Perfect Hash Families

of Strength Three with Three Rows

R. Fuji-Hara*
University of Tsukuba

What is PHF ?

(k,v)-hash function :　$h : A \to B$

$$|A| = k,\ |B| = v$$

$\mathcal{H}$: a set of (k, v)-hash functions $|\mathcal{H}| = N$

$\mathcal{H}$ is called $PHF(N; k, v, t)$ if

What is PHF？

(k,v)-hash function :　$h : A \to B$

$$|A| = k,\ |B| = v$$

$\mathcal{H}$: a set of (k, v)-hash functions $|\mathcal{H}| = N$

$\mathcal{H}$ is called $PHF(N; k, v, t)$ if

for any $X \subseteq A,\ |X| = t$

there exits at least one $h \in \mathcal{H}$ such that

$h|_X$ is one-to-one

Example 1

$h_i : \mathbb{Z}_{12} \to \mathbb{Z}_4$

k=12,   v=4

	0	1	2	3	4	5	6	7	8	9	10	11
h_1	0	0	0	1	1	1	2	2	2	3	3	3
h_2	3	0	2	1	2	3	1	0	3	2	0	1
h_3	2	1	3	0	2	1	1	2	3	0	0	3

Example 1

$h_i : \mathbb{Z}_{12} \to \mathbb{Z}_4$

k=12,   v=4

	0	1	2	3	4	5	6	7	8	9	10	11
h_1	0	0	0	1	1	1	2	2	2	3	3	3
h_2	3	0	2	1	2	3	1	0	3	2	0	1
h_3	2	1	3	0	2	1	1	2	3	0	0	3

Example 1

$h_i : \mathbb{Z}_{12} \to \mathbb{Z}_4$

k=12,   v=4

$PHF(3; 12, 4, 2)$

	0	1	2	3	4	5	6	7	8	9	10	11
h_1	0	0	0	1	1	1	2	2	2	3	3	3
h_2	3	0	2	1	2	3	1	0	3	2	0	1
h_3	2	1	3	0	2	1	1	2	3	0	0	3

Applications

- Fast Retrieval of Frequently Used Data (Compact Storage)
- Secure Frame Proof Code (Finger Printing)
- Key Distribution Patterns
- Broadcast Encryption
- Threshold Cryptography
- Group Testing

Bounds

PHFN(k,v,t) : the smallest N for which a PHF(N;,k,v,t) exists

$$\text{There is a PHF}(N;k,v,2) \text{ iff } k \leq v^N$$

$$\text{PHFN}(k,v,2) = \lceil \log_v k \rceil$$

Mehlhorn(1982)

$$PHFN(k,v,t) \geq \frac{\log k}{\log v}$$

Fredman and Komlos(1984)

$$PHFN(k,v,t) \geq \frac{\binom{k-1}{t-1} v^{t-2} \log(k-t+2)}{\binom{v-1}{t-2} k^{t-2} \log(v-t+2)}$$

Points and Blocks

$$h_i : A \to B$$

$$|A| = k,\ |B| = v$$

Point Set : Domain of the functions h_i

Blocks : $$B_{i,b} = \{a \mid h_i(a) = b,\},$$
$$b \in B,\ 1 \leq i \leq |\mathcal{H}|$$

Example 2

	0	1	2	3	4	5	6	7	8	9	10	11
h_1	0	0	0	1	1	1	2	2	2	3	3	3
h_2	3	0	2	1	2	3	1	0	3	2	0	1
h_3	2	1	3	0	2	1	1	2	3	0	0	3

$$B_{1,0} = \{0,1,2\},\ B_{1,1} = \{3,4,5\},\ B_{1,2} = \{6,7,8\},\ B_{1,3} = \{9,10,11\}$$

$$B_{2,0} = \{1,7,10\},\ B_{2,1} = \{3,6,11\},\ B_{2,2} = \{2,4,9\},\ B_{2,3} = \{0,5,8\}$$

$$B_{3,0} = \{3,9,10\},\ B_{3,1} = \{1,5,6\},\ B_{3,2} = \{0,4,7\},\ B_{3,3} = \{2,8,11\}$$

t-Separating Resolvable Block Design (t-SRBD)

(defined by Atici, Magliveras, Stinson and Wei)

1. A is a finite set (*points*)

2. Π is a set of parallel classes (the members of a classe are called *blocks*)

3. For any t-subset X of A, there exists a parallel class π such that the t points in X occur in t different blocks of π

Theorem

There exists a $\mathrm{PHF}(N; k, v, t)$ if and only if there exists t-$\mathrm{SRBD}(k, b, N, v)$,

where $|A| = k$

$|\Pi| = N$

b: the number of blocks

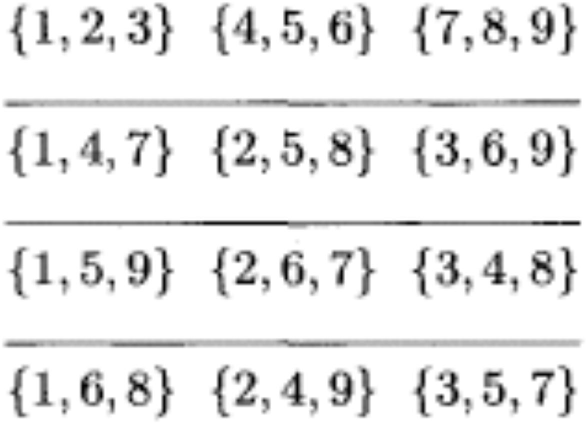
$v = \max\{|\pi| : \pi \in \Pi\}$

from Resolvable BIBD

Theorem (Atici, Magliveras, Stinson and Wei,1996)

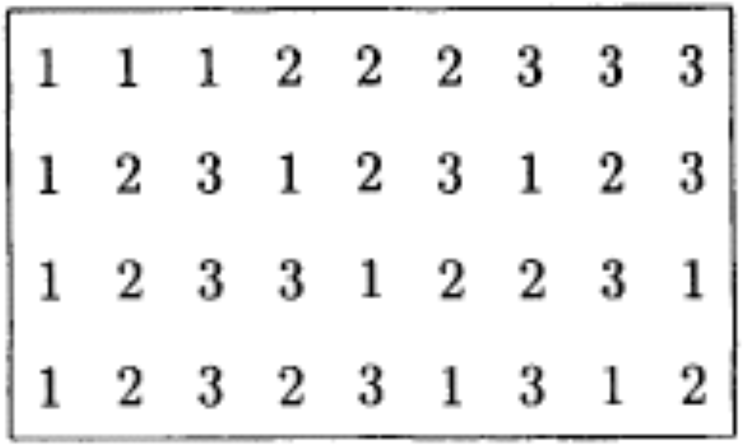
If there exists a resolvable (v,b,r,k,λ)BIBD, then there exists a PHF$(N; v, v/k, t)$, where $r \geq N > \lambda\binom{t}{2}$

Resolvable (9,12,4,3,1)BIBD



1	2	3
$\{1,2,3\}$	$\{4,5,6\}$	$\{7,8,9\}$
$\{1,4,7\}$	$\{2,5,8\}$	$\{3,6,9\}$
$\{1,5,9\}$	$\{2,6,7\}$	$\{3,4,8\}$
$\{1,6,8\}$	$\{2,4,9\}$	$\{3,5,7\}$

PHF(4; 9,3,3)



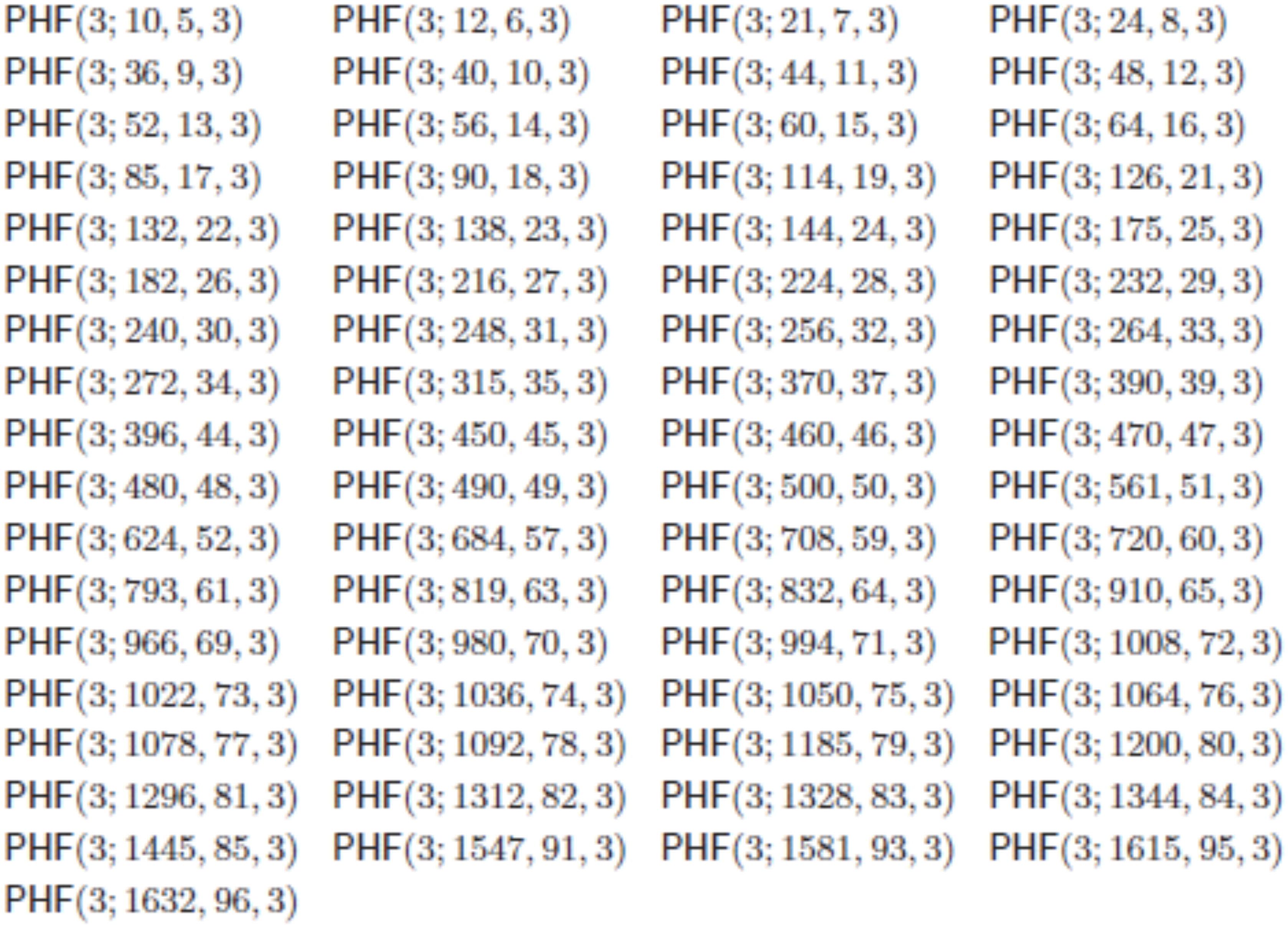
1	2	3	4	5	6	7	8	9
1	1	1	2	2	2	3	3	3
1	2	3	1	2	3	1	2	3
1	2	3	3	1	2	2	3	1
1	2	3	2	3	1	3	1	2

