

第二届全国组合数学与图论会议

最优 w -示踪码的研究

姓名：马俊

上海交通大学理学院数学系



最优 w -示踪码的研究



§ 1. 研究背景. . .



§ 2. 长为 $w + 1$ 的 w -示踪码的组合性质. . .



§ 3. 极小 $w + 1$ 色 q 元 w -IPP图. . .



§ 4. 长为 $w + 1$ 的最优 w -示踪码的存在性. . .



§ 5. 构造长为 $w + 1$ 的最优 w -示踪码所需算法. . .



1 研究背景

1998年, Hollmann和van Lint等人针对数字指纹的合谋容忍编码问题, 首次提出示踪码(codes with identifiable parents property, IPP)的概念。

2001年, Staddon和Stinson等人将示踪码的概念推广到更一般的情形, 得到 w -示踪码(codes with w -identifiable parents property, w -IPP)的概念。

设 Q 是字母表, C 是一个码。 X 称为码 C 的子码, 如果 X 是 C 的非空子集。 Q^n 中元素 d 称为 C 的子码 X 的后代, 如果对于任何坐标 i , 在 X 中都存在码字 x , 使得 $x_i = d_i$ 。 C 的子码 X 的所有后代组成的集合记作 $desc(X, C)$ 。

设 $d \in Q^n$ 。 码 C 的子码 X 称为 d 的父代集, 如果 $d \in desc(X, C)$ 。 在 C 中, d 的所有元素个数不超过 w 的父代集组成的集合记作 $\mathcal{H}_w(d, C)$ 。

定义. 设 C 是一个 (N, n, q) -码, w 是整数, $w \geq 2$ 。 如果对于任何 $d \in Q^n$, 在 C 中都有或者 $\mathcal{H}_w(d, C) = \emptyset$, 或者

$$\bigcap_{X \in \mathcal{H}_w(d, C)} X \neq \emptyset$$

成立, 那么 C 称为 w -示踪码。

一个例子

设 $w = 2$, $\mathcal{C} = \{(1, 1, 1), (2, 2, 2), (3, 3, 3), (1, 2, 3)\}$ 。

考虑 $d = (1, 2, 2)$, 令 $X_1 = \{(1, 1, 1), (2, 2, 2)\}$, $X_2 = \{(2, 2, 2), (1, 2, 3)\}$ 。

显然, $\mathcal{H}_2(d, \mathcal{C}) = \{X_1, X_2\}$ 。

进一步, 我们有 $\bigcap_{X \in \mathcal{H}_2(d, \mathcal{C})} X = \{(2, 2, 2)\}$ 。

我们可以证明 \mathcal{C} 是一个2-示踪码



人们的研究主要从最优 w -示踪码的性质与构造展开。

设

$$F_w(n, q) = \max\{|C| \mid C \text{ 是长为 } n \text{ 的 } q \text{ 元 } w\text{-示踪码}\}$$

如果 C 是长为 n 的 q 元 w -示踪码, 且 $|C| = F_w(n, q)$, 那么 C 称为长为 n 的 q 元最优 w -示踪码。



(1) 设 $w \geq 2$, $q \leq w$, C 是 (N, n, q) -码, Staddon 和 Stinson 等人指出, 此时, 如果 $N \geq q + 1$, 那么 C 不可能是 w -示踪码。

注意到, 对任意 $w \geq 2$, 长为 n 的 q 元重复码

$$(1, 1, \dots, 1)(2, 2, \dots, 2) \cdots (q, q, \dots, q)$$

总是 w -示踪码。因此, 对于任意 $w \geq 2$ 及 $q \leq w$, $F_w(n, q) = q$

这样, 在本文对最优 w -示踪码的存在性讨论中, 总是假设 $N > q > w$ 。

(2) 当 $w = 2$ 时, Hollmann 等人在 1998 年给出关于长为 n 的 q 元最优 2-示踪码的界: 对于任意 $n \geq 3$, 存在常数 $c > 0$, 使得

$$c\left(\frac{q}{4}\right)^{\lceil \frac{n}{3} \rceil} \leq F_2(n, q) \leq 3q^{\lceil \frac{n}{3} \rceil}$$

