Computational Methods in Finite Geometry

Anton Betten

Colorado State University

Summer School, Brighton, 2017

Q: What makes a problem interesting?

Maybe it is being **difficult**.

If this is true, then **Finite Geometry** is full of interesting problems.

In the words of John F. Kennedy:

We choose to go to the moon and do the other things not because they are easy but because they are hard.

In the words of Peter Cameron:

That a problem is hard does not mean we should not solve it.

Prologue

The goal is this lecture sequence is to say something meaningful about the problem of constructing and classifying combinatorial objects.

(with an emphasis on objects from finite geometry).

A large number of problems can be reduced to classifying orbits of groups acting on sets.

The sets are often very large and at times not readily available.

We need to perform search and isomorph rejection at the same time.

Terminology

Let G be a group.

Let G act on a finite set X.

For $x, y \in X$, say that $x \sim_G y$ if x and y belong to the same G-orbit.

Terminology

The isomorphism problem is the following:

Given $x, y \in X$, determine whether $x \sim_G y$ or not.

Terminology

The classification problem is the problem of determining the orbits of G on X, for instance by listing one element from each orbit.

Such a list of orbit representatives is called a transversal for the orbits of G on X.

From now on, assume that a transversal for the orbits of G on X has been fixed.

Suppose that $r_1, \ldots r_\ell$ is a transversal for the G-orbits on X.

Terminology

The recognition problem is the following:

Given $x \in X$, find the unique r_i with $r_i \sim_G x$.

Terminology

The constructive recognition problem is the following:

Given $x \in X$, find the unique r_i with $r_i \sim_G x$ and find an element $g \in G$ with

$$x^g = r_i.$$

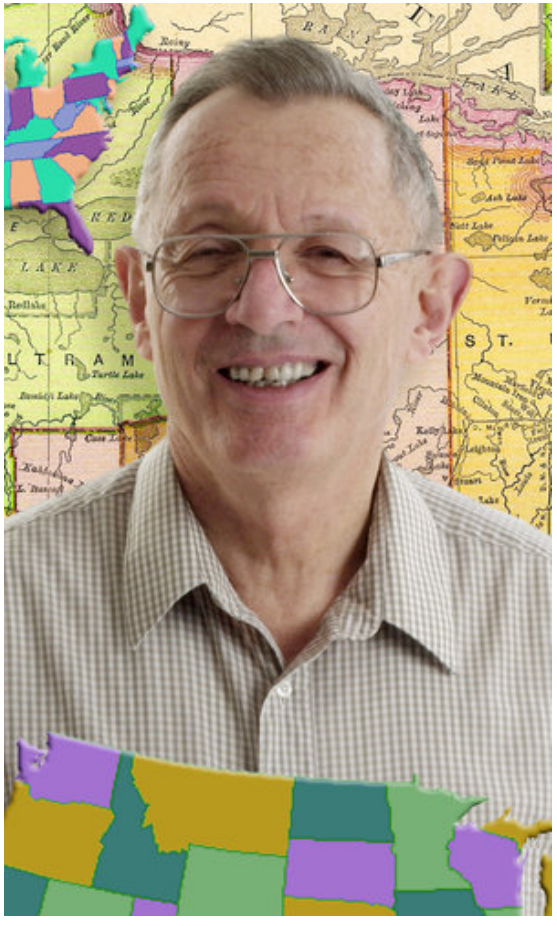
Computer Usage

The problems we will discuss typically require a great many number of cases to be considered.

These cases will be considered by computer.

Some mathematicians feel uneasy about the use of computers as a means to prove theorems.

“Without computers, we would be stuck only proving theorems that have short proofs.”



Ken Appel
1932 – 2013

Four Colors Suffice

The New York Times writes:

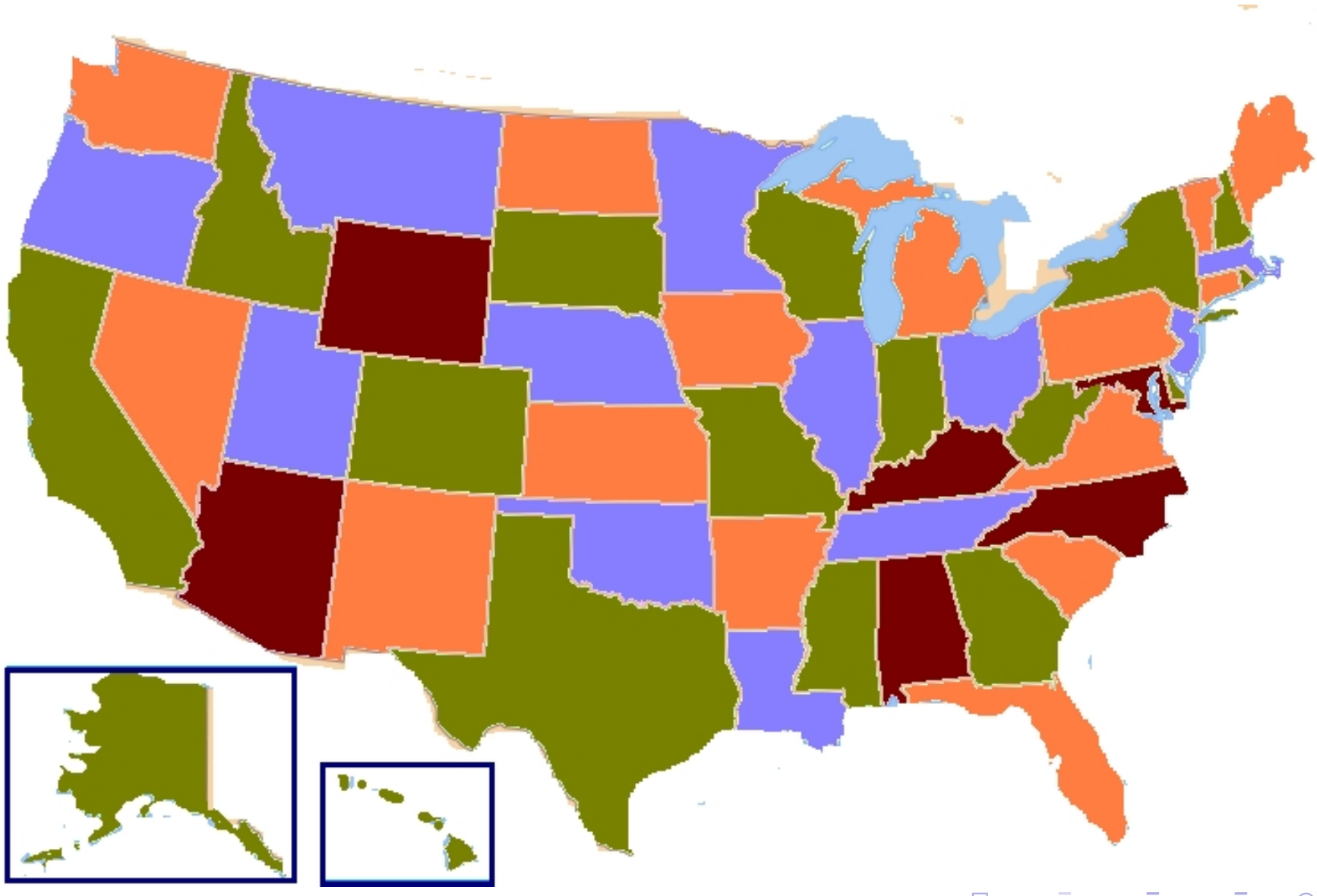
Some of the thorniest problems in math are simple to state but hideously complex under the surface.

