	2^2*19	2^3*5^2	$7*29$
19	2^2*3*5	2^3*29	5^5*7	$2*3^3$	$3*23$	3^2*17	$2*3*13$
2^3*3^3	$7*23$	17	2^2*13	3^2*19	$2*3^2*5$	$2*29$	$3*5^2$
3^3*5	$2*3*19$	$2*5^2$	$3*29$	2^3*23	3^3*7	13	2^2*17
$2*3*5^2$	3^2*29	3^2*5	$2*19$	$7*13$	2^3*17	2^2*23	3^3
$7*17$	2^3*13	2^2*3^3	23	$2*3*29$	3^2*5^2	$3*19$	$2*3*5$
2^2*29	5^2	$7*19$	2^3*3*5	$3*17$	$2*13$	$2*3^4$	3^2*23
$3*13$	$2*17$	$2*3*23$	7^3	2^2*5^2	29	$3*5*7$	2^3*19

36 officers (*Euler* 1779)

腓特烈大帝的阅兵难题-----*Euler* 的困惑

Latin square

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 4 & 3 \\ 2 & 3 & 1 & 4 \\ 3 & 4 & 2 & 1 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

Orthogonal Latin squares

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 11 & 22 & 33 \\ 32 & 13 & 21 \\ 23 & 31 & 12 \end{pmatrix}$$

正交拉丁方与正交拉丁方组

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	2	3	4	2	1	4	3	3	4	1	2	4	3	2	1
1	2	3	4	3	4	1	2	4	3	2	1	2	1	4	3
1	2	3	4	4	3	2	1	2	1	4	3	3	4	1	2

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \\ 5 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \\ 2 & 3 & 4 & 5 & 1 \\ 5 & 1 & 2 & 3 & 4 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

Euler's conjecture

不存在 6 阶正交拉丁方！

不存在 $4k+2$ 阶正交拉丁方！

现在的结论

对任意正整数 $n \neq 2, 6$, 存在 n 阶正交拉丁方.

$\exists\ 2-MOLS(n)$ for $n \neq 2,\ 6$;

$\exists\ 3-MOLS(n)$ for $n \neq 2,\ 3,\ 6,\ 10$;

$\exists\ 4-MOLS(n)$ for $n \neq 2,\ 3,\ 4,\ 6,\ 10,\ 14,\ 18,\ 22$;

Kirkman's schoolgirl problem

(*T. P. Kirkman 1847*)

SUN	MON	TUE	WED	THU	FRI	SAT
1 2 3	1 4 5	1 6 7	1 8 9	1 10 11	1 12 13	1 14 15
4 8 12	2 8 10	2 9 11	2 12 14	2 13 15	2 4 6	2 5 7
5 10 15	3 13 14	3 12 15	3 5 6	3 4 7	3 9 10	3 8 11
6 11 13	6 9 15	4 10 14	4 11 15	5 9 12	5 11 14	4 9 13
7 9 14	7 11 12	5 8 13	7 10 13	6 8 14	7 8 15	6 10 12

Thomas Penyngton Kirkman（英格兰教会的教区长）

<Lady's and Gentleman's Diary>

$KTS(15) \quad \{a\} \cup (Z_7 \times Z_2) \ \bmod 7$

{a, 50, 31} , {01, 41, 51} , {00, 10, 11} , {20, 40, 61} , {30, 60, 21}

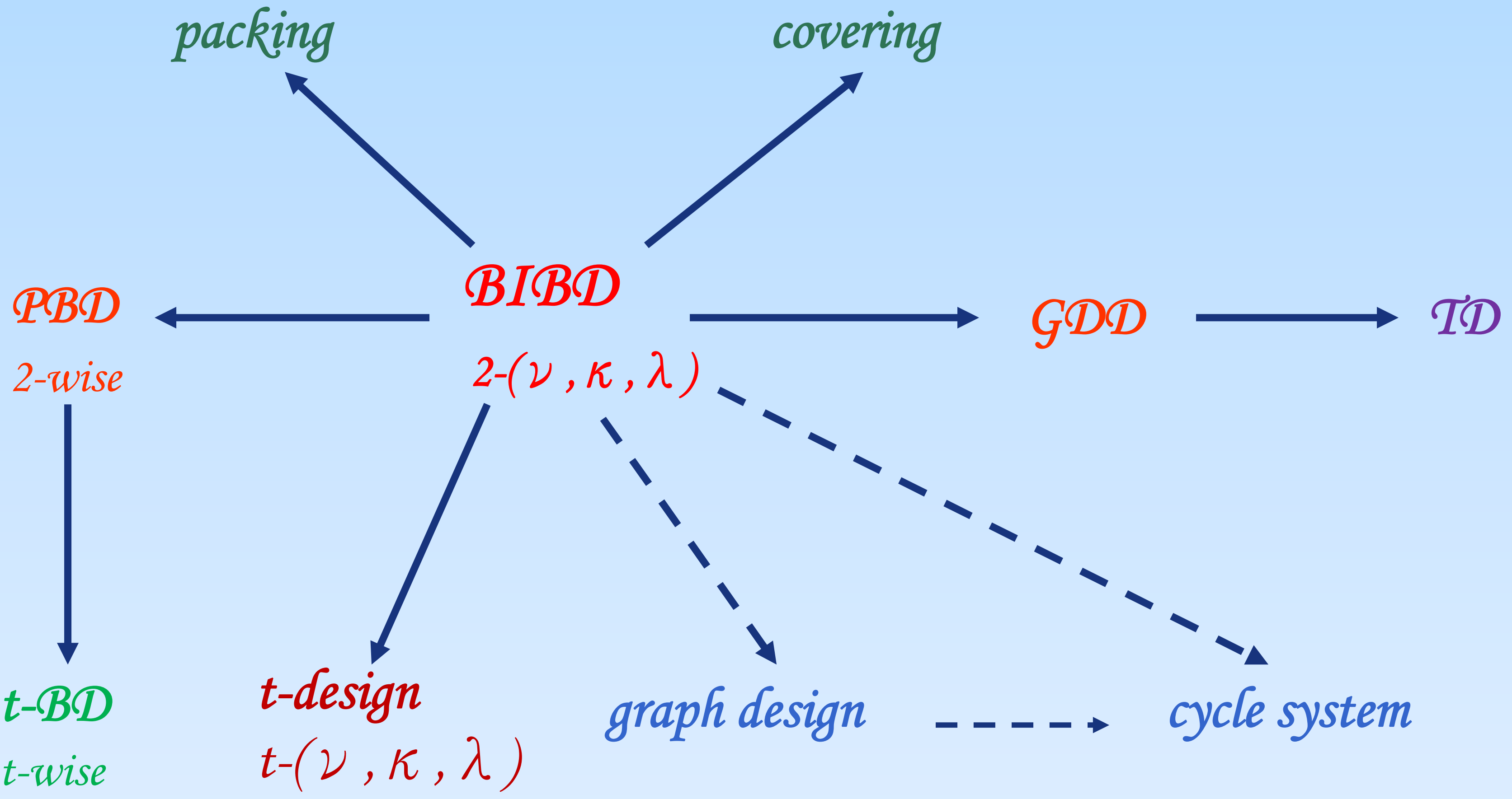
$LKTS(15) \quad \{a, b\} \cup Z_{13} \ \bmod 13$