(3) 2004 年, Vu Dong Tô 和 Reiheanh 利用图论的方法, 解决了长为 3 的 q 元最优 2-示踪码的存在性问题, 得到比较好的界。

(4) 2004 年, Alon 等人使用概率方法给出长为 $w + 1$ 的 q 元最优 w -示踪码的界: 对任意 $w \geq 2$,

$$F_w(w + 1, q) = \left(\frac{2w - 1}{2w - 3} - o(1)\right)q$$

基于以上的研究现状，我们研究了长为 $w + 1$ 的 w -示踪码。



设 \mathcal{G} 是一个 n -色图。对于 \mathcal{G} 的任何一个顶点 v ，和顶点 v 关联的边上出现的不同颜色的数目称为 v 的色度，并记为 $d_c(v)$ 。

设 G 是 \mathcal{G} 的一个子图， G 称为 \mathcal{G} 的一个 n -模式，如果 G 恰由 \mathcal{G} 中 n 条不同颜色的边组成。

如果存在一个 q 元码 C ，使得 $C^* = \mathcal{G}$ ，那么 \mathcal{G} 称为一个 q 元码图。进一步，如果这个码 C 是 w -示踪码，那么 \mathcal{G} 称为 q 元 w -IPP图。显然地，如果 \mathcal{G} 是 q 元 w -IPP图，那么所有满足 $C^* = \mathcal{G}$ 的码 C 都是 w -示踪码。

\mathcal{G} 的任意一种颜色 i 诱导出的子图记为 $T_i(\mathcal{G})$ 。当 \mathcal{G} 是 q 元码图时，容易发现， $T_i(\mathcal{G})$ 的每一个连通分支都是一个团，这样，把 $T_i(\mathcal{G})$ 中的极大团的数目记为 $\#T_i(\mathcal{G})$ 。显然地， $\#T_i(\mathcal{G}) \leq q$ 。下述定理给出一个 n -色图 \mathcal{G} 是 q 元码图的充分必要条件。

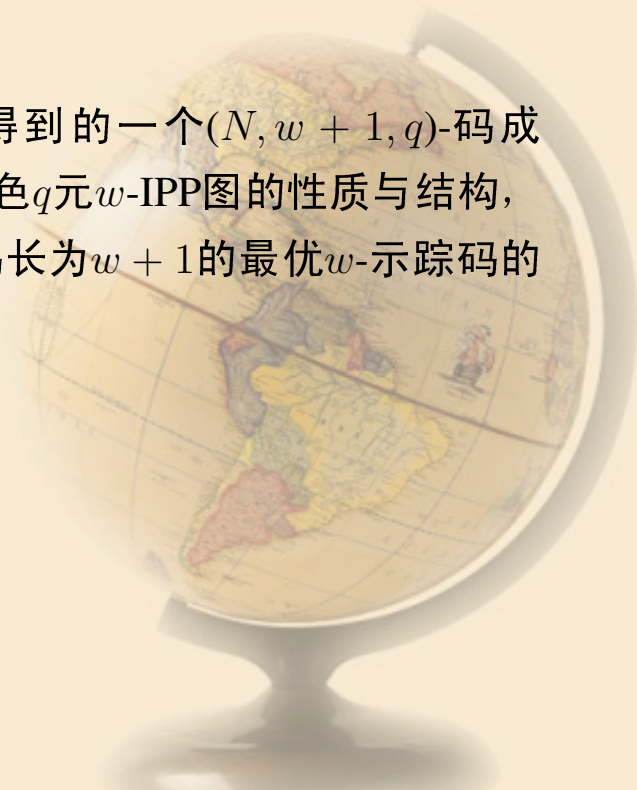
定理. 设 \mathcal{G} 是 n -色图。那么 \mathcal{G} 是 q 元码图的充分必要条件是对于任何颜色 i ， $T_i(\mathcal{G})$ 的每一个连通分支都是一个团，且 $\#T_i(\mathcal{G}) \leq q$ 。

长为 $w + 1$ 的码成为 w -示踪码的充分必要条件

定理. 设 C 是一个 $(N, w + 1, q)$ -码, $N > q$, C^* 是 C 的 n -色图。那么 C 是 w -示踪码的充分必要条件是在 C^* 的任何一个 $(w + 1)$ -模式中, 至多存在一个色度大于 1 的顶点。

2 极小 $w + 1$ 色 q 元 w -IPP图

本论文给出极小 $w + 1$ 色 q 元 w -IPP图的定义，以前面得到的一个 $(N, w + 1, q)$ -码成为 w -示踪码的充分必要条件为基础，详细讨论极小 $w + 1$ 色 q 元 w -IPP图的性质与结构，并给出极小 $w + 1$ 色 q 元 w -IPP图的分类。这为完全解决码长为 $w + 1$ 的最优 w -示踪码的存在性问题创造了条件。