Such is the case with the four-color theorem, first enunciated by an English mapmaker, Francis Guthrie, in 1852.

He asserted that to create a map in which no adjacent countries are the same color, only four colors are needed.

Although everyone believed it was true, proof had eluded a century of mathematicians until Dr. Appel attended a lecture in 1972 by Dr. Haken.

A proper 4-coloring



FOUR COLORS
SUFFICE

Kenneth Appel and Wofgang Haken in the 1970s

From the NY-Times:

Their four-color proof earned newspaper headlines and a prestigious award in mathematics, the Delbert Ray Fulkerson Prize.

But the notion of computer proofs drew skepticism in some academic circles.

In a visit to one university, Dr. Appel and Dr. Haken said, professors barred them from meeting graduate students lest the students' minds become contaminated.

Hailed in some circles as “a major intellectual feat,” the proof shepherded computers toward a greater role in higher math.

But it made many mathematicians uneasy; they worried about computer bugs and wondered how they could check or understand a “proof” they could not see.

And it ignited a long-running debate about what constitutes a mathematical proof.

The work which will be presented here makes great use of computers to perform and handle automatic case divisions.

If you are uneasy about this, maybe this talk is not for you.

At times, we may split a problem into thousands or sometimes hundreds of thousands of cases.

Comment:

Why do we need these classifications?

In mathematics, we develop theory to explain the examples.

If we don't have examples, it can be quite difficult to build theory.

There are many problems in finite geometry where we need more examples to make progress.

I would like to illustrate some instances of such problems.

Some of these problems have already been mentioned in the lectures by previous speakers.

List of problems for the next few lectures:

- BLT-sets (related to flocks).
- Parallelisms in $\mathrm{PG}(3, q)$
- Optimal linear codes
- Cubic surfaces

My goal is to show that these are not separate problems.

The same set of basic algorithmic tools can be applied to attack many of these problems.

A Lemma

Let $\mathcal{A}$ and $\mathcal{B}$ be two disjoint finite sets.

A relation $\mathfrak{R}$ between $\mathcal{A}$ and $\mathcal{B}$ is a subset of the cartesian product $\mathcal{A} \times \mathcal{B}$.

Suppose that there is a group G acting on both $\mathcal{A}$ and $\mathcal{B}$.

A relation $\mathfrak{R}$ between $\mathcal{A}$ and $\mathcal{B}$ is G-invariant if

$$(a, b) \in \mathfrak{R} \iff (a^g, b^g) \in \mathfrak{R}$$

for all $a \in \mathcal{A}$, $b \in \mathcal{B}$ and all $g \in G$.

Here, we use exponential notation to indicate the group action.

Some more terminology:

We say that $(a, b) \in \mathcal{A} \times \mathcal{B}$ is an *incident pair* (or a *flag*) if $(a, b) \in \mathfrak{R}$.

An orbit of G on incident pairs in $\mathfrak{R}$ is called a *flag-orbit*.

Every flag orbit is associated with exactly one orbit of G on $\mathcal{A}$ and one orbit of G on $\mathcal{B}$.

For $x \in \mathcal{A}$, we say that $\mathrm{Orb}_G\big((a, b)\big)$ *lies over* $\mathrm{Orb}_G(x)$ if $\mathrm{Orb}_G(x) = \Pi_1\Big(\mathrm{Orb}_G\big((a, b)\big)\Big)$.

For $y \in \mathcal{B}$, we say that $\mathrm{Orb}_G\big((a, b)\big)$ *lies over* $\mathrm{Orb}_G(y)$ if $\mathrm{Orb}_G(y) = \Pi_2\Big(\mathrm{Orb}_G\big((a, b)\big)\Big)$.

Here, Π_i is the projection onto the i-th component.

The following Lemma relates the G-orbits on $\mathcal{A}$ and the G-orbits on $\mathcal{B}$.

LEMMA:

Let G be a group acting on disjoint finite sets $\mathcal{A}$ and $\mathcal{B}$, and let $\mathfrak{R}$ be a G-invariant relation between $\mathcal{A}$ and $\mathcal{B}$.

Let $a_1, \ldots, a_m$ be representatives for the orbits of G on $\mathcal{A}$, so

$$\mathcal{A} = \bigcup_{i=1}^{m} \mathrm{Orb}_G(a_i).$$

Let $b_1, \ldots, b_n$ be representatives for the orbits of G on $\mathcal{B}$, so

$$\mathcal{B} = \bigcup_{j=1}^{n} \mathrm{Orb}_G(b_j).$$

For $a \in \mathcal{A}$, let

$$N_{\mathcal{B}}(a) = \{(a, b) \in \{a\} \times \mathcal{B} \mid (a, b) \in \mathfrak{R}\}.$$

For $b \in \mathcal{B}$, let

$$N_{\mathcal{A}}(b) = \{(a, b) \in \mathcal{A} \times \{b\} \mid (a, b) \in \mathfrak{R}\}.$$

For each $i = 1, \ldots, m$, the set $N_{\mathcal{B}}(a_i)$ is a $\mathrm{Stab}_G(a_i)$-set. Let

$$t_{i,k} = (a_i, b_{i,k}), \qquad k = 1, \ldots, K_i$$

be representatives of the orbits of $\mathrm{Stab}_G(a_i)$ on $N_{\mathcal{B}}(a_i)$, so

$$N_{\mathcal{B}}(a_i) = \bigcup_{k=1}^{K_i} \mathcal{T}_{i,k}$$

where

$$\mathcal{T}_{i,k} = \mathrm{Orb}_{\mathrm{Stab}_G(a_i)}\left(t_{i,k}\right).$$

For each $j = 1, \ldots n$, the set $N_{\mathcal{A}}(b_j)$ is a $\mathrm{Stab}_G(b_j)$-set. Let

$$s_{j,\ell} = (a_{j,\ell}, b_j), \qquad \ell = 1, \ldots, L_j$$

be representatives of the orbits of $\mathrm{Stab}_G(b_j)$ on $N_{\mathcal{A}}(b_j)$, so

$$N_{\mathcal{A}}(b_j) = \bigcup_{i=1}^{L_j} \mathcal{S}_{j,\ell} \qquad \ell = 1, \ldots, L_j,$$

where

$$\mathcal{S}_{j,\ell} = \mathrm{Orb}_{\mathrm{Stab}_G(b_j)}(s_{j,\ell}), \qquad \ell = 1, \ldots, L_j.$$