SUN			MON			TUE			WED			THU			FRI			SAT		
0	*a*	*b*	2	8	*b*	11	12	*b*	5	7	*b*	4	9	*b*	1	10	*b*	3	6	*b*
8	9	12	1	6	*a*	4	10	*a*	3	12	*a*	2	5	*a*	9	11	*a*	7	8	*a*
3	7	10	4	7	11	6	7	9	2	9	10	6	8	10	5	6	12	5	10	11
2	6	11	3	5	9	1	2	3	1	8	11	1	7	12	3	4	8	2	4	12
1	4	5	0	10	12	0	5	8	0	4	6	0	3	11	0	2	7	0	1	9

(1850 Sylvester, Cayley —— 1974 Denniston)

组　合　设　计　家　族

- 区组设计 block design



表阵形组合设计

有序设计　　　　频率方

直交表 ← 正交表 ↔ **正交拉丁方** ← 拉丁方 → 拉丁矩

Tuscan方

Room 方

Youden 方　　Hadamard 矩阵　　Costas 阵　　差矩阵

Howell 设计

- 有向区组设计

有向图设计 → Mendelsohn design

有向图设计 → directed design

- 其它组合设计

PBIB　　Skolem 序列

赛程设计　　差集　有限几何　　图标号

结合方案　　de Bruijn 序列

- 相关问题

简单的　　纯的　　可分解的

大集　　超大集　　不同构计数

区组设计(BIBD)

Balanced Incomplete Block Design

A $BIBD(v,b,r,k,\lambda)$ is a pair (X,β) where X is a v-set and β is a collection of b k-subsets of X (blocks) such that each element of X is contained in exactly r blocks and any 2-subset of X is contained in exactly λ blocks.

$$vr = bk, \quad r(k-1) = \lambda(v-1)$$

$$\exists\,(v,k,\lambda)-BIBD \Rightarrow \begin{matrix} k(k-1) \mid \lambda v(v-1) \\ (k-1) \mid \lambda(v-1) \end{matrix}$$

$$Fisher's\ inequality:\ 2 \le k < v \Rightarrow b \ge v$$

Examples for **BIBD**

2-(7, 3, 1) : {0, 1, 3} mod 7

2-(9, 3, 1) :

0 1 2	0 3 6	0 4 8	0 5 7
3 4 5	1 4 7	1 5 6	1 3 8
6 7 8	2 5 8	2 3 7	2 4 6

$$\begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \end{pmatrix}$$

2-(16, 6, 2) :

1 2 3 4 8 12	0 2 3 5 9 13	0 1 3 6 10 14	
0 1 2 7 11 15	0 5 6 7 8 12	1 4 6 7 9 13	
2 4 5 7 10 14	3 4 5 6 11 15	0 4 9 10 11 12	
1 5 8 10 11 13	2 6 8 9 11 14	3 7 8 9 10 15	
0 4 8 13 14 15	1 5 9 12 14 15	2 6 10 12 13 15	3 7 11 12 13 14

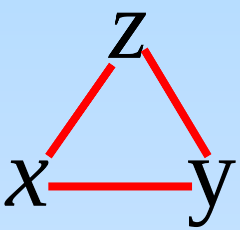
$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \\ 12 & 13 & 14 & 15 \end{pmatrix}$$

2-(15, 3, 1) : {0, 1, 4}, {0, 7, 13}, {0, 5, 10} mod 15

2-(9, 4, 3) : GF(9)上本原元 $x \to x^2 + x + 2 = 0$

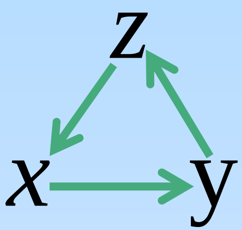
$$\{1, x^2, x^4, x^6\} + y,\ \{x, x^3, x^5, x^7\} + y,\ y \in GF(9).$$

Six types of triples and the corresponding triple sysems



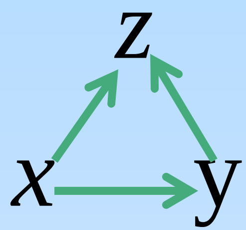
$\{x, y, z\}$

Steiner



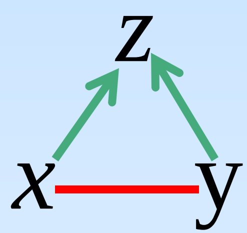
$\langle x, y, z \rangle$

Mendelsohn



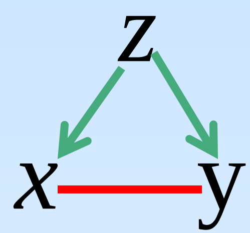
(x, y, z)