偏序关系 \ll

首先，在所有 q 元 $w + 1$ 色码图组成的集合上给出一个关系 \ll_q 。

设 \mathcal{G}_1 和 \mathcal{G}_2 是两个 q 元 $w + 1$ 色码图。 \mathcal{G}_1 和 \mathcal{G}_2 之间有**关系 \ll_q** ，记为 $\mathcal{G}_1 \ll_q \mathcal{G}_2$ ，如果

(1) 对任何 $i \in \{1, 2, \dots, w + 1\}$ ，都有 $\#T_i(\mathcal{G}_1) \leq \#T_i(\mathcal{G}_2)$ ，

(2) 存在 $i \in \{1, 2, \dots, w + 1\}$ ，使得 $\#T_i(\mathcal{G}_1) < \#T_i(\mathcal{G}_2)$ 。

记 $\mathcal{G}_1 =_q \mathcal{G}_2$ ，如果对于任何的 $i \in \{1, 2, \dots, w + 1\}$ 都有 $\#T_i(\mathcal{G}_1) = \#T_i(\mathcal{G}_2)$ 成立。

设 \mathcal{G} 是 $(w + 1)$ -色图。注意到， \mathcal{G} 可以视为它的连通子图的并，这样， \mathcal{G} 的一个连通子图 \mathcal{P} 称为 **k -色部**，如果 \mathcal{P} 包含 k 种颜色。因此， \mathcal{G} 中的连通子图可分为 $w + 2$ 种类型，其中，0-色部是一个孤立点。如果在 \mathcal{G} 的一个 k -色部中出现的所有不同颜色是 i_1, i_2, \dots, i_k ，那么集合 $\{i_1, i_2, \dots, i_k\}$ 称为这个 k -色部的色型。

然后，在所有 q 元 $w + 1$ 色码图组成的集合上给出一个关系 \prec_q 。

设 \mathcal{G}_1 和 \mathcal{G}_2 是两个 q 元 $w + 1$ 色码图。 \mathcal{G}_1 和 \mathcal{G}_2 之间有**关系 \prec_q** ，记为 $\mathcal{G}_1 \prec_q \mathcal{G}_2$ ，如果 \mathcal{G}_1 中3-色部的个数比 \mathcal{G}_2 中的少。

最后，定义集合

$$\mathcal{L} = \{G \mid G \text{ 是 } q \text{ 元 } w + 1 \text{ 色 } w - \text{IPP 图, 且 } |G| \geq q + 1\}$$

并在 \mathcal{L} 上建立偏序关系 \ll 。

定义. 设 $G_1 \in \mathcal{L}$ 和 $G_2 \in \mathcal{L}$ 。 G_1 和 G_2 之间有 **关系 \ll** ，记为 $G_1 \ll G_2$ ，如果 $G_1 <_q G_2$ ，或者当 $G_1 =_q G_2$ 时， $G_1 \prec_q G_2$ 。

设 $G \in \mathcal{L}$ ，在 \mathcal{L} 中， G 称为 **极小的**，如果对任意 $G' \in \mathcal{L}$ ，都有 $G \ll G'$ 。

极小 w -IPP图 的分类

下面，我们总是用 \mathcal{G} 表示偏序集 (\mathcal{L}, \ll) 中极小 q 元 $w + 1$ 色 w -IPP图。研究 \mathcal{G} 的所具有的性质与结构，我们得到它只能是下面五种类型之一。

类型一. \mathcal{G} 包含一个3-色部；

类型二. \mathcal{G} 包含一个 k -色部，且 $4 \leq k \leq w + 1$ ；

类型三. \mathcal{G} 恰包含一个2-色部；

类型四. \mathcal{G} 恰包含色型分别为 $\{i_1, i_2\}, \{i_1, i_3\}, \dots, \{i_1, i_{k+1}\}$ 的 k 个2-色部，且 $k \geq 2$ ；

类型五. \mathcal{G} 恰包含色型分别为 $\{i_1, i_2\}, \{i_1, i_3\}, \{i_2, i_3\}$ 的3个2-色部。



3 码长为 $w + 1$ 的最优 w -示踪码的存在性

给定码长和最小距离，如何找到具有最多码字个数的码是编码理论中的一个基本问题。

设 C 是码长为 n 的 q 元 w -示踪码，我们知道 C 的最小距离不小于 w 。因此，最优 w -示踪码的存在性问题是有关 w -示踪码的研究的基本问题之一。