Then:

(a) There is a canonical bijection ψ between the orbits

$$\{\mathcal{T}_{i,k} \mid i = 1, \ldots, m,\ k = 1, \ldots, K_i\}$$

and the orbits

$$\{\mathcal{S}_{j,\ell} \mid j = 1, \ldots, n,\ \ell = 1, \ldots, L_j\}.$$

(b)

$$\sum_{i=1}^{m} K_i = \sum_{j=1}^{n} L_j.$$

(c) If $\mathcal{T}_{i,k}$ and $\mathcal{S}_{j,\ell}$ are corresponding orbits under ψ, then

$$|\mathrm{Orb}_G(a_i)| \cdot |\mathcal{T}_{i,k}| = |\mathcal{S}_{j,\ell}| \cdot |\mathrm{Orb}_G(b_j)|.$$

Proof:

(a) Each of these sets of orbits is in canonical bijection to the orbits of G on incident pairs $(a, b) \in \mathfrak{R}$. Two orbits $\mathcal{T}_{i,k}$ and $\mathcal{S}_{j,\ell}$ are in correspondence if the representatives $(a_i, b_{i,k})$ and $(b_j, a_{j,\ell})$ lie in the same G-orbit, i.e., if there exists a $g \in G$ such that $(a_i, b_{i,k})^g = (b_j, a_{j,\ell})$.

(b) Follows from (a).

(c) Double count the number of incident pairs $(a, b) \in \mathfrak{R}$ in the G-orbit of $(a_i, b_{i,k})$ (which contains $(b_j, a_{j,\ell})$).

Let

$$\mathfrak{T}_i = \{\mathcal{T}_{i,k} \mid k = 1, \ldots, K_i\}, \quad i = 1, \ldots, m,$$
$$\mathfrak{S}_j = \{\mathcal{S}_{j,\ell} \mid \ell = 1, \ldots, L_j\}, \quad j = 1, \ldots, n.$$

Also, let

$$\mathfrak{T} = \bigcup_{i=1}^{m} \mathfrak{T}_i, \qquad \mathfrak{S} = \bigcup_{j=1}^{n} \mathfrak{S}_j.$$

The lemma provides a bijection

$$\psi : \mathfrak{T} \to \mathfrak{S}.$$

For $i = 1, \ldots, m$ and for $k = 1, \ldots, K_i$, let h_{ik} be an element $g \in G$ such that

$$t_{i,k}^{h_{ik}} = t_{i,k}^{\psi} = s_{j,\ell}.$$

The bijection ψ allows us to count the number of orbits in $\mathfrak{T}_i$ which are associated with elements from $\mathfrak{S}_j$. More precisely, let

$$d_{i,j} = \left| \left(\mathfrak{T}_i \right)^{\psi} \cap \mathfrak{S}_j \right| \quad 1 \leq i \leq m,\ 1 \leq j \leq n,$$

and form the $m \times n$ matrix

$$D = \left(d_{i,j} \right).$$

We call this matrix the *decomposition matrix* for the orbits of G on $\mathfrak{R}$. The ordering of rows and columns of the decomposition matrix depends on the order in which we arrange the orbits of G on $\mathcal{A}$ and on $\mathcal{B}$.

The origins of this Lemma are somewhat unclear.

If G is transitive on $\mathcal{A}$ and on $\mathcal{B}$, the Lemma is known.

Even though the general case is not much harder to prove, the Lemma in this form does not seem to be published anywhere.

Comment 1

The purpose of the Lemma is to be able to lift a classification from one group action to another, related group action.

It can be used to devise an algorithm to compute the orbits of a group G acting on a partially ordered set.

Comment 2

There are different ways use the Lemma in algorithms:

There is a backtrack approach which favors recomputing the orbit representatives as we go along.

An example is Brendan McKay's program nauty. This is well-known in the graph theory community.

There is another approach where we store group elements associated to the mapping ψ.

An example is Bernd Schmalz's algorithm Leiterspiel.

This algorithm is perhaps a bit more universal than nauty. It can be made to apply to actions on sets and action on subspaces. It is therefore quite useful in finite geometry.

Topic # 1

BLT-sets over small finite fields

BLT-sets are related to many other objects of interest (flocks, projective planes, generalized quadrangles etc.).

Classifying BLT-sets up to projective equivalence is a difficult problem.

However, the number of BLT-sets for a given q seems to be relatively small.

This makes is interesting to compile lists of classified BLT-sets for small parameter values q.

10 infinite families of BLT-sets are known.

This still leaves many BLT-sets unexplained.

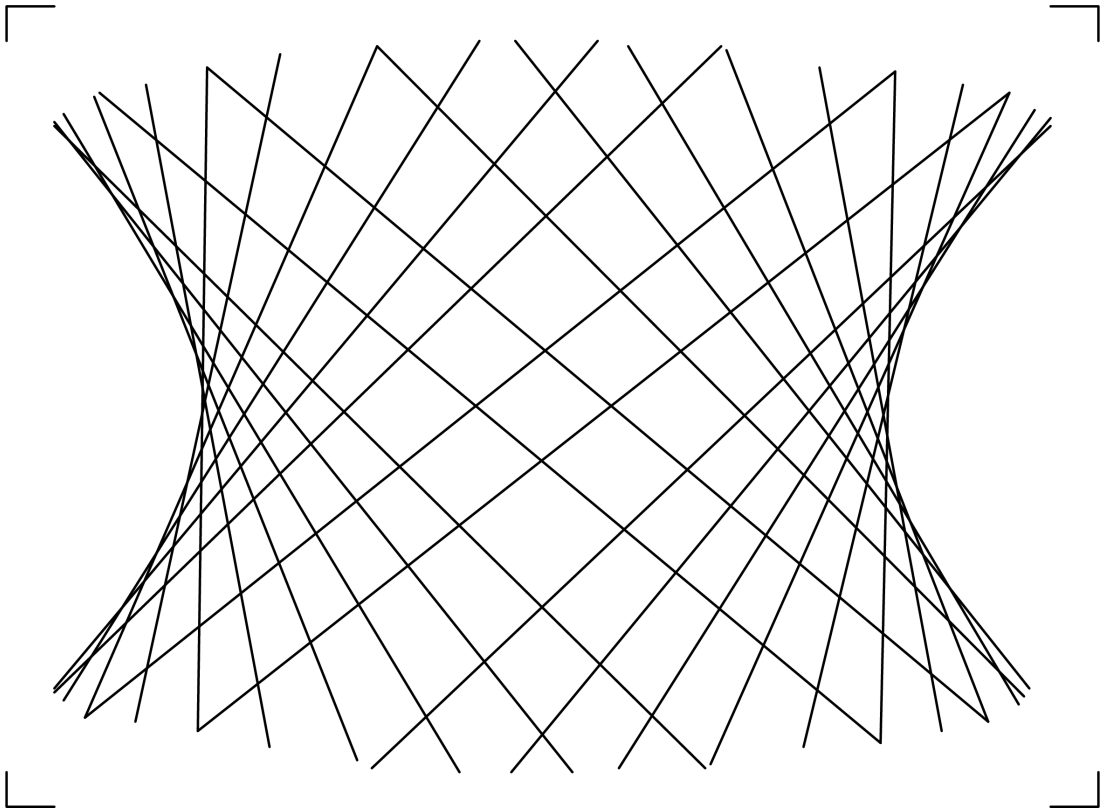
We hope that by providing more examples, we can help find new constrctions that would otherwise be very difficult to find.