Directed



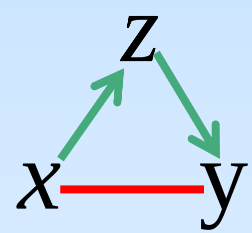
$[x, y, z]_1$

T_1



$[x, y, z]_2$

T_2



$[x, y, z]_3$

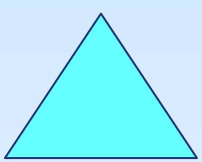
T_3

K_v — complete graph of order v

DK_v — complete symmetric directed graph of order v

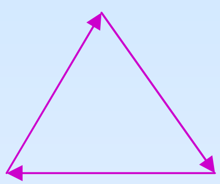
$STS(v)$	a partition of edges of	K_v	into	C_3
$MTS(v)$	a partition of edges of	DK_v	into	$\overrightarrow{C}_3$
$DTS(v)$	a partition of edges of	DK_v	into	TT_3
$HTS(v)$	a partition of edges of	DK_v	into	$\overrightarrow{C}_3$ or TT_3

triangle



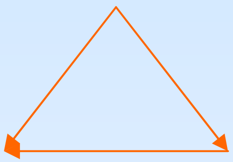
C_3

cyclic triangle



$\overrightarrow{C}_3$

transitive triangle



TT_3

The existence for triple systems

$$\exists\, STS(v) \Leftrightarrow v \equiv 1,3 \mod 6$$

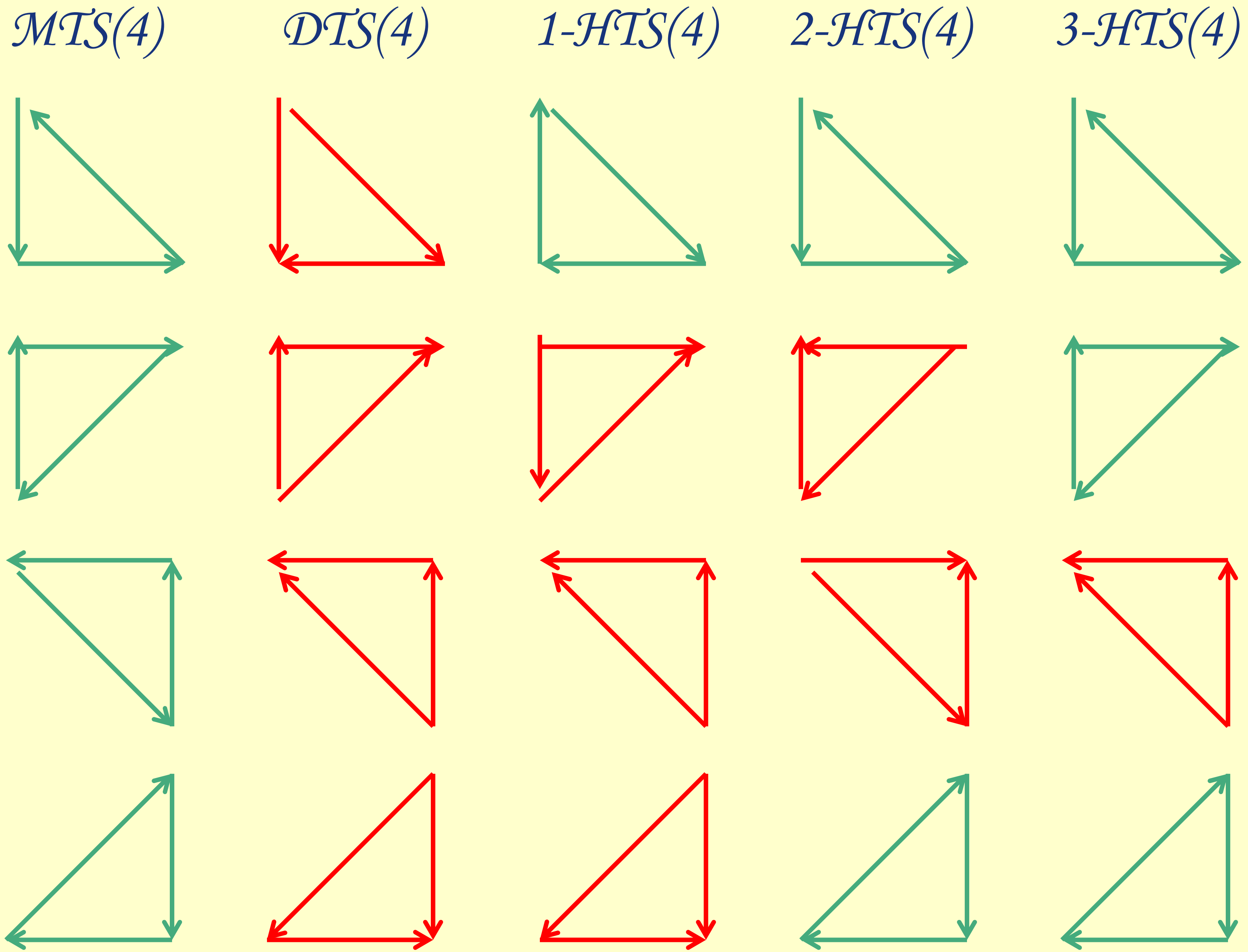
$$\exists\, KTS(v) \Leftrightarrow v \equiv 3 \mod 6$$

$$\exists\, MTS(v) \Leftrightarrow v \equiv 0,1 \mod 3,\ v \neq 6$$

$$\exists\, DTS(v)\ (HTS(v)) \Leftrightarrow v \equiv 0,1 \mod 3$$

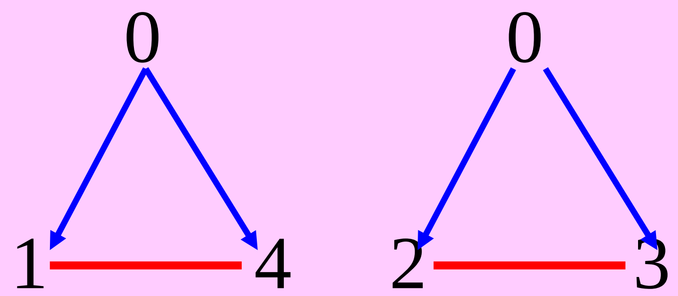
$$\exists\, T_1(v)\ (T_2(v)) \Leftrightarrow v \equiv 1 \mod 2$$

$$\exists\, T_3(v) \Leftrightarrow v \equiv 1 \mod 2,\ v \neq 3,5$$


MTS(4)
DTS(4)
1-HTS(4)
2-HTS(4)
3-HTS(4)