码长为3的最优2-示踪码的存在性问题，已由Vu Dong Tô和Reihaneh完全解决。Alon等使用非构造性的概率方法给出了码长为 $w + 1$ 的 q 元最优 w -示踪码的码字个数的界。

本论文使用构造性的方法，完全解决了码长为 $w + 1$ 的 q 元最优 w -示踪码的存在性问题。

$F_w(w + 1, q)$ 的下界

对任意 $q \geq 8w - 5$, 取 $r = \max\{x | (2w - 3)x^2 + 3x + 1 \leq q\}$, 那么 $r \geq 2$, 且 $(2w - 3)r^2 + 3r + 1 \leq q < (2w - 3)(r + 1)^2 + 3(r + 1)$ 。让 $q = (2w - 3)r^2 + 3r + 2(2w - 3)t + s$, 其中, $1 \leq s \leq 2(2w - 3)$ 。容易得到, $0 \leq t \leq r + 1$ 。定义函数 $h(q)$ 如下,

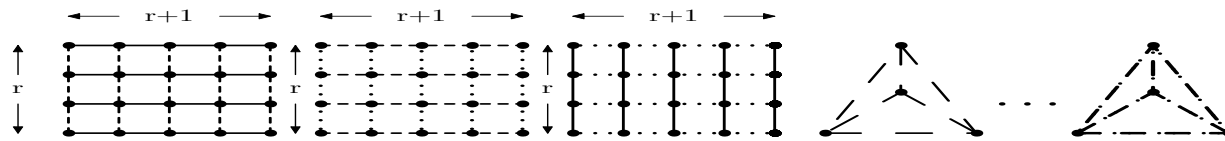
$$h(q) = \begin{cases} 1 & \text{当 } t = 0 \text{ 时,} \\ 2 & \text{当 } 1 \leq t \leq \lfloor \frac{1}{2}(r + 1) \rfloor \text{ 时,} \\ 3 & \text{当 } \lfloor \frac{1}{2}(r + 1) \rfloor + 1 \leq t \leq r + 1. \end{cases}$$

根据函数 $h(q)$ 的取值, 我们给出下面对应的三种构造。

构造一：当 $h(q) = 1$ 时，取 $x = y = z = r$ ， $x' = y' = z' = r + 1$ ，

$$n_i = \begin{cases} r^2 + r & \text{当 } i = 1, 2, 3 \text{ 时,} \\ 2r^2 & \text{当 } 4 \leq i \leq w \text{ 时,} \\ 2r^2 + s - 1 & \text{当 } i = w + 1 \text{。} \end{cases}$$

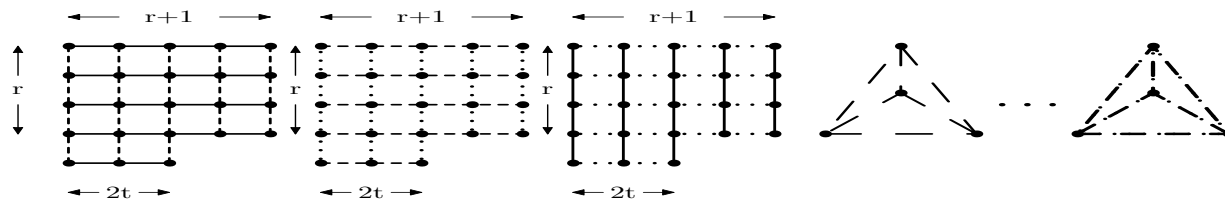
构造如下的图 \mathcal{M}_1 。



构造二：当 $h(q) = 2$ 时，取 $x = y = z = r + 1$ ， $x' = y' = z' = r + 1$ ，

$$n_i = \begin{cases} r^2 + r + 2t & \text{当 } i = 1, 2, 3 \text{ 时,} \\ 2r^2 + 4t & \text{当 } 4 \leq i \leq w \text{ 时,} \\ 2r^2 + 4t + s - 2 & \text{当 } i = w + 1 \text{。} \end{cases}$$