We have developed a software system *Orbiter* to support the classification of combinatorial objects.

The system is a library of C++ classes, available on github.

BLT-sets

Quadrics in projective space (picture credit: Peter Cameron):



Depending on the dimension, they may contain points, lines, and possibly higher dimensional subspaces.

The quadric $Q(4, q)$ is the set of projective points

$$[x_0 : x_1 : x_2 : x_3 : x_4]$$

with coordinates $x_i \in \mathbb{F}_q$ satisfying the equation

$$x_0^2 + x_1 x_2 + x_3 x_4 = 0.$$

It contains points and lines.

This gives rise to an *incidence structure* $(\mathcal{P}, \mathcal{L})$:

- $\mathcal{P}$ is the set of points on the quadric.
- $\mathcal{L}$ is the set of lines on the quadric.

We can think of the elements of $\mathcal{L}$ as subsets of $\mathcal{P}$ of size $q+1$.

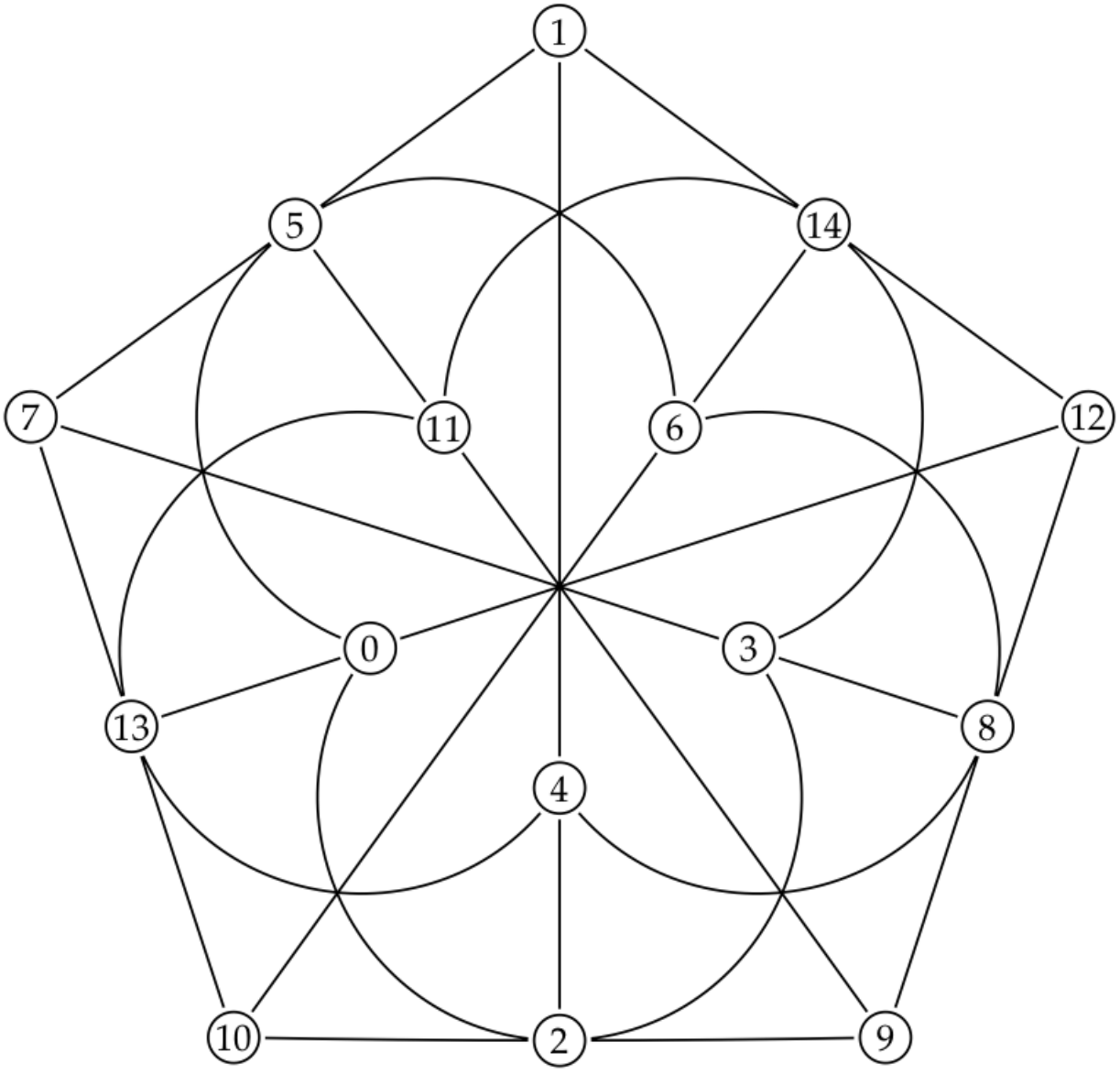
Smallest example: $q = 2$

There are 15 projective points on $Q(4, 2)$.

We label them using the numbers 0 through 14.

There are also 15 lines contained in the quadric.

$Q(4,2)$ (15 points, 15 lines)



The lines (as subsets):

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

Notation:

> *We say that two points P and Q are* collinear *(written as $P \sim Q$) if there is a line (i.e., a subset) that contains both.*

Example: $0 \sim 2$ but $0 \not\sim 1$.

Observe: Not any two points are collinear, so this is different from a projective space, for instance (it is known as a *polar space*).