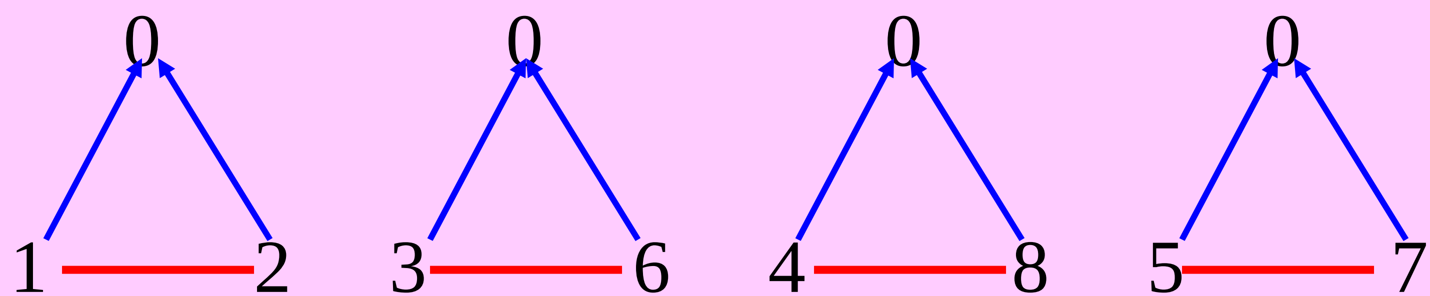
Three special types of triple systems

$T_1(5)$:



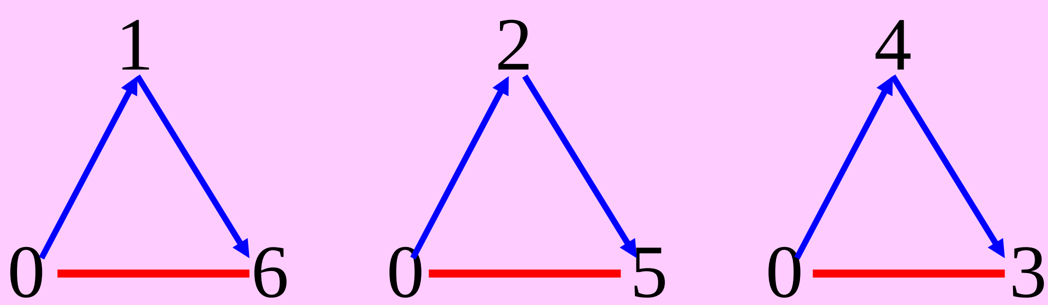
mod 5

$T_2(9)$:



(develop 9)

$T_3(7)$:



mod 7

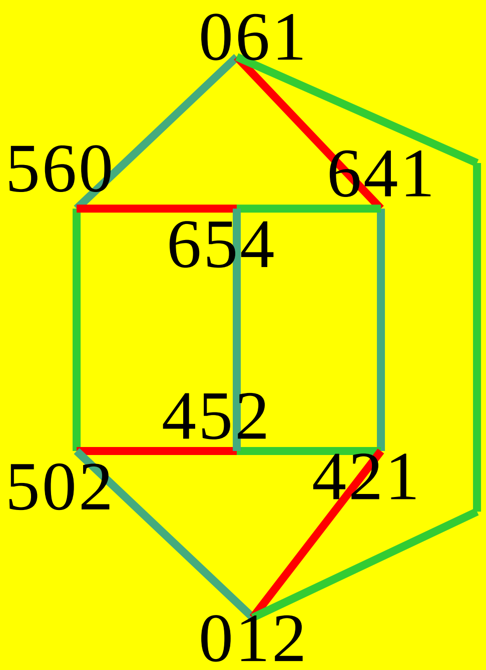
Nonisomorphic MTS(7)s

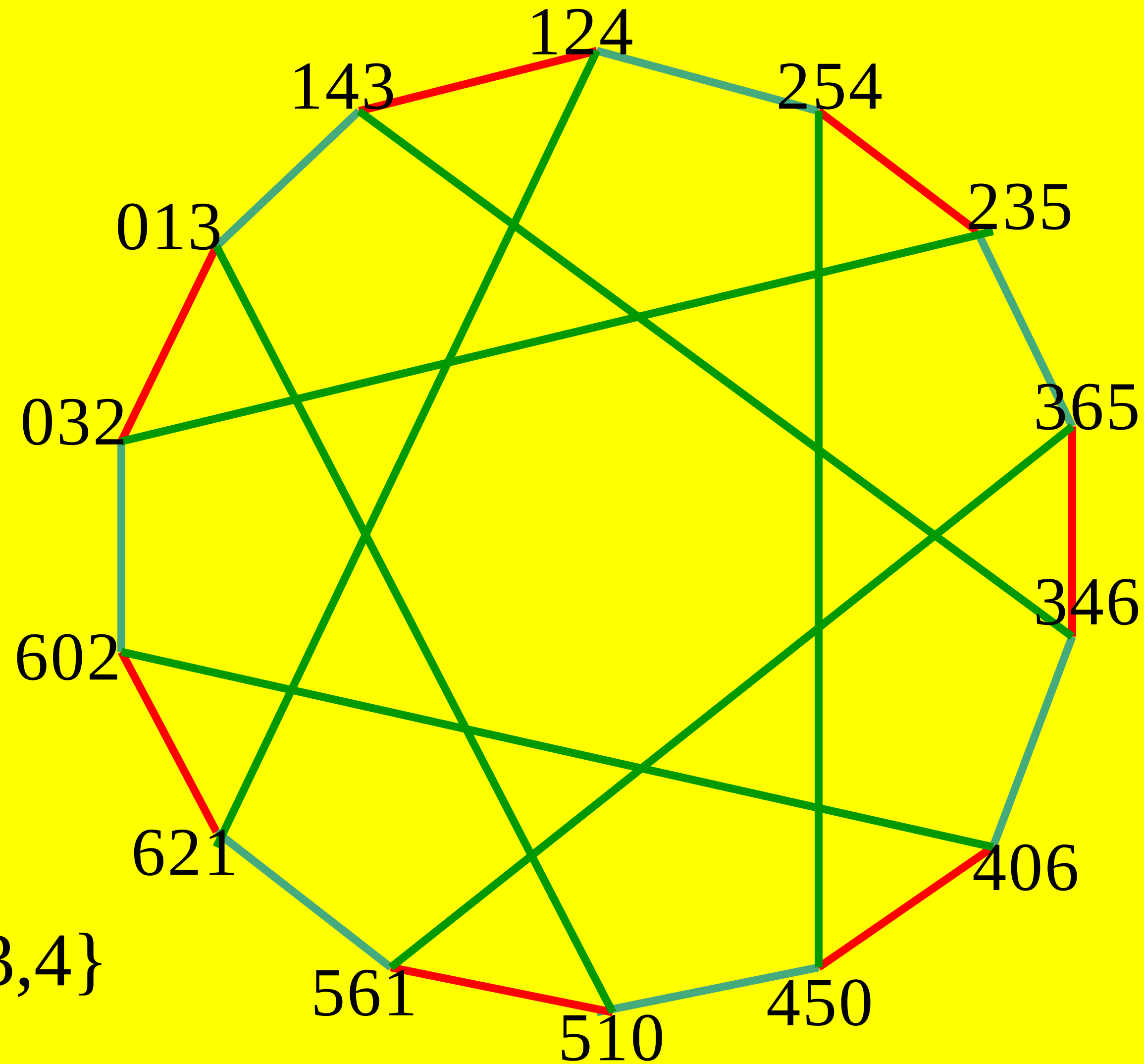
013 124 235 346 450 561 602
310 421 532 643 054 165 206