Strength Three with Three Rows

The smallest nontrivial case

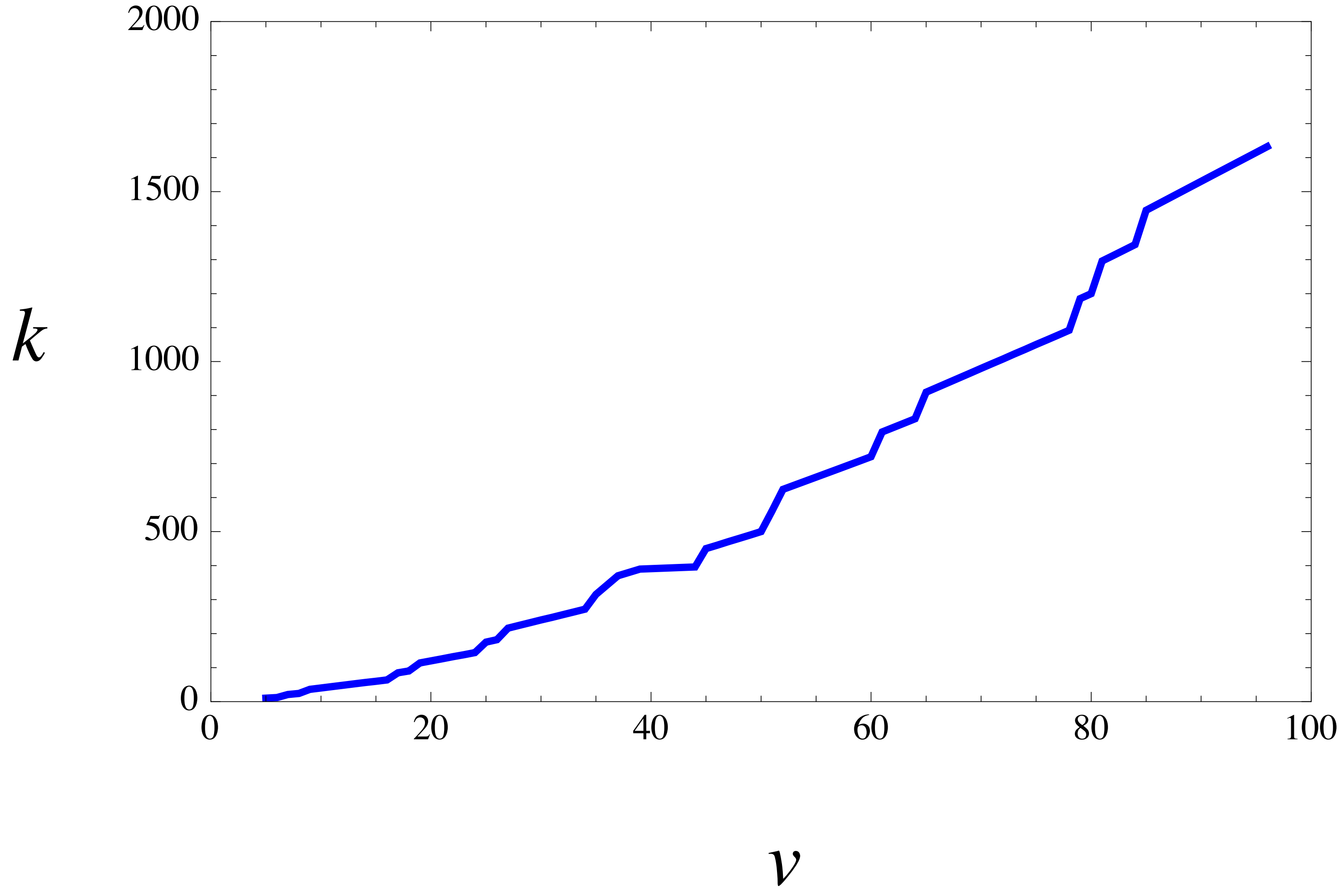
The table by Walker II and Colbourn

(Perfect Hash Families: Constructions and Existence, J. of Math, Crypto. , 2007)