The incidence matrix $\mathcal{I}$:
rows = points, columns = lines.

$$\left[\begin{array}{c|cccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
5 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
7 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
8 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
9 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
10 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
12 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
13 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
14 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0
\end{array}\right]$$

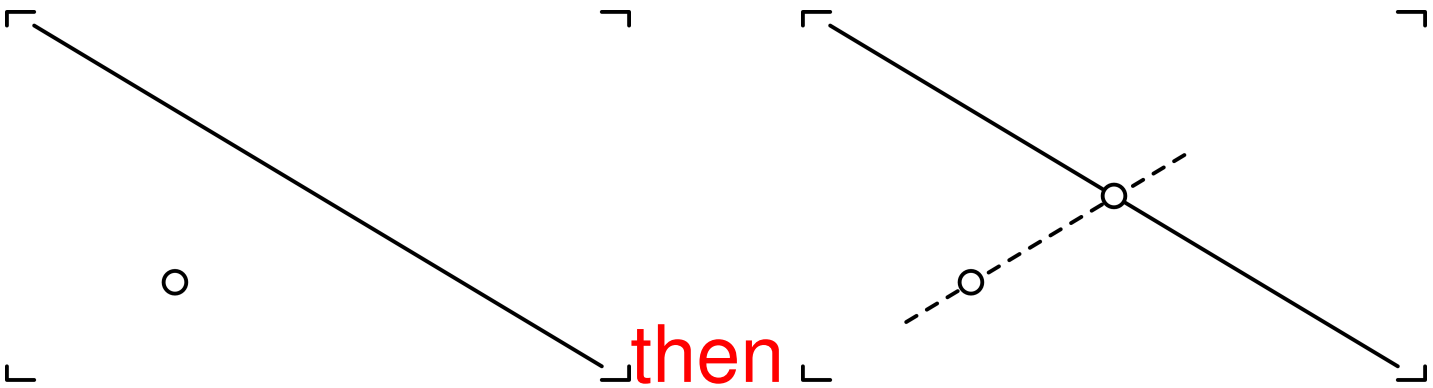
We verify that $0 \sim 2$ because there is a column that has a one in both row 0 and in row 2:

$$\left[\begin{array}{c|cccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
5 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
7 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
8 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
9 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
10 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
12 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
13 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
14 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0
\end{array}\right]$$

However, $0 \not\sim 1$ because no column contains both 0 and 1.

The *Generalized Quadrangle Axiom*:

> *If a point P is not on a line ℓ then there is exactly one point Q on ℓ such that P and Q are collinear.*



The $Q(4, q)$ quadric is a generalized quadrangle with parameters $s = t = q$.

The following definition is due to Bader, Lunardon and Thas 1990:

Definition

A BLT-set is a set of $q+1$ points on $Q(4,q)$ such that *no quadric point is collinear to three points in the set*.

The name BLT is due to William Kantor.

Classification

The Isomorphism Problem for BLT-Sets:

Definition

Two BLT-sets are isomorphic if they are projectively equivalent (under a symmetry of the $Q(4, q)$).

The group of $Q(4, q)$ is the orthogonal group $\mathrm{P\Gamma O}(5, q)$.

So, if $\mathcal{B}_1$ and $\mathcal{B}_2$ are BLT-sets and if there is an invertible 5×5 matrix M over $\mathbb{F}_q$ and a field automorphism ϕ of $\mathbb{F}_q$ such that

$$Q(4,q)^{(M,\phi)} = Q(4,q) \quad \text{and} \quad \mathcal{B}_1^{(M,\phi)} = \mathcal{B}_2$$

then $\mathcal{B}_1$ and $\mathcal{B}_2$ are isomorphic.

Here, (M, ϕ) is the mapping that takes

$$[x_0 : x_1 : x_2 : x_3 : x_4]$$

to

$$([x_0, x_1, x_2, x_3, x_4] \cdot M)^{\phi}$$

We are mapping sets pointwise:

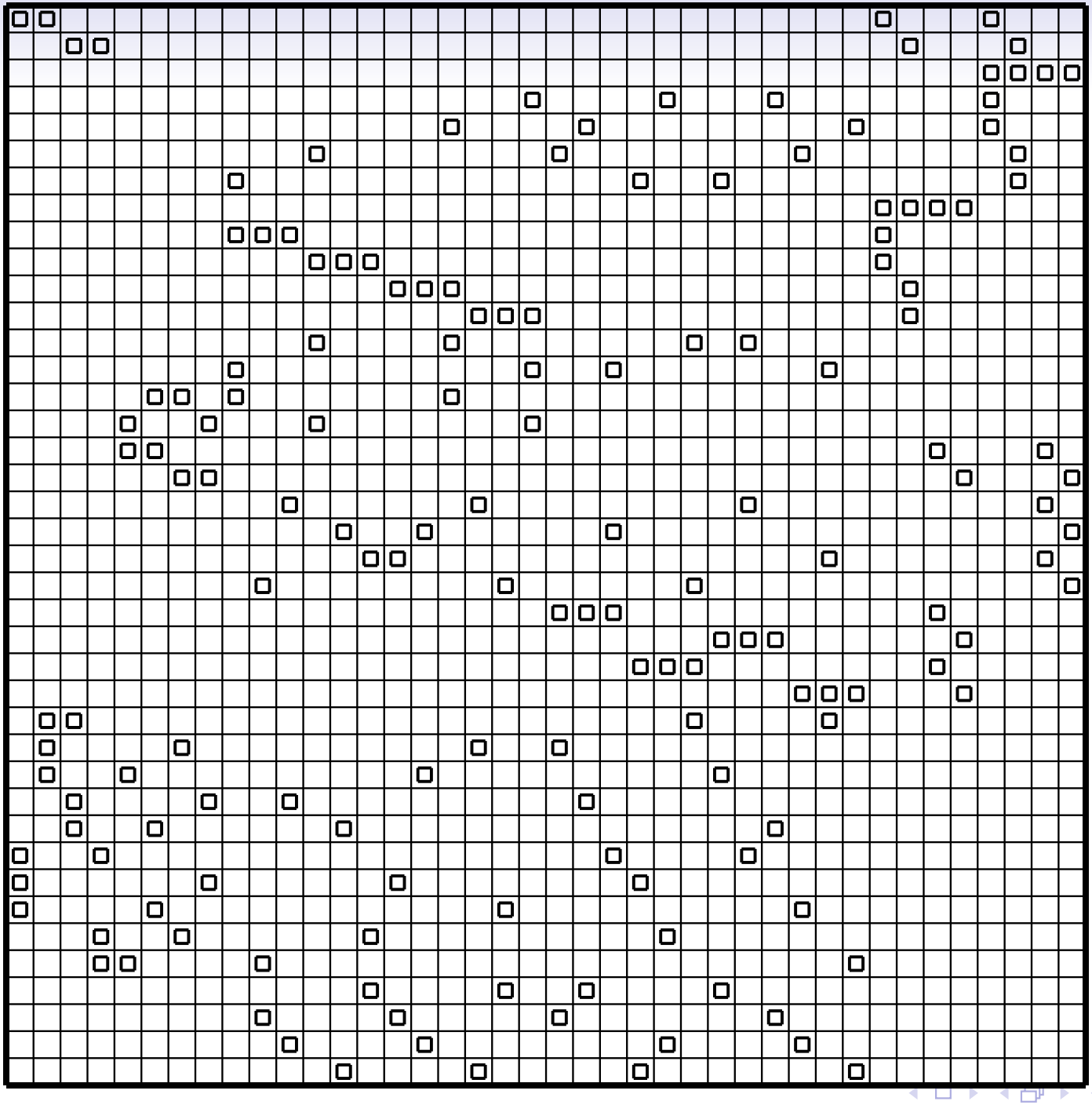
$$\mathcal{B}_1^{(M,\phi)} = \{P^{(M,\phi)} \mid P \in \mathcal{B}_1\}.$$

What is known about BLT-sets?