034 135 236 012 025 056 061
430 531 632 465 416 421 452

013 026 032 045 051 064 124
254 143 156 162 346 235 365

Nonisomorphisic MTS(7)

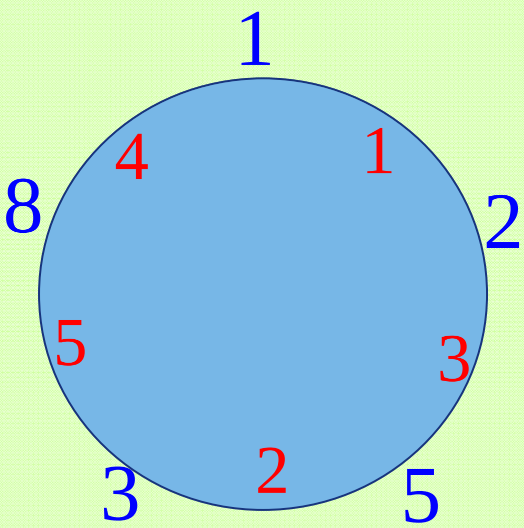




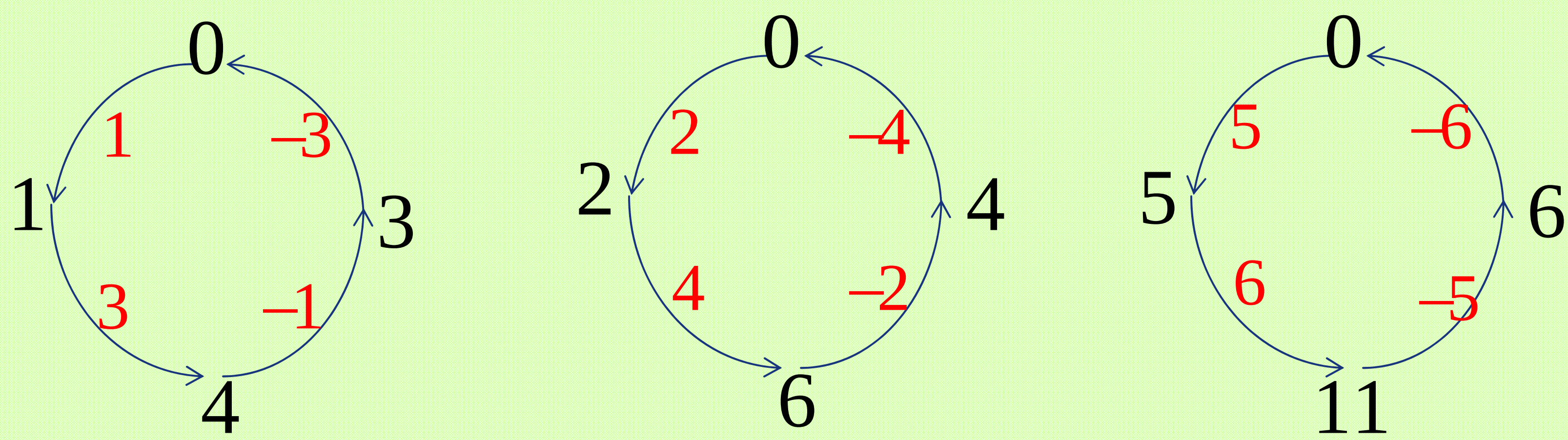
$sub - MTS(3)s$ on

$\{1,3,5\},\{2,3,6\},\{0,3,4\}$

Cycle system



mod 11 *5-cycle system of* K_{11}



mod 13 *4-cycle system of* DK_{13}

Hadamard Matrix

a (1,-1)-matrix $\mathcal{H}_n$ of order n, satisfying

$$H_n H_n^T = nI_n$$

$$\boxed{\exists\, H_n \Rightarrow n = 1, 2 \text{ or } 4 \mid n}$$

$$H_1 = (1),\ H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},\ H_8 = \begin{pmatrix} H_4 & H_4 \\ H_4 & -H_4 \end{pmatrix}$$

$$\textit{Hadamard conjecture}: \exists\, H_n \Leftrightarrow n = 1, 2 \text{ or } 4 \mid n$$

67	14	58		23	
24	57	13		68	
38		47	25		16
15		26	37		48
	28		46	17	35
	36		18	45	27

Howell Design

H(6,8)

Room square

of order 7

A0			15		46	23
34	A1			26		50
61	45	A2			30	
	02	56	A3			41
52		13	60	A4		
	63		24	01	A5	
		04		35	12	A6

Golf design of order 7

4					
5	3				
6	2	1			
2	0	6	5		
3	6	4	0	1	
1	5	0	4	3	2

2	4	5	1	6	3
	6	4	5	3	0
		0	3	1	5
			6	2	1
				0	2
					4

0	6	1	4	3	2	5
6	1	0	5	2	4	3
1	0	2	6	5	3	4
4	5	6	3	0	1	2
3	2	5	0	4	6	1
2	4	3	1	6	5	0
5	3	4	2	1	0	6

5					
3	4				
2	6	5			
6	3	0	1		
1	0	6	4	2	
4	2	1	0	5	3

3	6	1	5	4	2
	5	0	6	2	4
		4	1	0	3
			2	6	5
				3	0
					1

Costas array

#			
		#	
			#
	#		

#				
		#		
			#	
	#			
				#

		#				
					#	
						#
#						
				#		
	#					
			#			

Skolem sequences

A *Skolem sequence* *of order* n *is a partition of the set* $\{1,2,\cdots,2n\}$ *into* n *ordered pairs* $(a_1,b_1),\ (a_2,b_2),\cdots,\ (a_n,b_n)$ *such that* $b_k - a_k = k$ *for* $1 \le k \le n$.