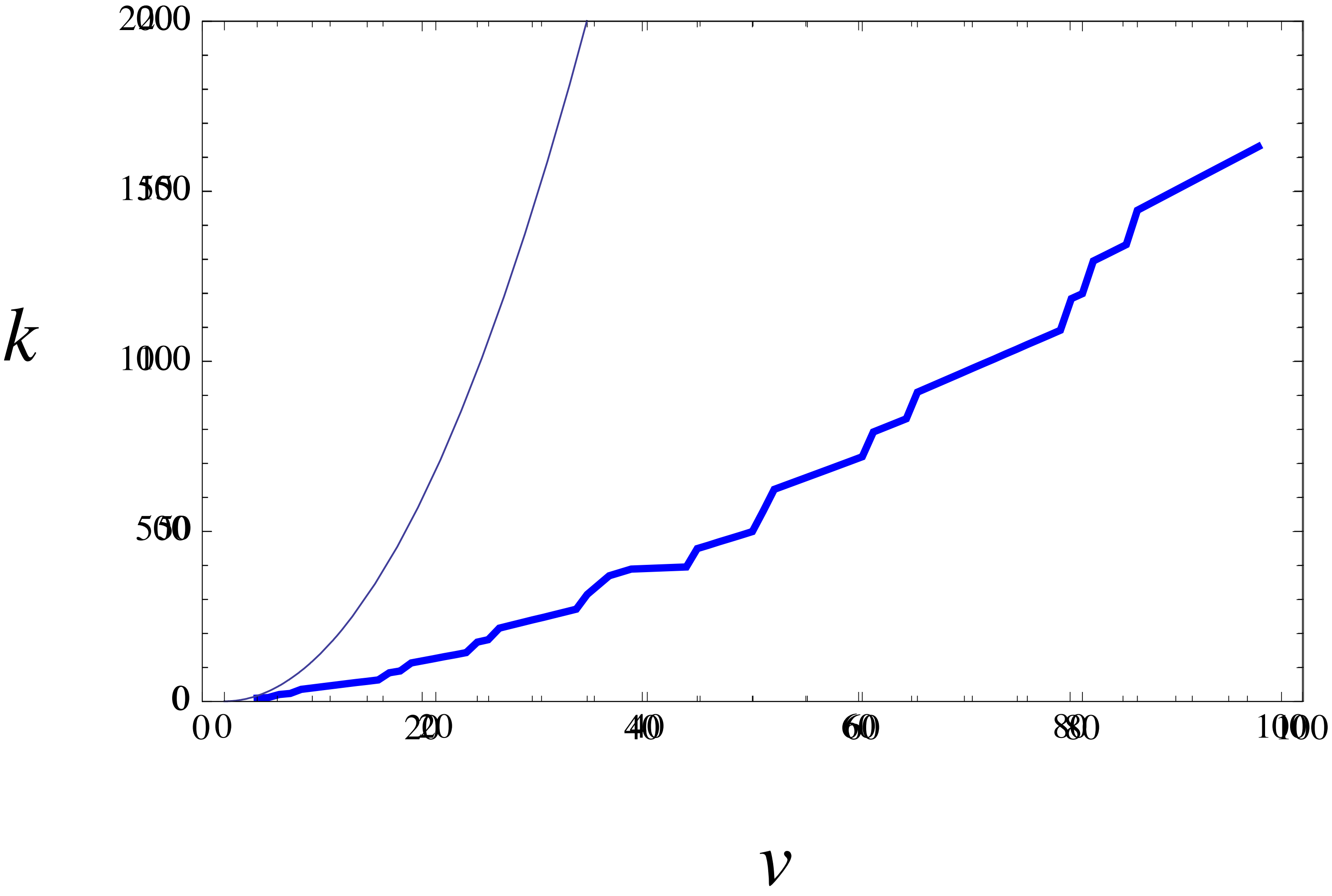


$\mathsf{PHF}(3; 10, 5, 3)$ $\mathsf{PHF}(3; 12, 6, 3)$ $\mathsf{PHF}(3; 21, 7, 3)$ $\mathsf{PHF}(3; 24, 8, 3)$
$\mathsf{PHF}(3; 36, 9, 3)$ $\mathsf{PHF}(3; 40, 10, 3)$ $\mathsf{PHF}(3; 44, 11, 3)$ $\mathsf{PHF}(3; 48, 12, 3)$
$\mathsf{PHF}(3; 52, 13, 3)$ $\mathsf{PHF}(3; 56, 14, 3)$ $\mathsf{PHF}(3; 60, 15, 3)$ $\mathsf{PHF}(3; 64, 16, 3)$
$\mathsf{PHF}(3; 85, 17, 3)$ $\mathsf{PHF}(3; 90, 18, 3)$ $\mathsf{PHF}(3; 114, 19, 3)$ $\mathsf{PHF}(3; 126, 21, 3)$
$\mathsf{PHF}(3; 132, 22, 3)$ $\mathsf{PHF}(3; 138, 23, 3)$ $\mathsf{PHF}(3; 144, 24, 3)$ $\mathsf{PHF}(3; 175, 25, 3)$
$\mathsf{PHF}(3; 182, 26, 3)$ $\mathsf{PHF}(3; 216, 27, 3)$ $\mathsf{PHF}(3; 224, 28, 3)$ $\mathsf{PHF}(3; 232, 29, 3)$
$\mathsf{PHF}(3; 240, 30, 3)$ $\mathsf{PHF}(3; 248, 31, 3)$ $\mathsf{PHF}(3; 256, 32, 3)$ $\mathsf{PHF}(3; 264, 33, 3)$
$\mathsf{PHF}(3; 272, 34, 3)$ $\mathsf{PHF}(3; 315, 35, 3)$ $\mathsf{PHF}(3; 370, 37, 3)$ $\mathsf{PHF}(3; 390, 39, 3)$
$\mathsf{PHF}(3; 396, 44, 3)$ $\mathsf{PHF}(3; 450, 45, 3)$ $\mathsf{PHF}(3; 460, 46, 3)$ $\mathsf{PHF}(3; 470, 47, 3)$
$\mathsf{PHF}(3; 480, 48, 3)$ $\mathsf{PHF}(3; 490, 49, 3)$ $\mathsf{PHF}(3; 500, 50, 3)$ $\mathsf{PHF}(3; 561, 51, 3)$
$\mathsf{PHF}(3; 624, 52, 3)$ $\mathsf{PHF}(3; 684, 57, 3)$ $\mathsf{PHF}(3; 708, 59, 3)$ $\mathsf{PHF}(3; 720, 60, 3)$
$\mathsf{PHF}(3; 793, 61, 3)$ $\mathsf{PHF}(3; 819, 63, 3)$ $\mathsf{PHF}(3; 832, 64, 3)$ $\mathsf{PHF}(3; 910, 65, 3)$
$\mathsf{PHF}(3; 966, 69, 3)$ $\mathsf{PHF}(3; 980, 70, 3)$ $\mathsf{PHF}(3; 994, 71, 3)$ $\mathsf{PHF}(3; 1008, 72, 3)$
$\mathsf{PHF}(3; 1022, 73, 3)$ $\mathsf{PHF}(3; 1036, 74, 3)$ $\mathsf{PHF}(3; 1050, 75, 3)$ $\mathsf{PHF}(3; 1064, 76, 3)$
$\mathsf{PHF}(3; 1078, 77, 3)$ $\mathsf{PHF}(3; 1092, 78, 3)$ $\mathsf{PHF}(3; 1185, 79, 3)$ $\mathsf{PHF}(3; 1200, 80, 3)$
$\mathsf{PHF}(3; 1296, 81, 3)$ $\mathsf{PHF}(3; 1312, 82, 3)$ $\mathsf{PHF}(3; 1328, 83, 3)$ $\mathsf{PHF}(3; 1344, 84, 3)$
$\mathsf{PHF}(3; 1445, 85, 3)$ $\mathsf{PHF}(3; 1547, 91, 3)$ $\mathsf{PHF}(3; 1581, 93, 3)$ $\mathsf{PHF}(3; 1615, 95, 3)$
$\mathsf{PHF}(3; 1632, 96, 3)$

$k \leq v^3$?



$k \leq v^3$?



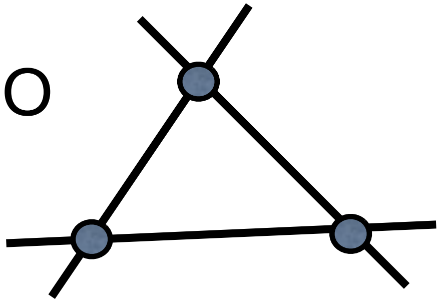
trrls (Walker II and Colbourn)

(triangle-free 3-regular resolvable linear space)

Linear space : no pair occurs in more than one block

3-regular = 3 resolution classes

triangle-free : No



Theorem (Walker II and Colbourn)

If there exists a trrls, then there exists a PHF of strength 3 with 3 rows

More General Condition

For a subset X of A, if a block meets X in at least two points then it is called a *secant block to X* .

1. points (k) and blocks
2. three resolution classes (containing at most v blocks)
3.

More General Condition

For a subset X of A, if a block meets X in at least two points then it is called a *secant block to X* .

1. points (k) and blocks
2. three resolution classes (containing at most v blocks)
3. there is no 3-subset X of A such that there are three secant blocks to X

More General Condition

For a subset X of A, if a block meets X in at least two points then it is called a *secant block to X* .

1. points (k) and blocks
2. three resolution classes (containing at most v blocks)
3. there is no 3-subset X of A such that there are three secant blocks to X

This system is equivalent to PHF(3; k,v,3)

Constructions

using

- Quadrics in PG(4,q)
- Hermitian Varieties in PG(3,q^2)

Quadrics in PG(4,q), Q(4,q)

$P = (x_0, x_1, x_2, x_3, x_4)$ point of PG(4,q)

$x_0^2 + x_1 x_2 + x_3 x_4 = 0$ (canonical form)

$(q^2+1)(q+1)$ points of PG(4,q)

$(q^2+1)(q+1)$ lines of PG(4,q)

This quadric is a linear space and triangle-free (Generalized Quadrangle)

Does there exist a parallel class in Q(4,q) ?

(mutually disjoint q^2+1 lines)

Does there exist a parallel class in Q(4,q) ?

(mutually disjoint q^2+1 lines)

Result of exhaustive search for PG(4,3):

Does there exist a parallel class in Q(4,q) ?

(mutually disjoint q^2+1 lines)

Result of exhaustive search for PG(4,3):

The maximum number of mutually disjoint lines (expecting 10 lines) is

Does there exist a parallel class in Q(4,q) ?

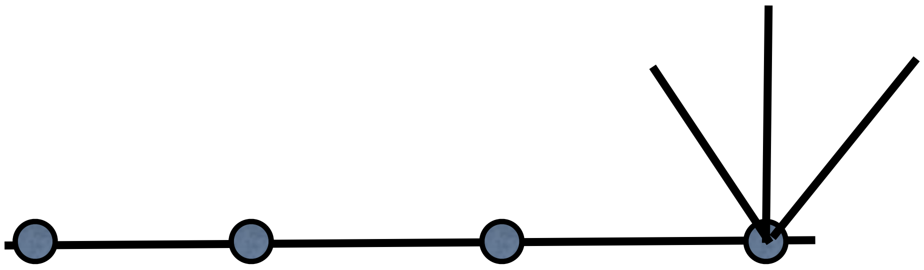
(mutually disjoint q^2+1 lines)

Result of exhaustive search for PG(4,3):

The maximum number of mutually disjoint lines (expecting 10 lines) is

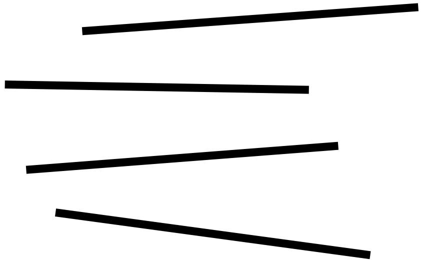
7

Q(4,q)

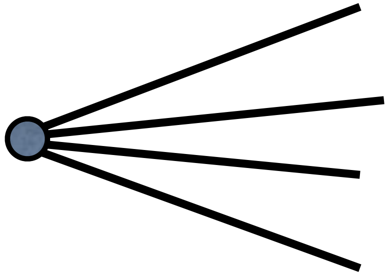


q+1 points on a line
q+1 lines at a point

$Q(4,q)^*$: Dual of Q(4,q)