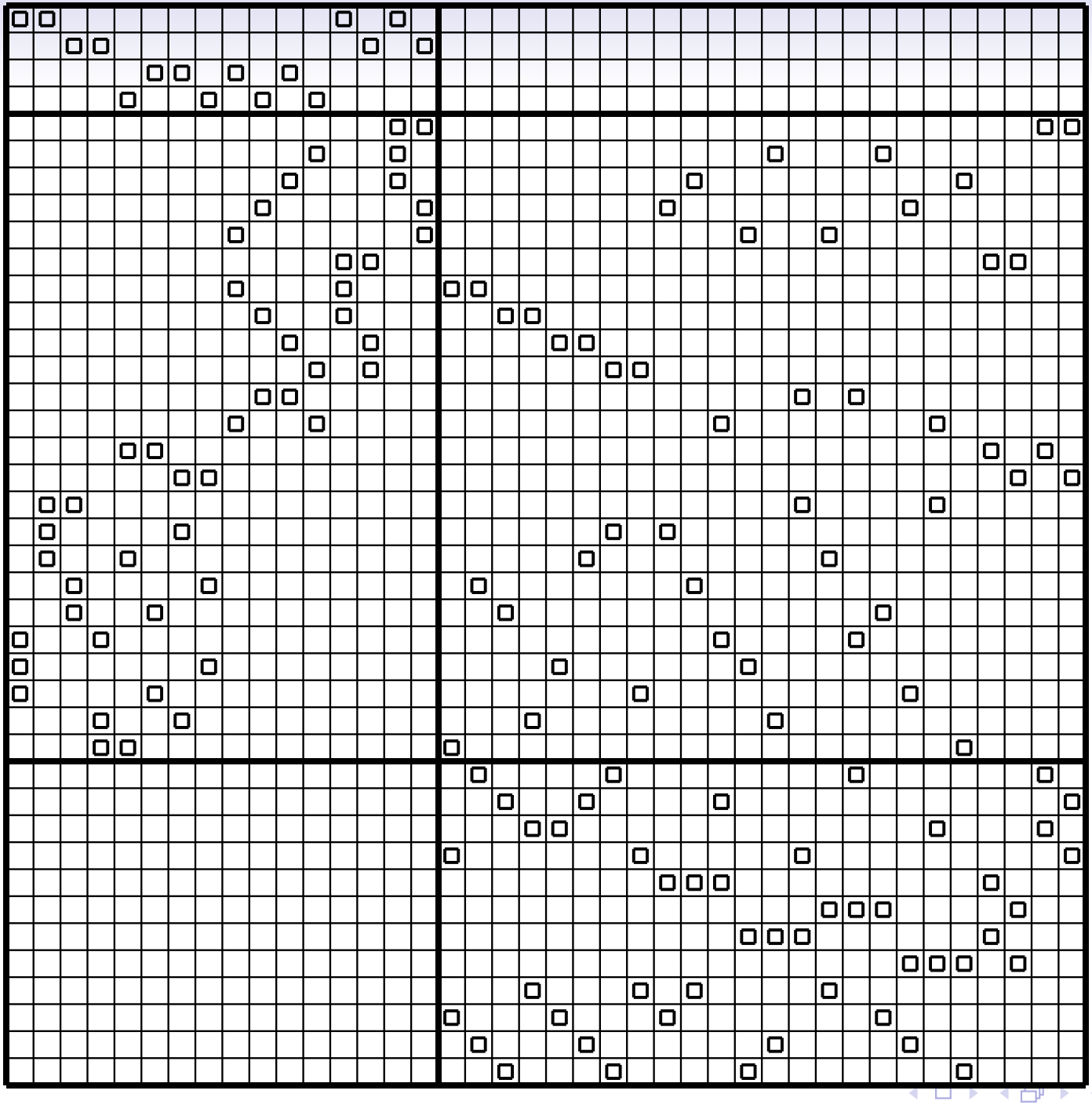
- $Q(4, q)$ has a BLT-set if and only if q is odd.

So, $Q(4, 2)$ above was *the wrong example*. Sorry!

Let's look at $Q(4, 3)$ (with 40 points and 40 lines):



Where is the BLT-set ?



Up to isomorphism, there is only one BLT-set of $Q(4,3)$.

Up to isomorphism, there are exactly two BLT-sets of $Q(4,5)$.

Here is the classification:

B. 2013

The BLT-sets are classified for $q \leq 67$:

q	BLT
3	1
5	2
7	2
9	3
11	4
13	3
17	6
19	5

q	BLT
23	9
25	6
27	6
29	9
31	8
37	7
41	10

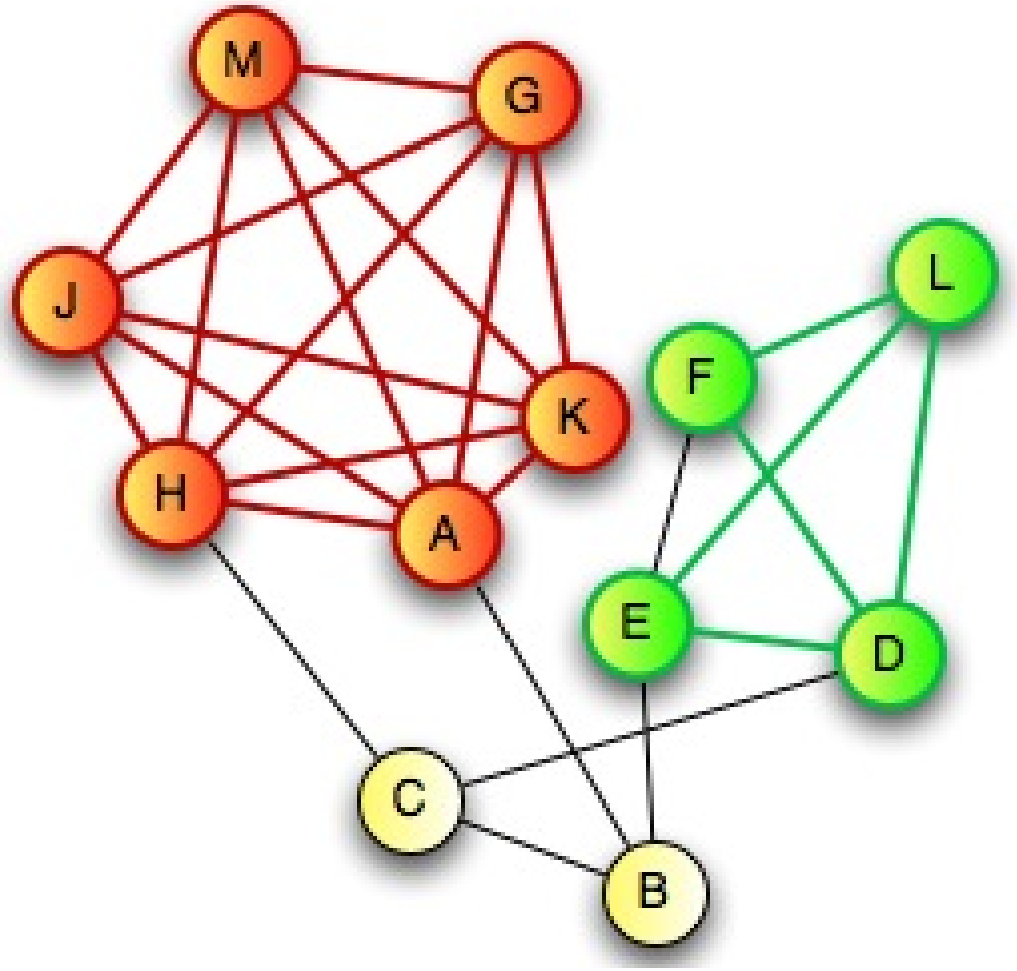
q	BLT
43	6
47	10
49	8
53	8
59	9
61	5
67	6