$n=1:\quad (1,2);$

$n=4:\ (1,2),\ (4,6),\ (5,8),\ (3,7);$

$n=5:\ (1,2),\ (4,6),\ (7,10),\ (5,9),\ (3,8);$

$n=8:\ (15,16),\ (5,7),\ (11,14),\ (9,13),\ (1,6),\ (2,8),\ (3,10),\ (4,12);$

$n=9:\ (3,4),\ (13,15),\ (6,9),\ (12,16),\ (2,7),\ (11,17),\ (1,8),\ (10,18),\ (5,14);$

$n=12:\ \cdots\cdots;$

$\cdots\cdots\cdots\cdots\cdots\cdots$

There exists a Skolem sequence of order n if and only if

$$n \equiv 0,1 \bmod 4$$

More about Skolem sequences

Skolem

$n=5:\ (1,2),(7,9),(3,6),(4,8),(5,10).$

hooked Skolem

$n=6:\ (1,2),(3,5),(8,11),(6,10),(4,9),(7,13).$

Langford

$n=5, d=3:\ (3,6),(5,9),(2,7),(4,10),(1,8).$

hooked

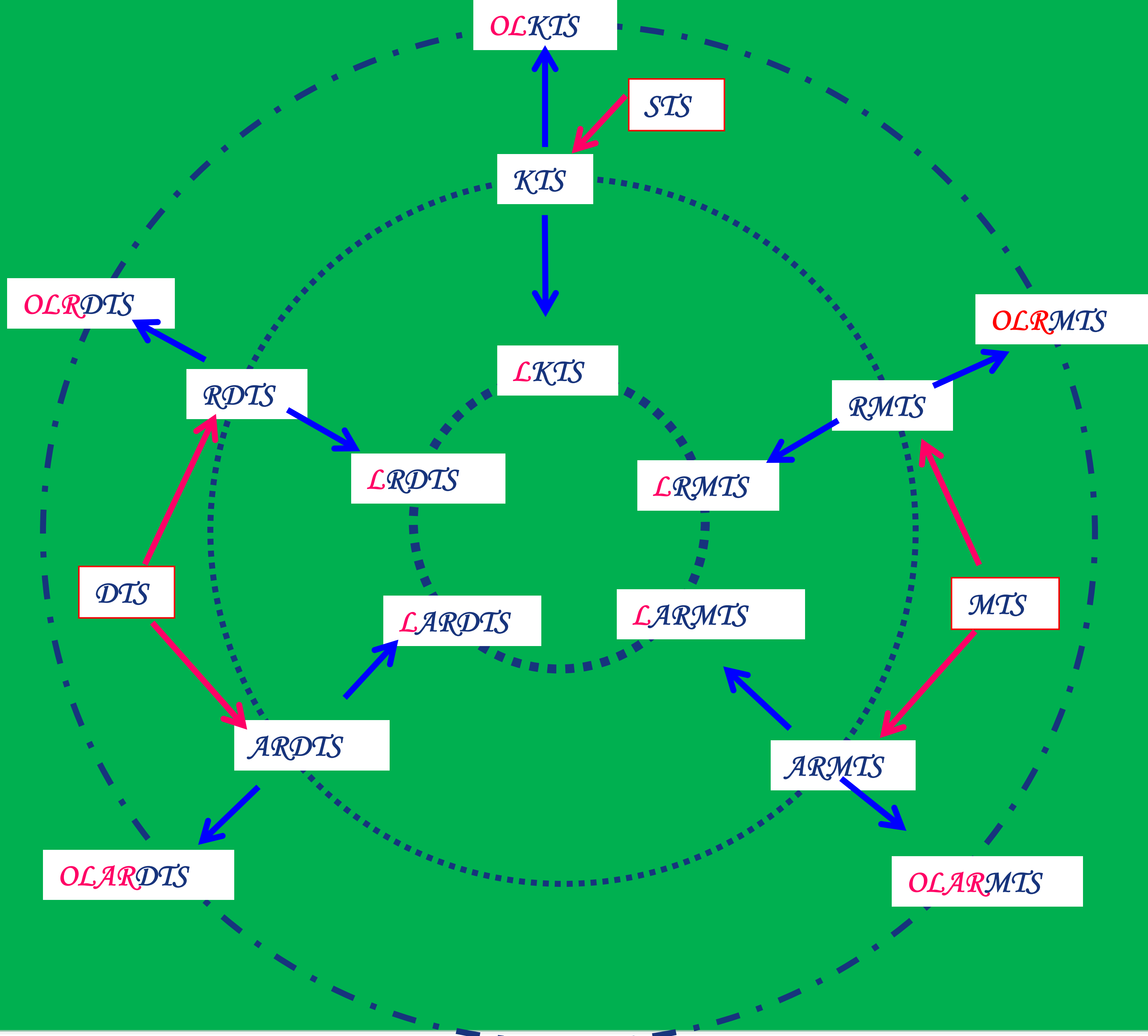
$n=5, d=2:\ (1,3),(6,9),(4,8),(2,7),(5,11).$