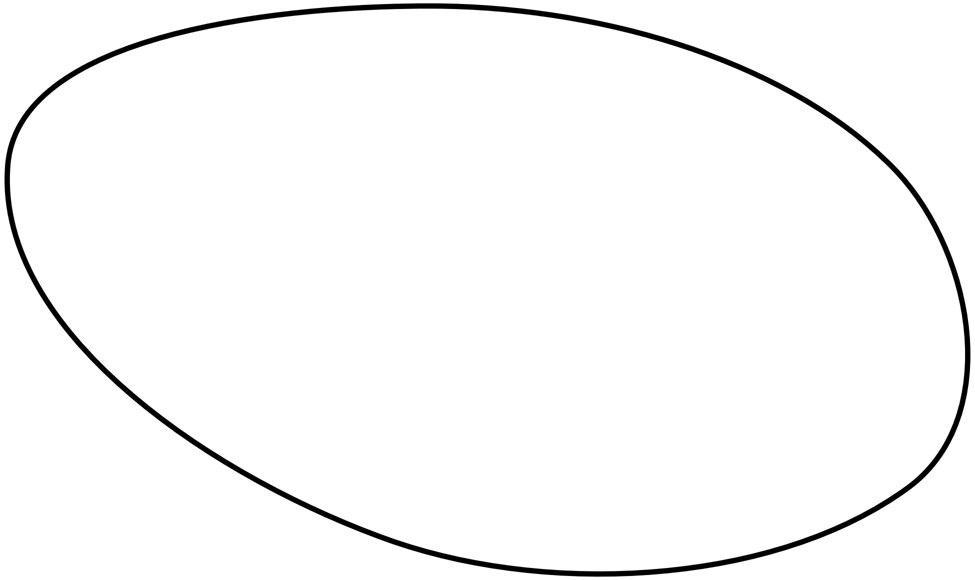


Points

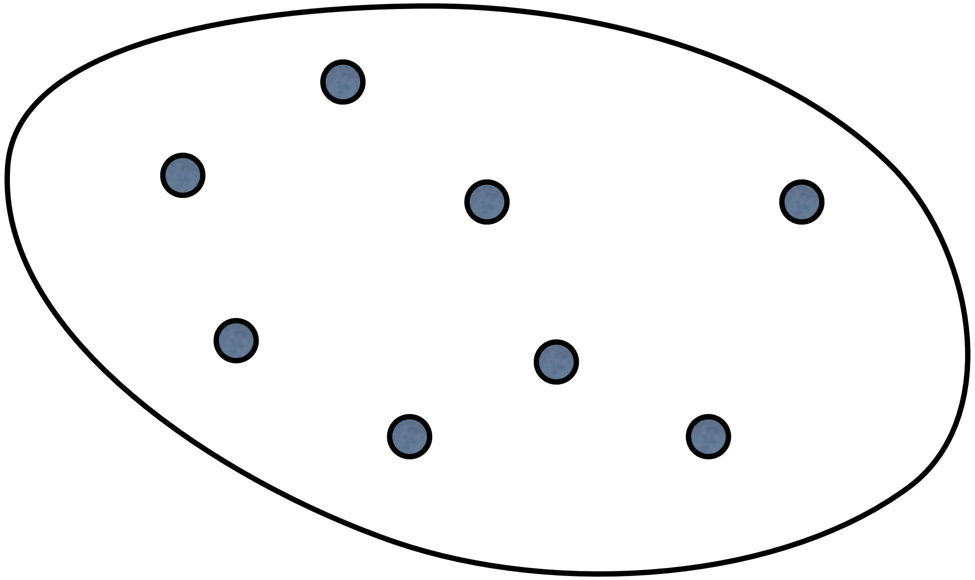


Block (cone)

A hyperplane of PG(4,q)



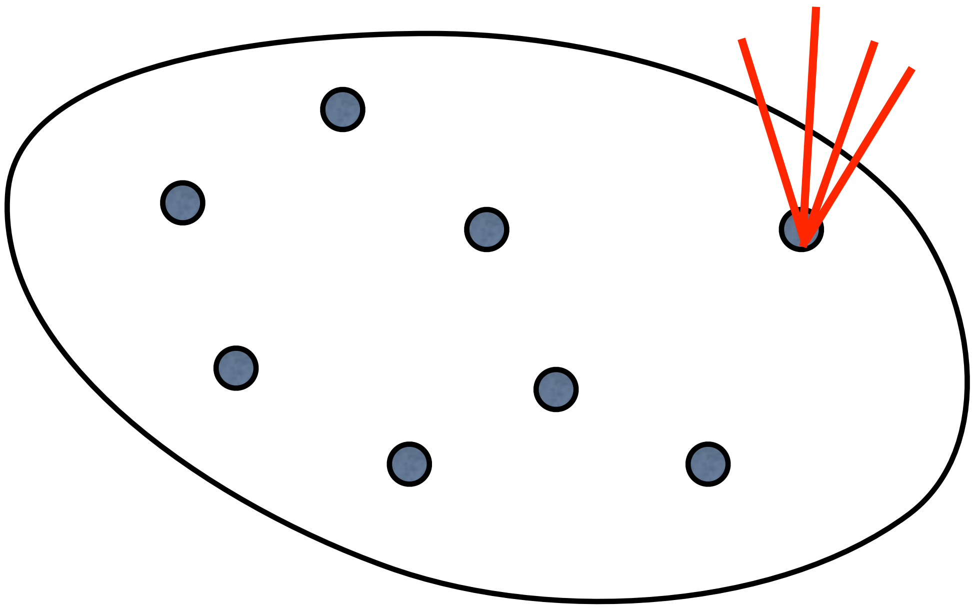
A hyperplane of PG(4,q)



Q(3,q): q^2+1 points,

no three points are collinear

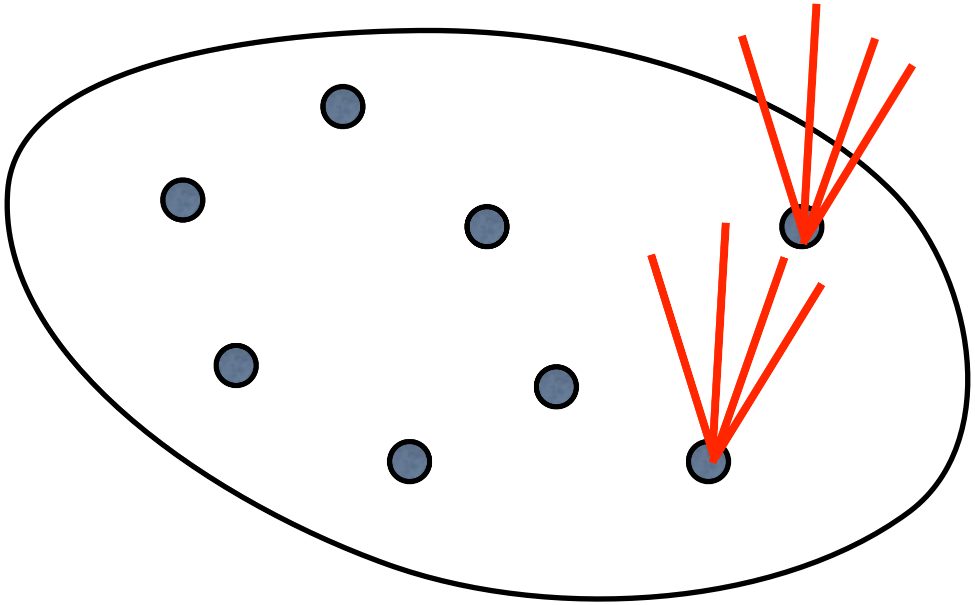
A hyperplane of PG(4,q)



Q(3,q): q^2+1 points,

no three points are collinear

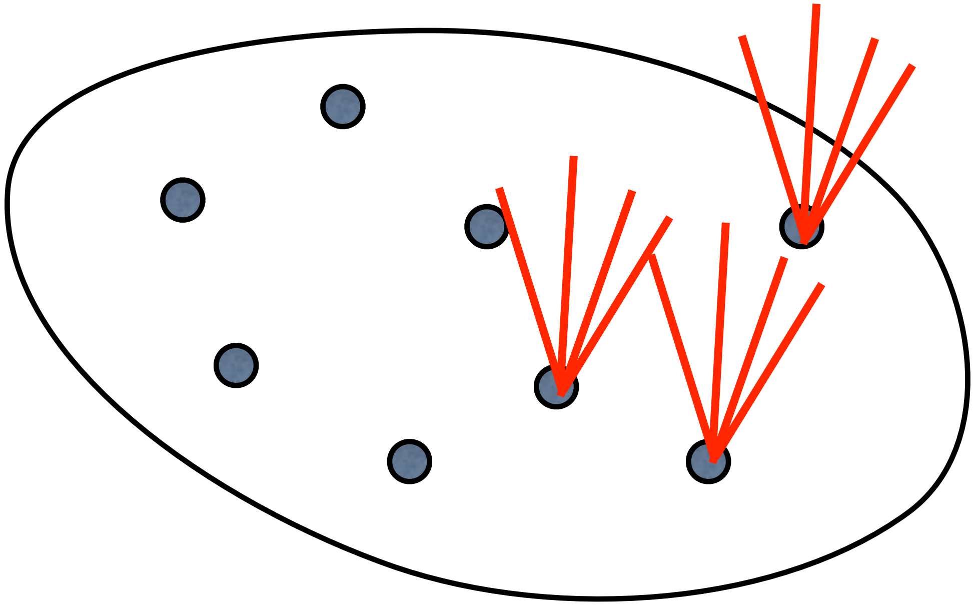
A hyperplane of PG(4,q)