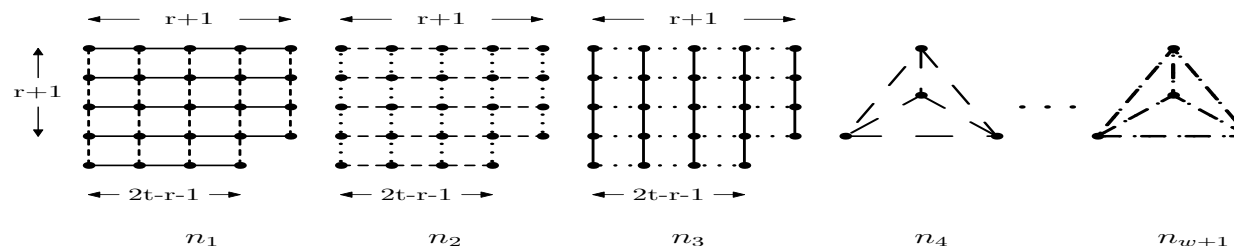
构造如下的图 \mathcal{M}_2 。



构造三：当 $h(q) = 3$ 时，取 $x = y = z = r + 2$ ， $x' = y' = z' = r + 1$ ，

$$n_i = \begin{cases} r^2 + r + 2t & \text{当 } i = 1, 2, 3 \text{ 时,} \\ 2r^2 + 4t & \text{当 } 4 \leq i \leq w \text{ 时,} \\ 2r^2 + 4t + s - 3 & \text{当 } i = w + 1 \text{。} \end{cases}$$

构造如下的图 \mathcal{M}_3 。





引理. 对任意 $q \geq 8w - 5$,

$$F_{w,w+1}(q) \geq |\mathcal{M}_{h(q)}| \geq \frac{2w-1}{2w-3}q^{-7} + \frac{9}{(2w-3)^2} - \frac{6}{2w-3} \sqrt{\frac{q-4(2w-3)}{2w-3} + \frac{9}{4(2w-3)^2}}.$$

当 $q \geq 25w^2$ 时, 我们有

$$\frac{2w-1}{2w-3}q^{-7} + \frac{9}{(2w-3)^2} - \frac{6}{2w-3} \sqrt{\frac{q-4(2w-3)}{2w-3} + \frac{9}{4(2w-3)^2}} > \left[\frac{w}{w-1}q - \frac{w+2}{w-1} \right].$$

这样, 我们得到如下推论。

推论. 对任意 $q \geq 25w^2$,

$$|\mathcal{M}_{h(q)}| > \left[\frac{w}{w-1}q - \frac{w+2}{w-1} \right].$$



定理. 设 $q \geq 25w^2$, 那么 \mathcal{G} 由色型分别为 $\{i_1, i_2\}$, $\{i_2, i_3\}$, $\{i_1, i_3\}$ 的三个2-色部和 $w - 2$ 个1-色部组成, 其中, $w - 2$ 个1-色部的颜色两两不同, 且全都不在三个2-色部中出现。这意味着 \mathcal{G} 是类型五。



$F_{w,w+1}(q)$ 的上界

定义. 设 $q \geq w + 3$ 。 $n_w(q)$ 表示 $\sum_{j=1}^{w+1} n_j$ 的最大值，其中 $n_j (j = 1, 2, \dots, w + 1)$, x, y, z, x', y', z' 是正整数，且满足如下条件：

$$\left\{ \begin{array}{l} x + z' + n_2 + \sum_{j=4}^{w+1} n_j \leq q, \\ y + x' + n_3 + \sum_{j=4}^{w+1} n_j \leq q, \\ z + y' + n_1 + \sum_{j=4}^{w+1} n_j \leq q, \\ \sum_{j=1}^{w+1} n_j - n_i + 1 \leq q \\ n_1 \leq xx', n_2 \leq yy', n_3 \leq zz'. \end{array} \right.$$

当 $4 \leq i \leq w + 1$ 时，

定理. 对任意 $q \geq w + 3$,

$$n_w(q) \leq \frac{2w-1}{2w-3}(q-1) + \frac{9(w-1)}{(2w-3)^2} - \frac{6}{2w-3} \sqrt{\frac{q+2w-1}{2w-3}}.$$

定理. 对任意 $q \geq 25w^2$, $F_w(w + 1, q) = n_w(q)$ 。

定理. 对任意 $q \geq 25w^2$, $|\mathcal{M}_{h(q)}| \leq F_w(w + 1, q) \leq |\mathcal{M}_{h(q)}| + 10$.