The Number of Isomorphism Classes of BLT-Sets of Order q

The numbers for $q \leq 29$ are due to a combination of Penttila, Royle, Thas.

Cliques

A clique in a graph Γ is a set of vertices such that the induced subgraph is complete.



$\{A, K, G, M, J, H\}$

is a maximal clique,

as is

$\{E, D, F, L\}$.
(besides all edges)

Cliques

Finding all maximal cliques in a graph is a difficult algorthm.

There is an algorithm to list all maximal cliques in a graph due to Bron and Kerbosch (from the 1970s).

The algorithm has exponential running time.

Cliques

To explain why we need cliques, let us look at the algorithm to classify BLT-sets.

We define a class of graphs Γ_S whose cliques are important.

We use subobjects:

A partial BLT-set of size s is a set of s points such that no point of $Q(4, q)$ is collinear to three points in S.

Observe that a partial BLT-set of size $q + 1$ is just a BLT-set.

Observe that any subset of a BLT-set is a partial BLT-set.

We choose an integer s (smallish).

Classify — up to isomorphism — all partial BLT-sets of size s.

For this, we use an algorithm that classifies orbits on posets.

The orbit representatives of partial BLT-sets of size s are called *starter*.

Let S be a starter (i.e., a partial BLT-set of size s for some small value of s).

The goal is to find all BLT-sets containing S.

This is known as *lifting* S.

Define a graph $\Gamma_S = (V, E)$ where

$$V = \left\{\text{points } P \in Q(4, q) \setminus S \mid S \cup \{P\} \text{ is partial BLT-set}\right\}$$

and

$$E = \left\{(P, Q) \in V \mid S \cup \{P, Q\} \text{ is partial BLT-set}\right\}$$

It is clear that every BLT-set containing S corresponds to a clique in Γ_S of size $q + 1 - s$.

Conversely, every clique of Γ_S of size $q + 1 - s$ gives rise to a BLT-set containing S.

This has been pointed out by Penttila.

Thus, we have reduced the problem of finding all BLT-sets containing S to the problem of finding all cliques of size $q + 1 - s$ in Γ_S.

Once this problem is solved, we also need to consider the problem of isomorphism classification of the liftings.

Rainbow Cliques

Color on the vertices of Γ_S:

Let ℓ be any line through any one of the points of the partial BLT-set.

Rainbow Cliques

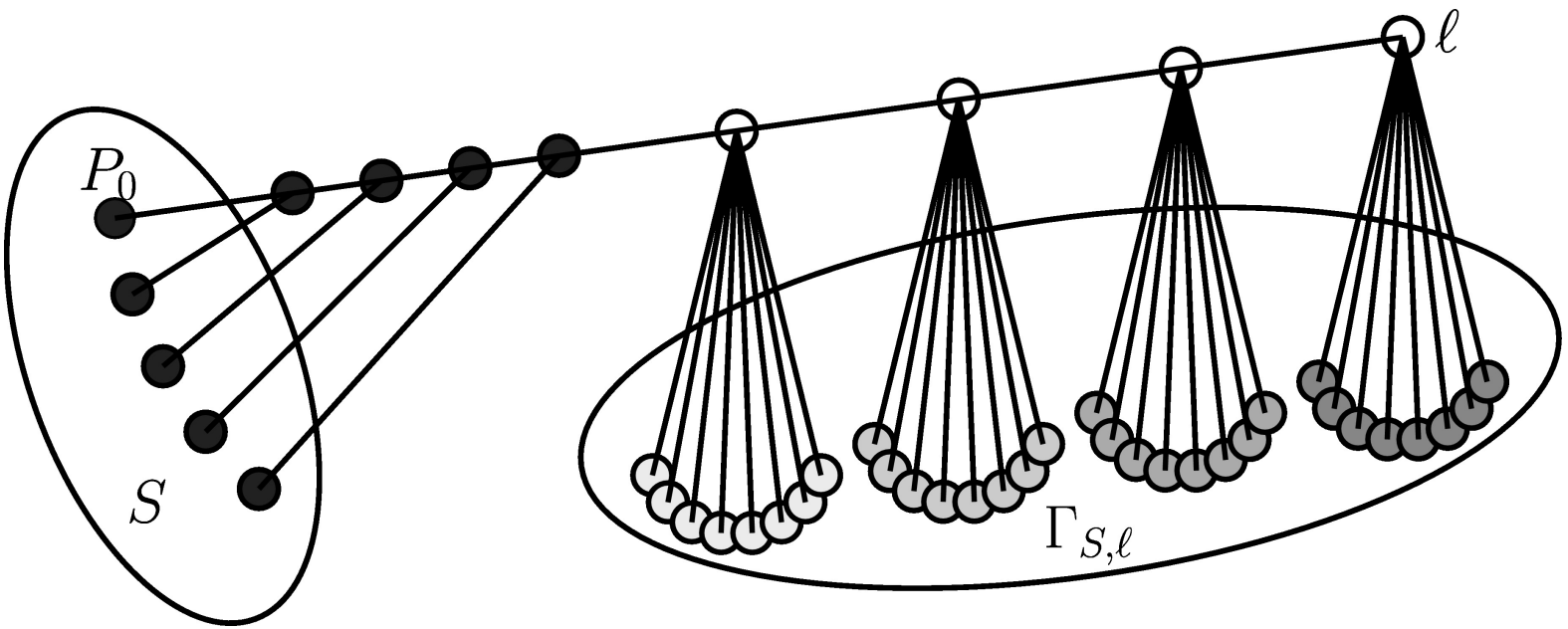
Color the points of V (the vertices of Γ_S):

Take the elements of $\ell \setminus \{S\}$ as colors.