Q(3,q): q^2+1 points,

no three points are collinear

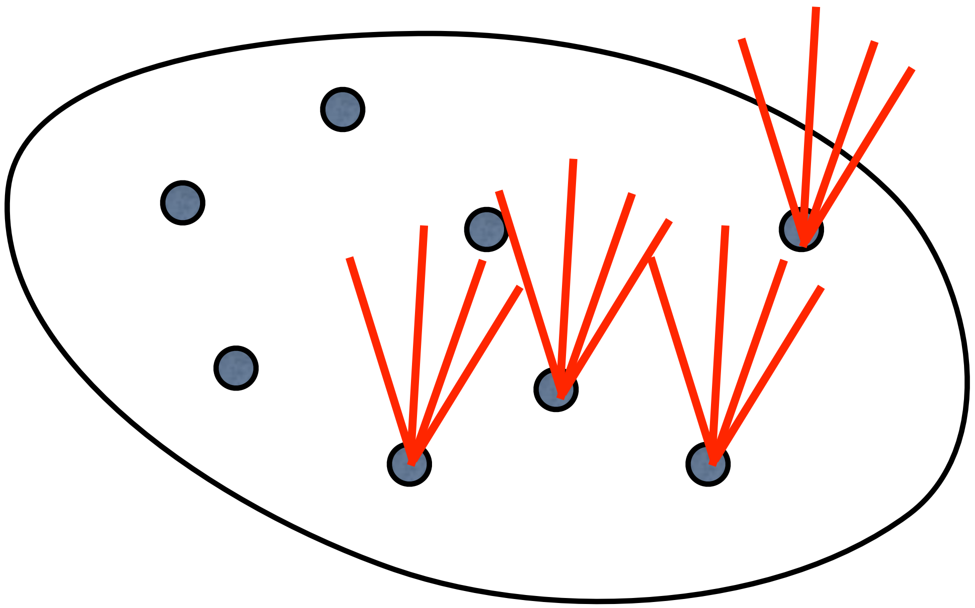
A hyperplane of PG(4,q)



Q(3,q): q^2+1 points,

no three points are collinear

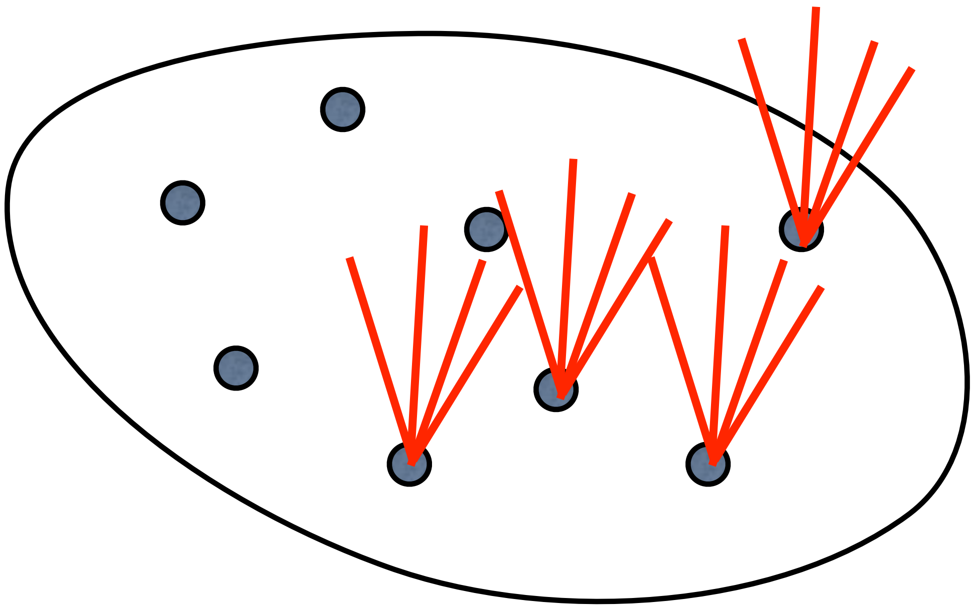
A hyperplane of PG(4,q)



Q(3,q): q^2+1 points,

no three points are collinear

A hyperplane of PG(4,q)