near – Skolem

$n=7, m=4:\ (1,2),(8,10),(4,7),(6,11),(3,9),(5,12).$

hooked

$n=6, m=3:\ (1,2),(6,8),(3,7),(4,9),(5,11).$


OLKTS
STS
KTS
LKTS
OLRDTS
RDTS
LRDTS
OLRMTS
RMTS
LRMTS
DTS
LARDTS
LARMTS
MTS
ARDTS
ARMTS
OLARDTS
OLARMTS

经典三元系大集的存在谱

$LSTS(v,\lambda)$	$6 \mid \lambda v(v-1), \lambda \mid (v-2), (v,\lambda) \neq (7,1).$ 1983 Lu Jiaxi, 1989 Luc Teirlinck
$LMTS(v,\lambda)$	$3 \mid \lambda v(v-1), \lambda \mid (v-2), (v,\lambda) \neq (6,1).$ 1994 Kang, Lei & Chang
$LDTS(v,\lambda)$	$3 \mid \lambda v(v-1), \lambda \mid (v-2).$ 1992 Kang & Chang
$LHTS(v,\lambda)$	$3 \mid \lambda v(v-1), \lambda \mid 4(v-2), (v,\lambda) \neq (3,1).$ 1996 Kang & Lei

* A short proof for *LSTS(v)* was given by L. Ji & L. Zhu.

Large Sets of ***Pure***

Mendelsohn (Directed) triple systems

$LPMTS(v)$	$v \equiv 0,1 \bmod 3,\ v \geq 4$ and $v \neq 6,7$
	J. Zhou, Y. Chang and L. Ji , 2006
$LPDTS(v)$	$v \equiv 0,1 \bmod 3$ and $v \geq 4$
	J. Zhou, Y. Chang and L. Ji , 2006

*　无遗留问题

在完全图中：*Large Sets of*

Hamilton cycle (path) decompositions

$LHCD(v)$	$odd\ \ v \geq 3$	*H. Zhao, Q.Kang,* 2005
$LHCD_2(v)$	$even\ \ v \geq 4$	*D. E. Bryant,* 1998
$LHPD(v)$	$even\ \ v \geq 2$	*H. Zhao, Q.Kang,* 2005
$LHPD_2(v)$	$odd\ \ v \geq 3$	*D. E. Bryant,* 1998

*　无遗留问题

在二分图中：*Large Sets of* **Hamilton cycle (path) decompositions**

$\lambda K_{n,n} \to H$-cycle	$\lambda \mid ((n-1)!)^2$, even $n \geq 2$ for any λ
$\lambda K_{n,n-1} \to H$-path	odd $n \geq 3$ for even λ
$\lambda K^*_{n,n} \to \vec{H}$-cycle	$\lambda \mid ((n-1)!)^2$
$\lambda K^*_{n,n-1} \to \vec{H}$-path	
$\lambda K_{n,n} \to H$-path	$\lambda \mid (2n-1)((n-1)!)^2,\ (2n-1) \mid \lambda$
$\lambda K^*_{n,n} \to \vec{H}$-path	
$K_{2t+1,2t+1} \setminus F \to H$-cycle	$K_{2t+1,2t} \setminus f \to H$-path