定理.

$$F_w(w + 1, q) = \begin{cases} q & \text{当 } 1 \leq q \leq w \text{ 时,} \\ \lfloor \frac{w+1}{w}q - \frac{1}{w} \rfloor & \text{当 } w + 1 \leq q \leq 2w + 1 \text{ 时,} \\ \max \left\{ \lfloor \frac{w+1}{w}q - \frac{1}{w} \rfloor, n_w(q) \right\} & \text{当 } 2w + 2 \leq q \leq w^2 + w \text{ 时,} \\ \max \left\{ \lfloor \frac{w}{w-1}q - \frac{w+2}{w-1} \rfloor, n_w(q) \right\} & \text{当 } w^2 + w + 1 \leq q \leq 25w^2 - 1 \text{ 时,} \\ n_w(q) & \text{当 } q \geq 25w^2 \text{ 时.} \end{cases}$$

4 构造码长 $w + 1$ 的最优 w -示踪码所需的算法

利用下面给出的复杂度为 $O(q^{w+1})$ 的算法，我们能够确定 $n_w(q)$ 及相应的 $n_1, n_2, \dots, n_{w+1}, x, x', y, y', z, z'$ 相应的值。

```

Initialize  $q$  and  $w$ .
Initialize  $Max = |\mathcal{M}_h(q)|$ .
Initialize  $(n_1, n_2, \dots, n_{w+1}, x, x', y, y', z, z') = \text{that of } \mathcal{M}_h(q)$ .
For  $x, x', y, y', z, z' \leftarrow 2$  to  $12w - 17 - \frac{9}{(2w-3)} + 6\sqrt{\frac{q-4(2w-3)}{2w-3} + \frac{9}{4(2w-3)^2}}$ 
{
  For  $n_4, n_5, \dots, n_{w+1} \leftarrow \frac{2}{2w-3}q - 6 + \frac{9}{(2w-3)^2} - \frac{6}{2w-3}\sqrt{\frac{q-4(2w-3)}{2w-3} + \frac{9}{4(2w-3)^2}}$  to  $q$ 
  {
     $n_2 = q - z' - x - \sum_{j=4}^{w+1} n_j$ ,
     $n_3 = q - x' - y - \sum_{j=4}^{w+1} n_j$ ,
     $n_1 = q - y' - z - \sum_{j=4}^{w+1} n_j$  or  $xx'$ .
    IF conditions satisfied, then
    {
      IF  $n_1 + n_2 + n_3 + \sum_{j=4}^{w+1} n_j > max$ , then
      {
         $Max = n_1 + n_2 + n_3 + \sum_{j=4}^{w+1} n_j$ 
        Save  $(n_1, n_2, \dots, n_{w+1}, x, x', y, y', z, z')$ 
      }
    }
  }
}
Output  $F_w(w + 1, q) = Max$ .
Output  $(n_1, n_2, \dots, n_{w+1}, x, x', y, y', z, z')$ .

```



表1

当 $1 \leq q \leq 80$ 时候, $F_3(4, q)$ 和 $|\mathcal{G}_{h(q)}|$ 的值

q	$F_3(4, q)$	$ \mathcal{G}_{h(q)} $	q	$F_3(4, q)$	$ \mathcal{G}_{h(q)} $	q	$F_3(4, q)$	$ \mathcal{G}_{h(q)} $	q	$F_3(4, q)$	$ \mathcal{G}_{h(q)} $
1	1		21	29	28	41	60	58	61	92	92
2	2		22	30	29	42	61	59	62	93	93
3	3		23	32	30	43	63	61	63	94	94
4	5		24	33	31	44	64	62	64	96	95
5	6		25	35	33	45	66	63	65	98	96
6	7		26	36	34	46	68	64	66	99	97
7	9		27	38	35	47	69	65	67	101	99
8	10		28	40	36	48	71	66	68	103	100
9	11		29	41	37	49	73	71	69	104	101
10	13		30	42	38	50	74	72	70	106	102
11	14		31	44	40	51	75	73	71	107	103
12	15		32	46	41	52	77	74	72	109	104
13	17		33	47	42	53	79	75	73	111	109
14	18		34	49	43	54	80	76	74	112	110
15	20		35	50	44	55	82	78	75	114	111
16	21		36	52	45	56	83	79	76	116	112
17	23		37	54	54	57	85	80	77	117	113
18	24		38	55	55	58	87	81	78	118	114
19	26	26	39	57	56	59	88	82	79	120	116
20	27	27	40	58	57	60	90	83	80	122	117



感谢各位老师！
感谢各位同学！