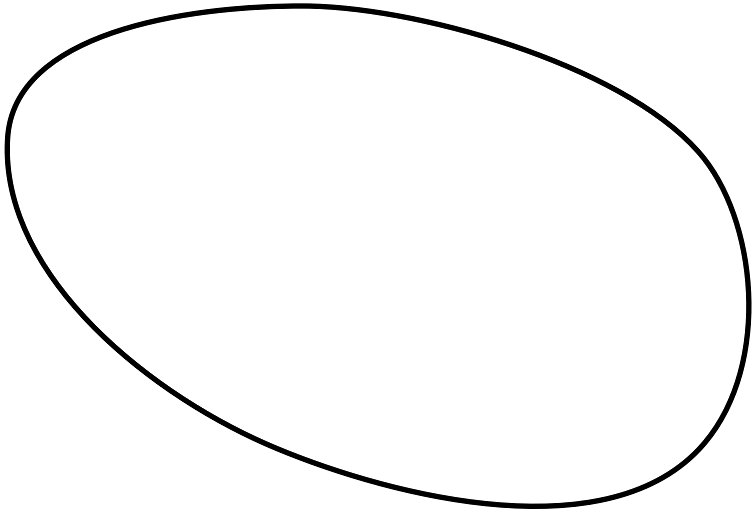


Q(3,q): q^2+1 points,

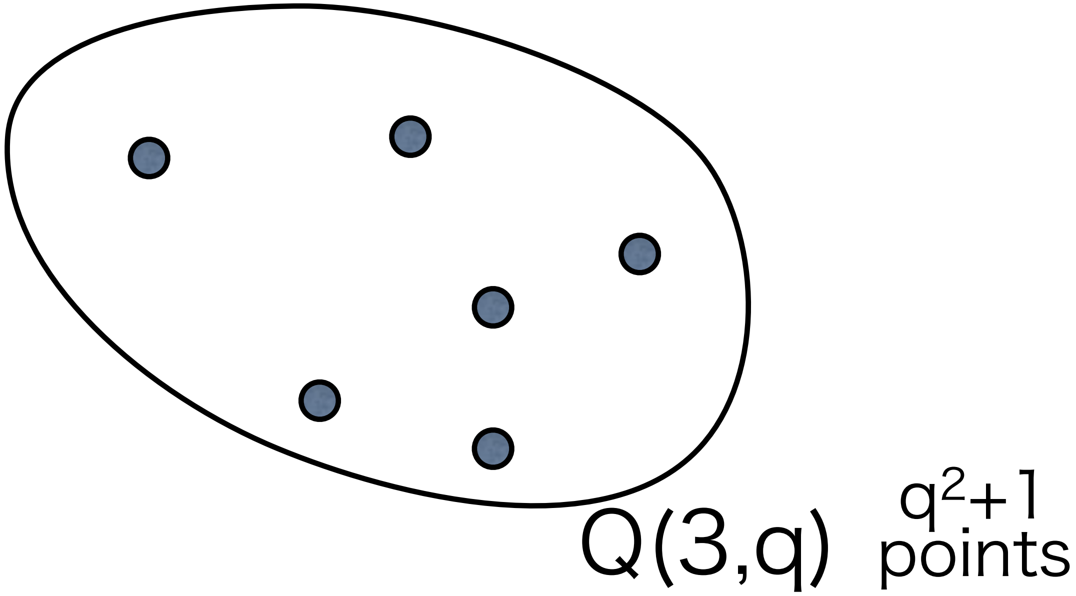
no three points are collinear

A spread of Q(4,q)*

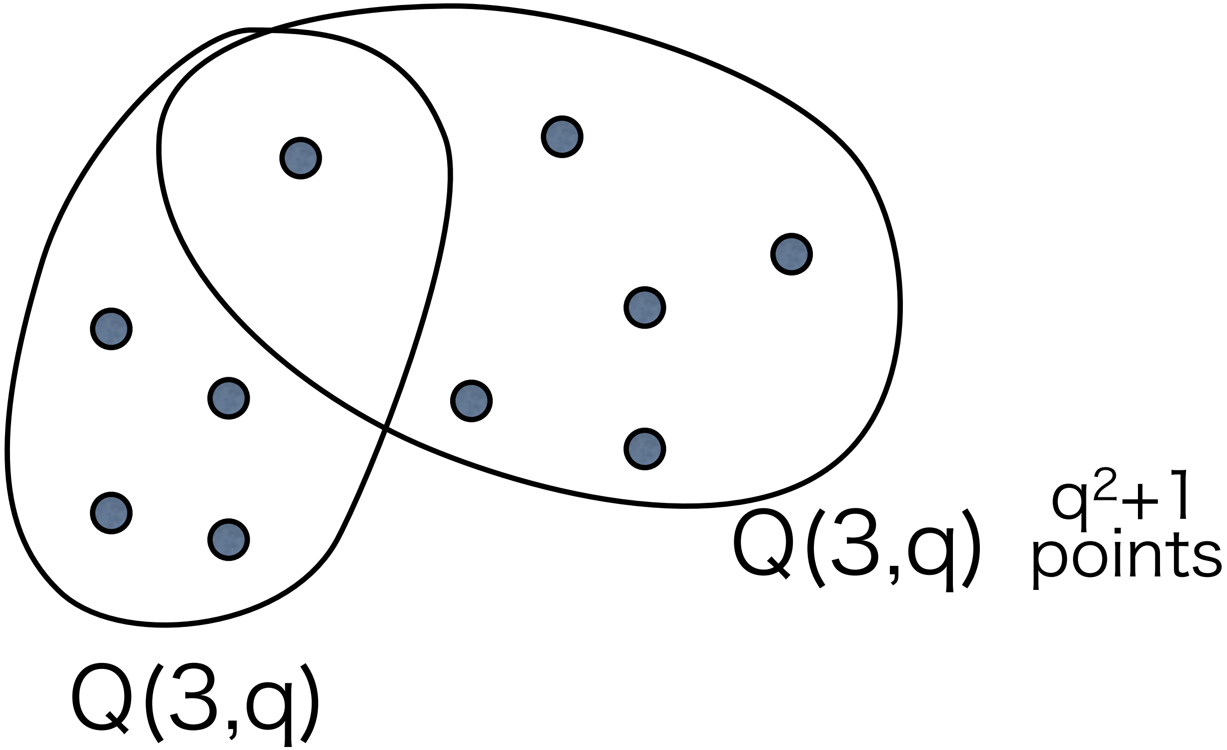
Hyperplanes containing a plane



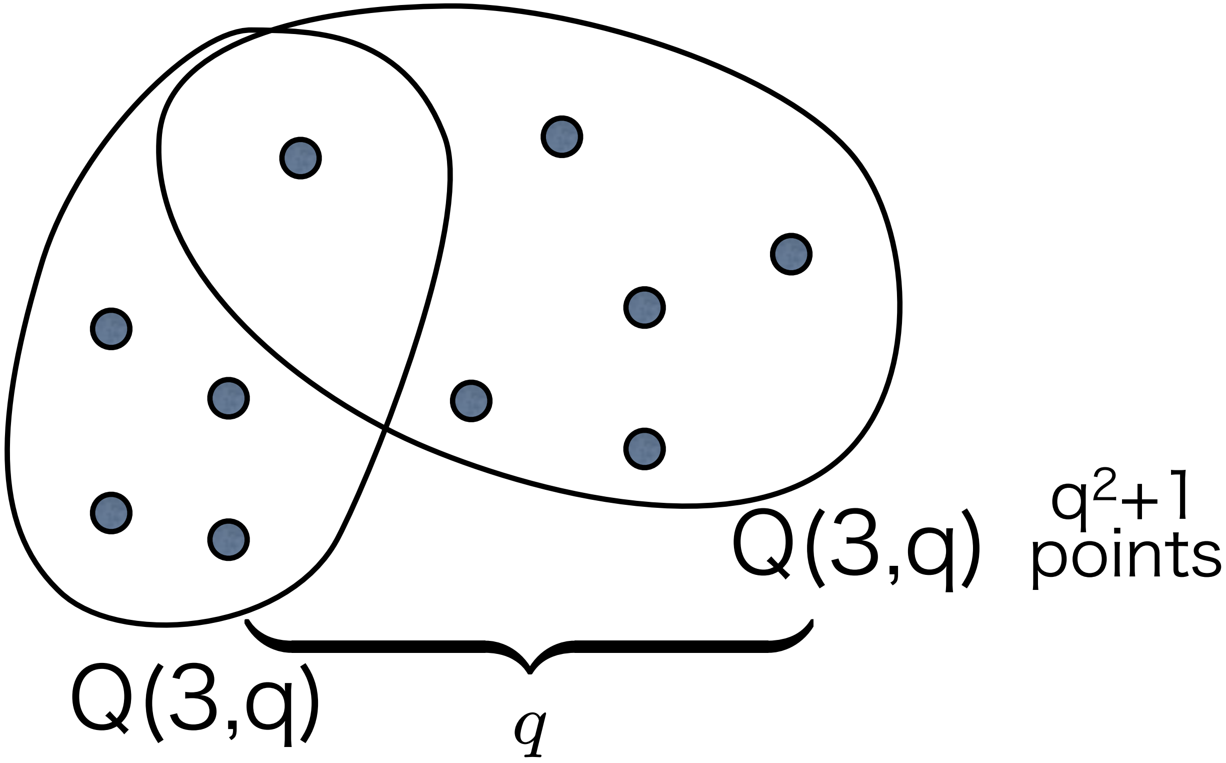
Hyperplanes containing a plane



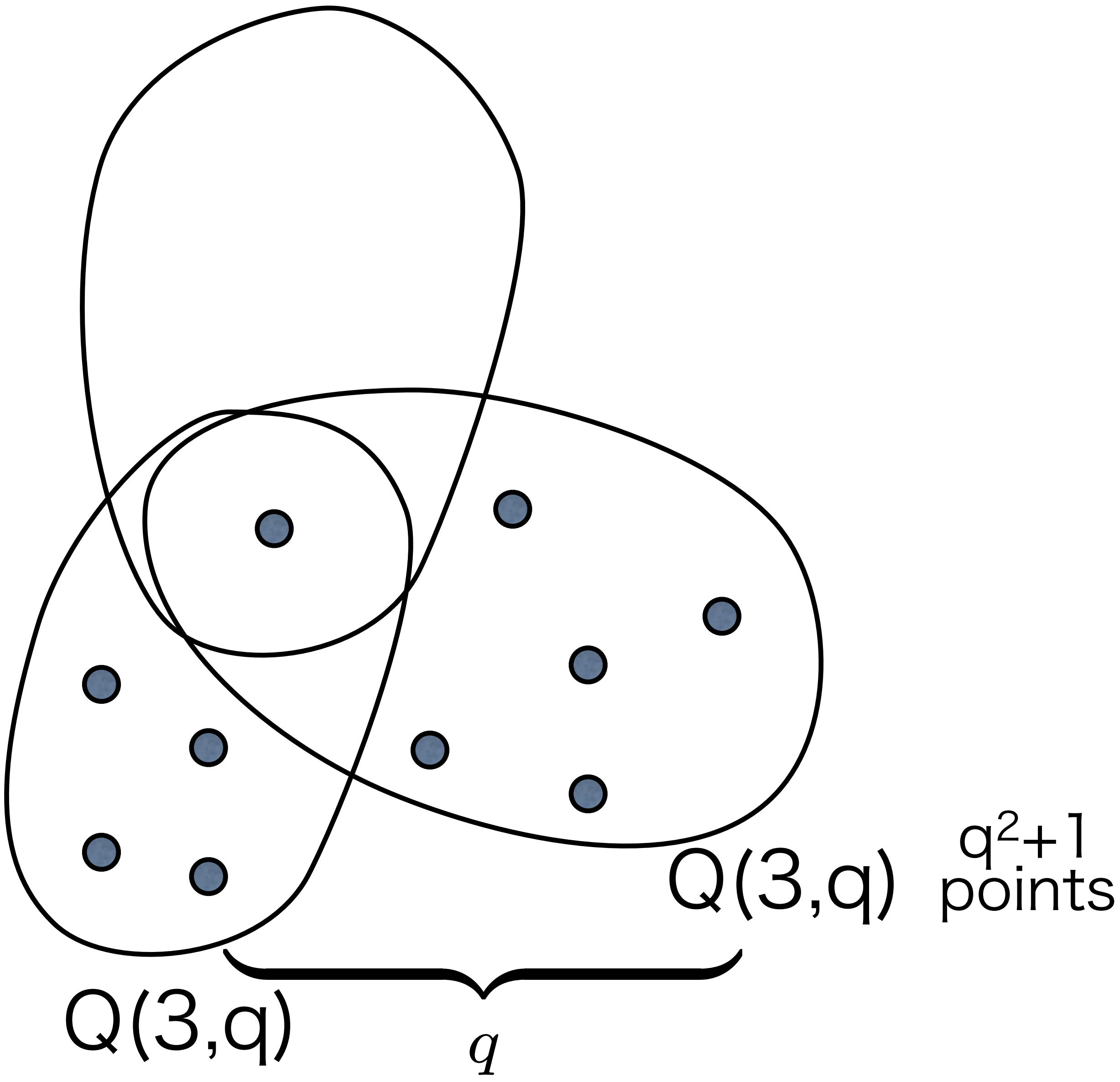
Hyperplanes containing a plane



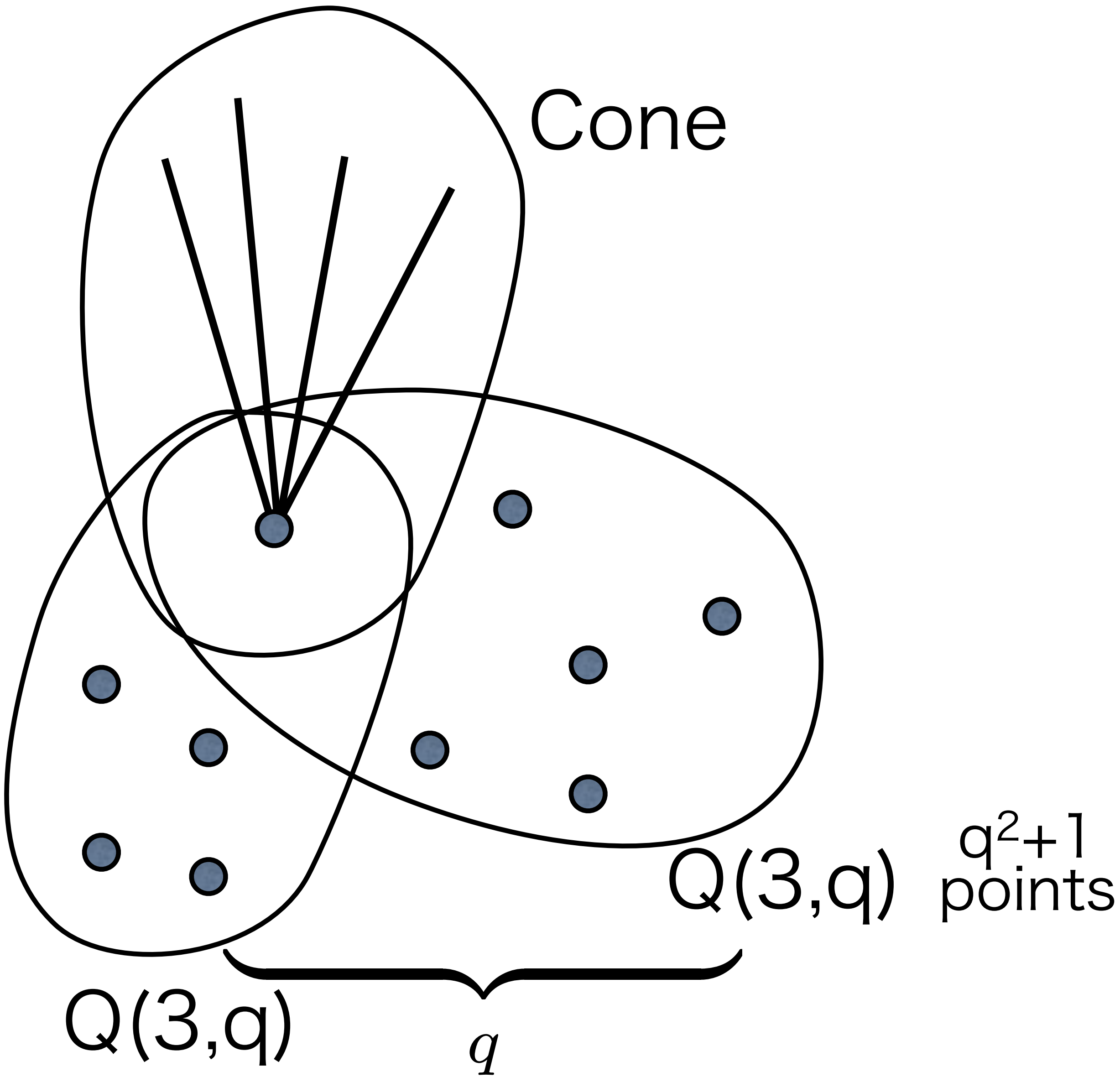
Hyperplanes containing a plane



Hyperplanes containing a plane



Hyperplanes containing a plane



$Q(4,q)^* \setminus C_0$

C_0 : a cone

$q^2(q+1)$ points