*　无遗留问题

H. Zhao & Q.Kang, 2006

密 码 学

古代加密学

墓碑铭文（古埃及、古希腊）

军用密码本（11世纪，“武经总要”，40个条目）

拉丁文通信密码（1722，被雍正放逐的康熙第九子与其儿子的通信）

专职密码秘书（16世纪末，文艺复兴时期的欧洲）

黑屋（18世纪，欧洲维也纳—秘密内阁办公室，破译拿破仑信件）

40 号房间（一次大战期间，英国曾破译德国 *15000*份电报）

我国的行帮会话……

古典密码体制

文字替换体制

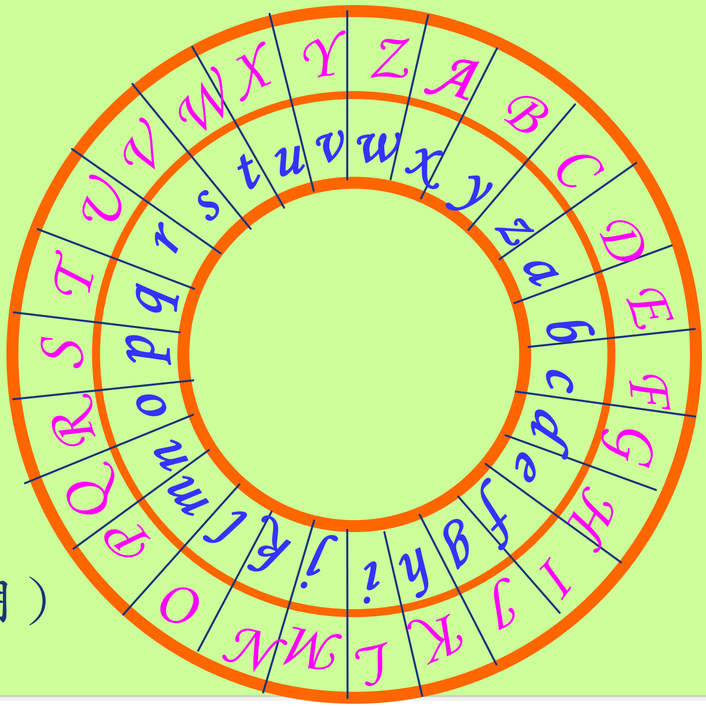
用读法改变文字书写顺序（古希腊的天书）

单字符单表代换（凯撒密码）

单字符多表代换（维吉尼亚密码）

矩阵变换（希尔密码，几何图案改变顺序）

多字符单表代换（漏格板）



机械密码体制

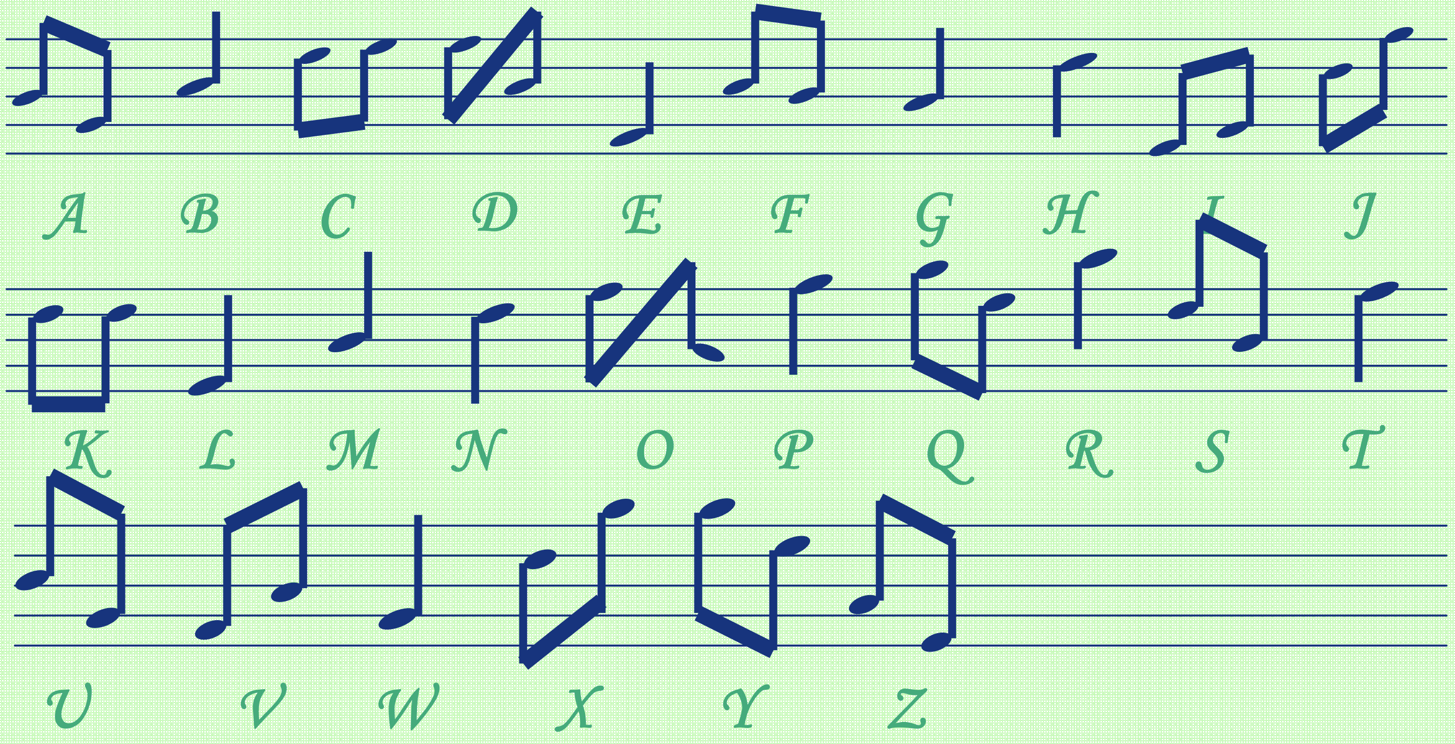
转轮密码机（美国密码之父，*1790*)

*M-209*密码机（二次世界大战中美国陆军使用）

符号替换体制，数字替换体制

电报诞生（*1845*）无线电诞生（*1895*）
无线电通讯在军事上的加密需求
紫密体系的破译（二战中日本“九七式欧文印字机”）
中途岛战役（*1942*）截击山本五十六（*1943.4.18*）

一次大战中间谍使用的五线谱音符



组合数学应用的范例

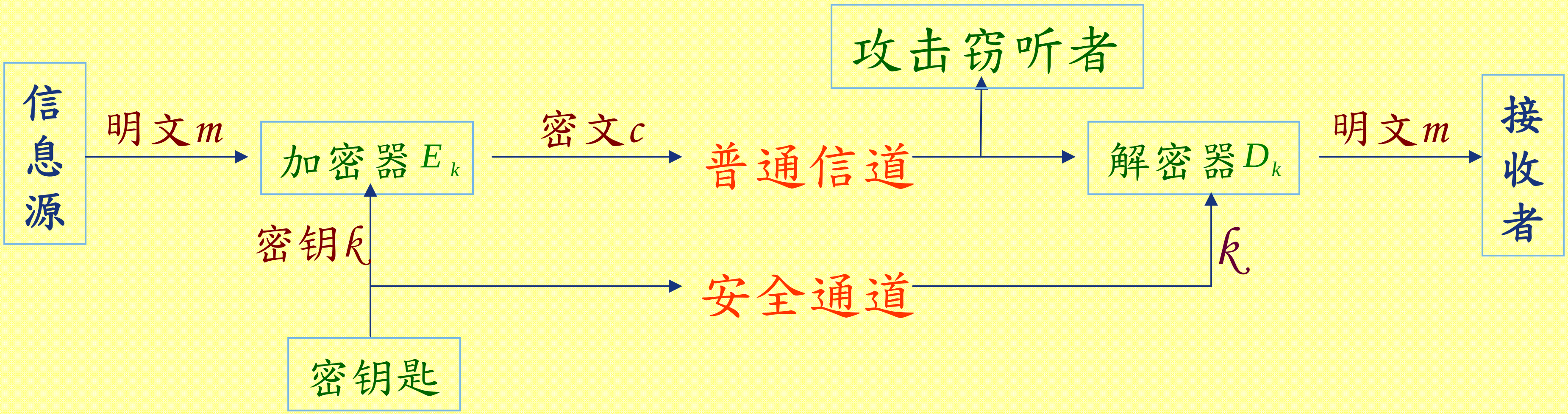
组合数学界的泰斗——

Thomas Tutte

他曾从德军的两条情报密码出发,用组合数学的方法,重建了敌人的密码机,确定了德军密码的内部结构,从而获得了极为重要的情报.对提前结束第二次世界大战作出了突出的贡献.

近代密码体制

Shannon 理论——保密系统的通信理论（*1949*）



- 数据加密标准体制DES（*Data Encryption System*）
- 国际数据加密算法IDEA(*International Data Encryption Algorithm*)
- 公钥密码体制PKC（*Public Key Cryptosystem*）
- *RSA* 体制（*R.L.Rivest*, *A.Shamir*, *L.Adleman* *1978*）
- 背包体制（*Merkle*, *Hellman* *1978*）
- 二次剩余系统（*Goldwasser*, *Micali* *1982*）
- 离散对数系统（*ElGamal* *1985*）
- 椭圆曲线系统，*McEliece* 系统…

Thank You !