q^2 blocks in a parallel class

q parallel classes

Theorem

There exists a PHF(3, $q^2(q+1)$, q^2, 3) for any prime power q , $q \geq 3$.

The Number of Columns k

$v=q^2$	W&C	Q(4,q)*
9	36	36
16	64	80
25	175	150
49	490	392
64	832	576
81	1296	810

Hermitian Varieties in PG(3,q^2), H(3,q^2)

$$x_0^{q+1}+x_1^{q+1}+x_2^{q+1}+x_3^{q+1}=0$$

(q^2+1)(q^3+1) points

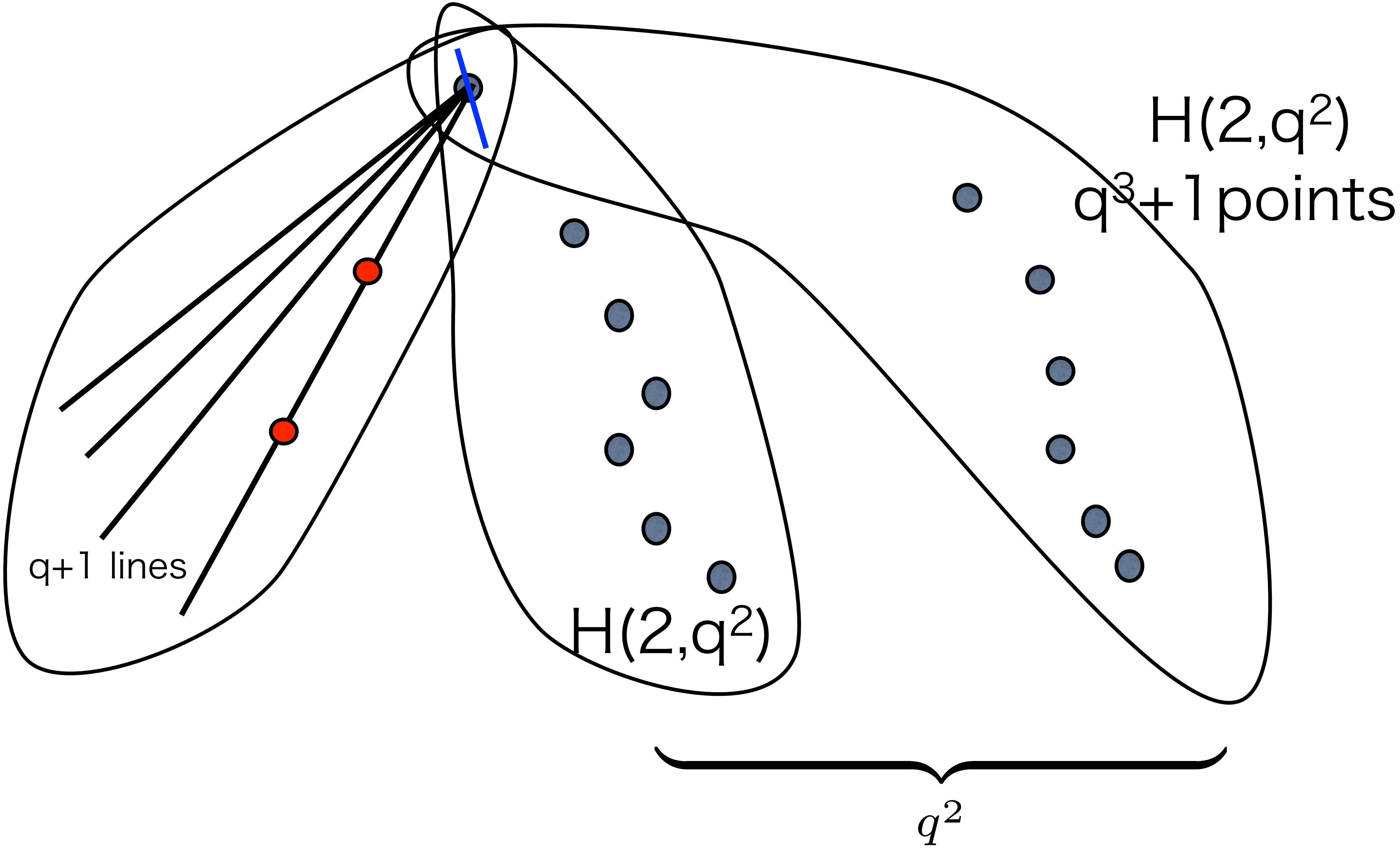
(q+1)(q^3+1) lines

q^2+1 points on a line, q+1 lines at a point

linear space and triangle-free

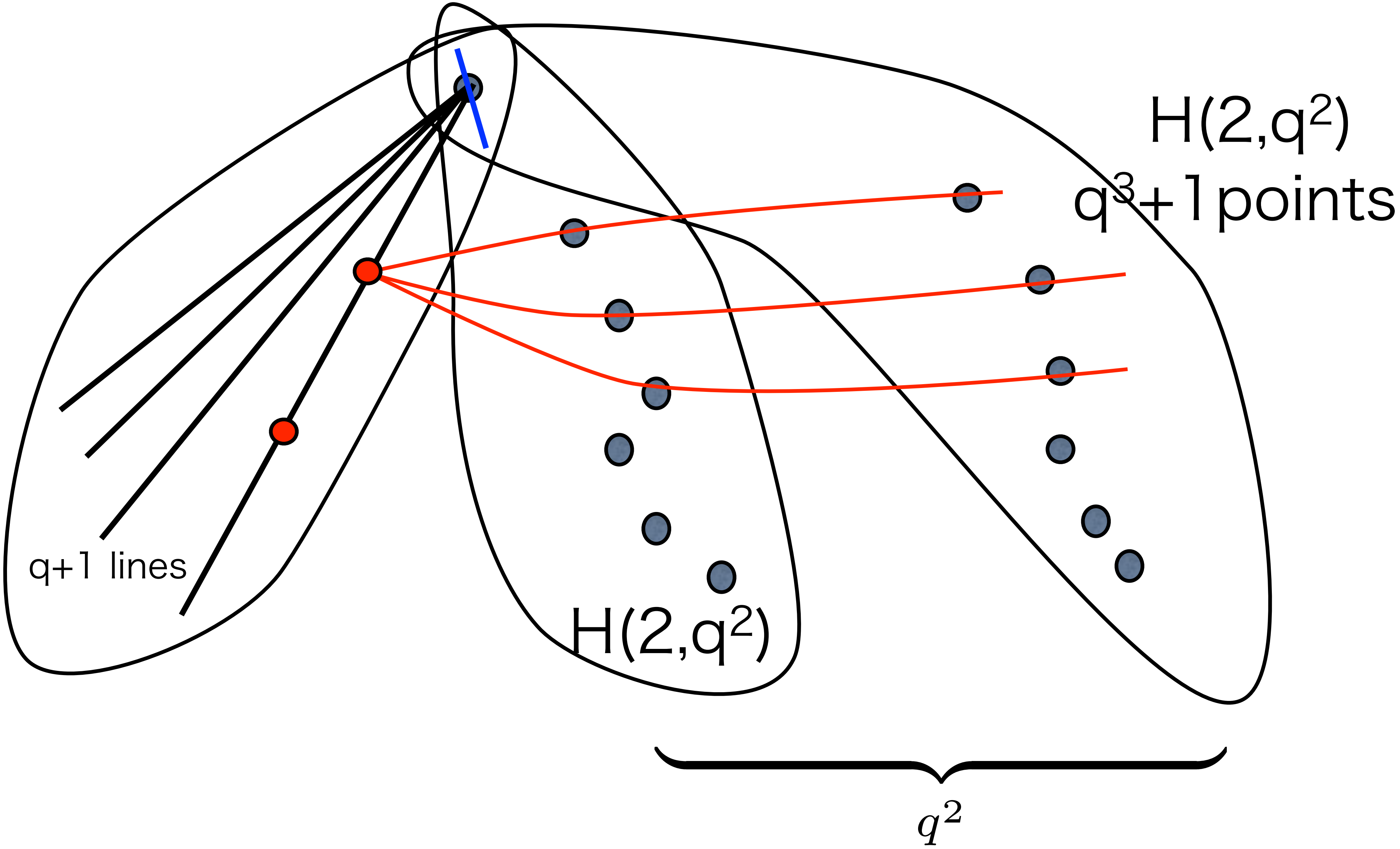
H(3,q²) primal

The planes containing a tangent line to H(3,q²)



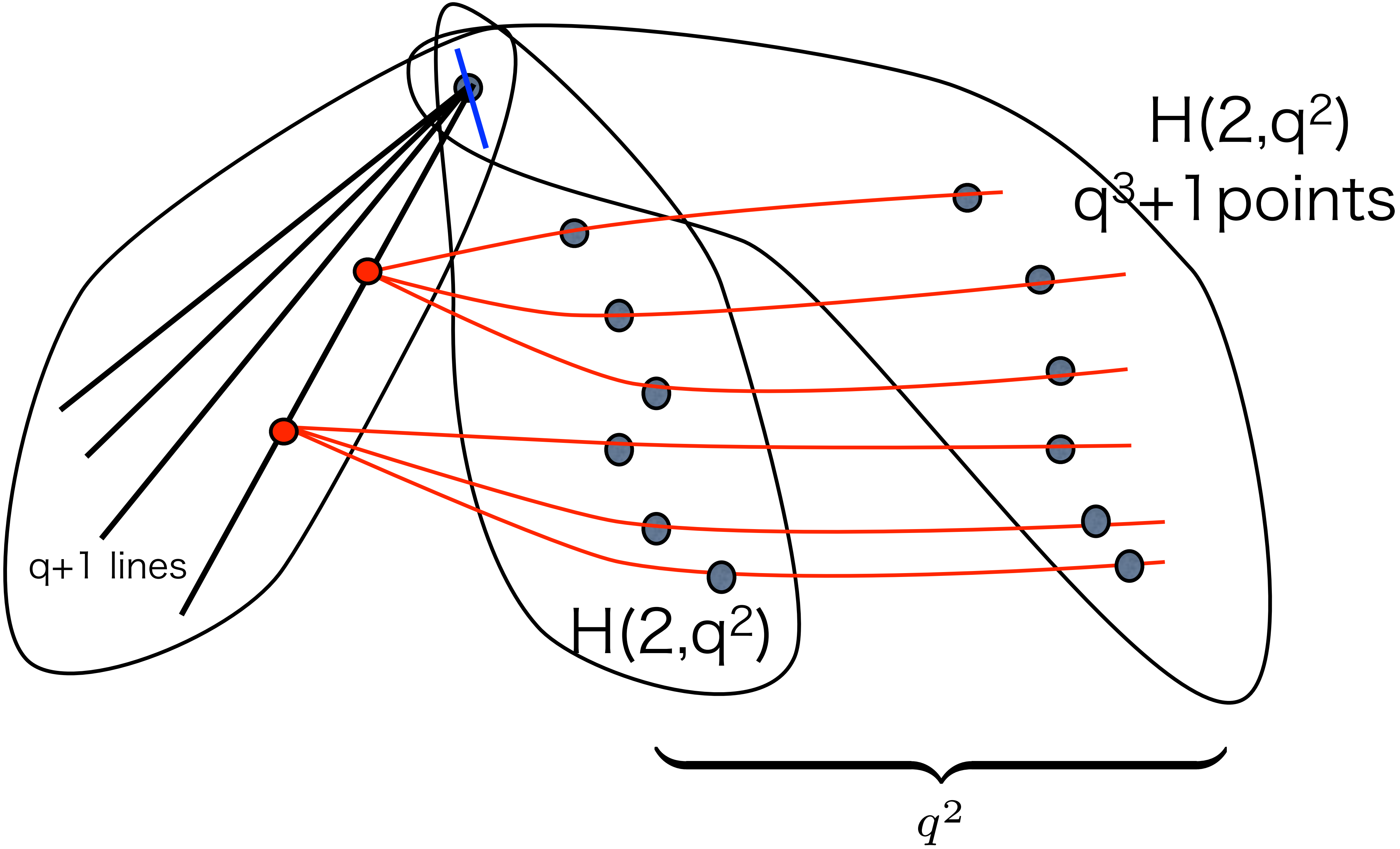
H(3,q^2) primal

The planes containing a tangent line to H(3,q^2)



$H(3,q^2)$ primal

The planes containing a tangent line to $H(3,q^2)$



The Number of Columns k

$v=q^3$	W&C
8	24
27	216
64	832

The Number of Columns k

$v=q^3$	W&C	$H(3,q^2)$
8	24	32
27	216	243
64	832	1024

$H(3,q^2)\backslash C_0$:

q^5 points

$q^3(q+1)$ lines

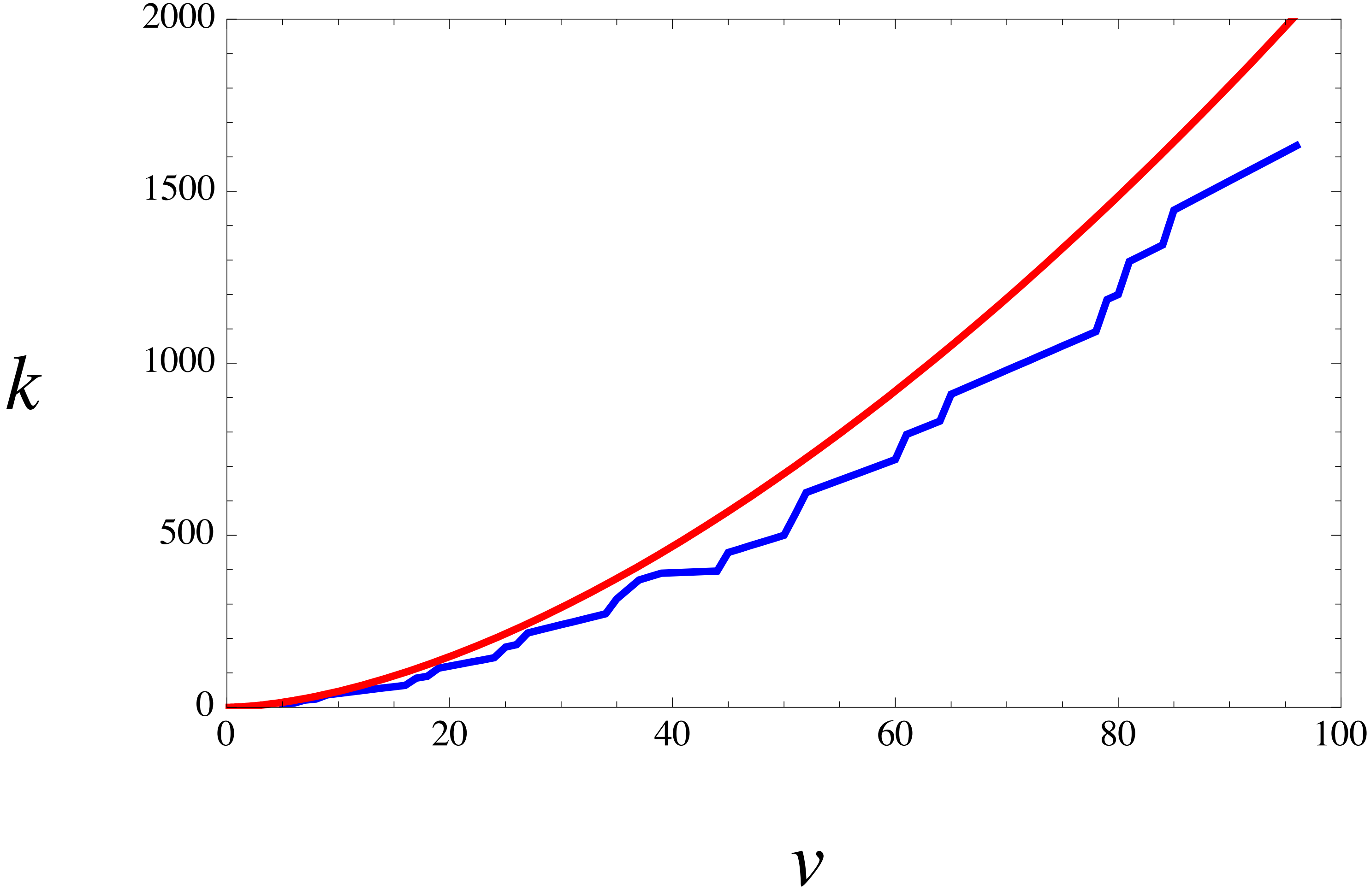
q^3 blocks in a spread

q+1spreads

Theorem

There exists a PHF(3; q^5, q^3, 3) for any prime power q.

The curve of $k=v^{(5/3)}$



Thank you !