Color a point $P \in V$ according to the point on ℓ that P is collinear with.

This defines a vertex colored graph $\Gamma_{S,\ell}$.

Example:



The Colored Graph $\Gamma_{S,\ell}$ (Edges not shown)

Definition:

Let Γ be a vertex colored graph. A *rainbow clique* in Γ is a clique that intersects each color class in eactly one element.

Lemma:

The BLT-sets containing S correspond one-to-one to the rainbow cliques in $\Gamma_{S,\ell}$.

Observe that it is much easier to search for rainbow cliques in $\Gamma_{S,\ell}$ than it is to search for cliques in Γ_S:

If the current clique is incomplete and if there are no candidates of a given color and we still need that color, then we can conclude that there is no rainbow clique cointaining the current clique.

This is a stopping condition.

Q: Where exactly is the difficult part in the classification algorithm of BLT-sets?

Most of the computing time is spent on the lifting of the starter partial BLT-sets.

We had to find all rainbow cliques of size ~ 60 in graphs with several thousand vertices.

The computations were performed in parallel (twice): Once on the Open Science Grid, the other time on a 64 CPU machine in the department.

The overall CPU-time was enormous. For the BLT-sets of order 67, we used ≈ 16 years of CPU time (each time).

Topic # 2

Spreads and Packings

Projective Geometry over a Finite Field

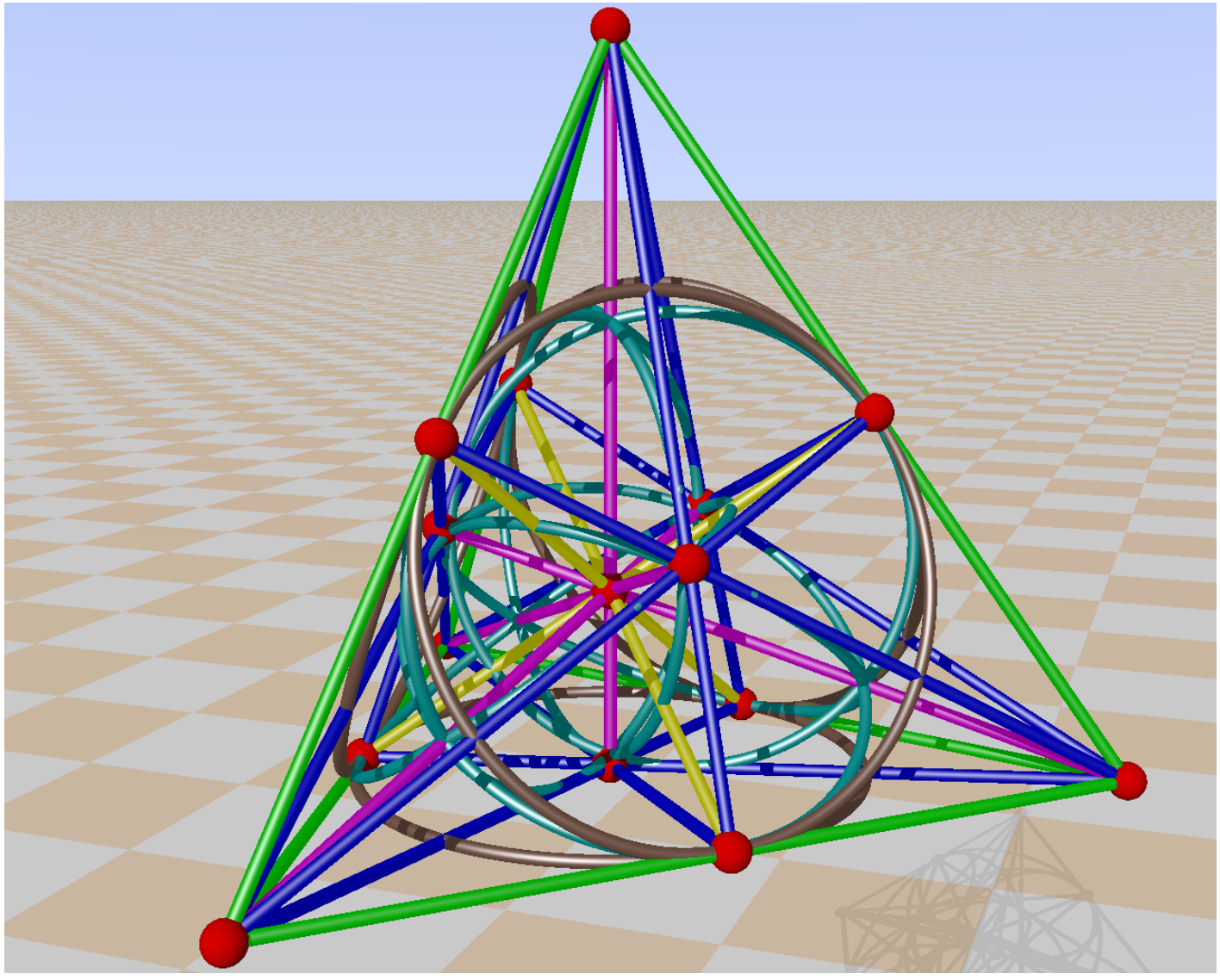
$\mathrm{PG}(n, q)$ is a point-line incidence structure.

$\mathrm{PG}(3, q)$ has $q^3 + q^2 + q + 1$ points and $q^4 + q^3 + 2q^2 + q + 1$ lines.

Each point is on $q^2 + q + 1$ lines and each line has $q + 1$ points.

Two lines intersect in at most one point. This happens precisely if the two lines lie in a plane. Otherwise they are called skew.

The smallest projective three-space PG(3, 2):



Coordinates

We use homogeneous coordinates

$$(a_0 : a_1 : a_2 : a_3), \quad a_i \in \mathbb{F}_q$$

to denote points.

Lines are subspaces of rank two.

Using a notation from coding theory, we write them as generator matrices:

$$\begin{bmatrix} a & b & c & d \\ e & f & g & h \end{bmatrix}$$

The subspace is obtained by taking the row-span of the generator matrix.

Symmetry

The symmetry group of $\mathrm{PG}(n, q)$ is generated by invertible $n \times n$ matrices over $\mathbb{F}_q$ (here $n = 4$):

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}$$

together with the field automorphism

$$\phi : \alpha \mapsto \alpha^p$$

acting as

$$\phi : (a_0 : a_1 : a_2 : a_3) \mapsto (a_0^p : a_1^p : a_2^p : a_3^p).$$

This is the group

$$\mathrm{P\Gamma L}(n, q)$$

Projective Geometry over a Finite Field

Objects inside $\mathrm{PG}(n, q)$ are called isomorphic (or projectively equivalent) if they lie in the same orbit under the symmetry group.

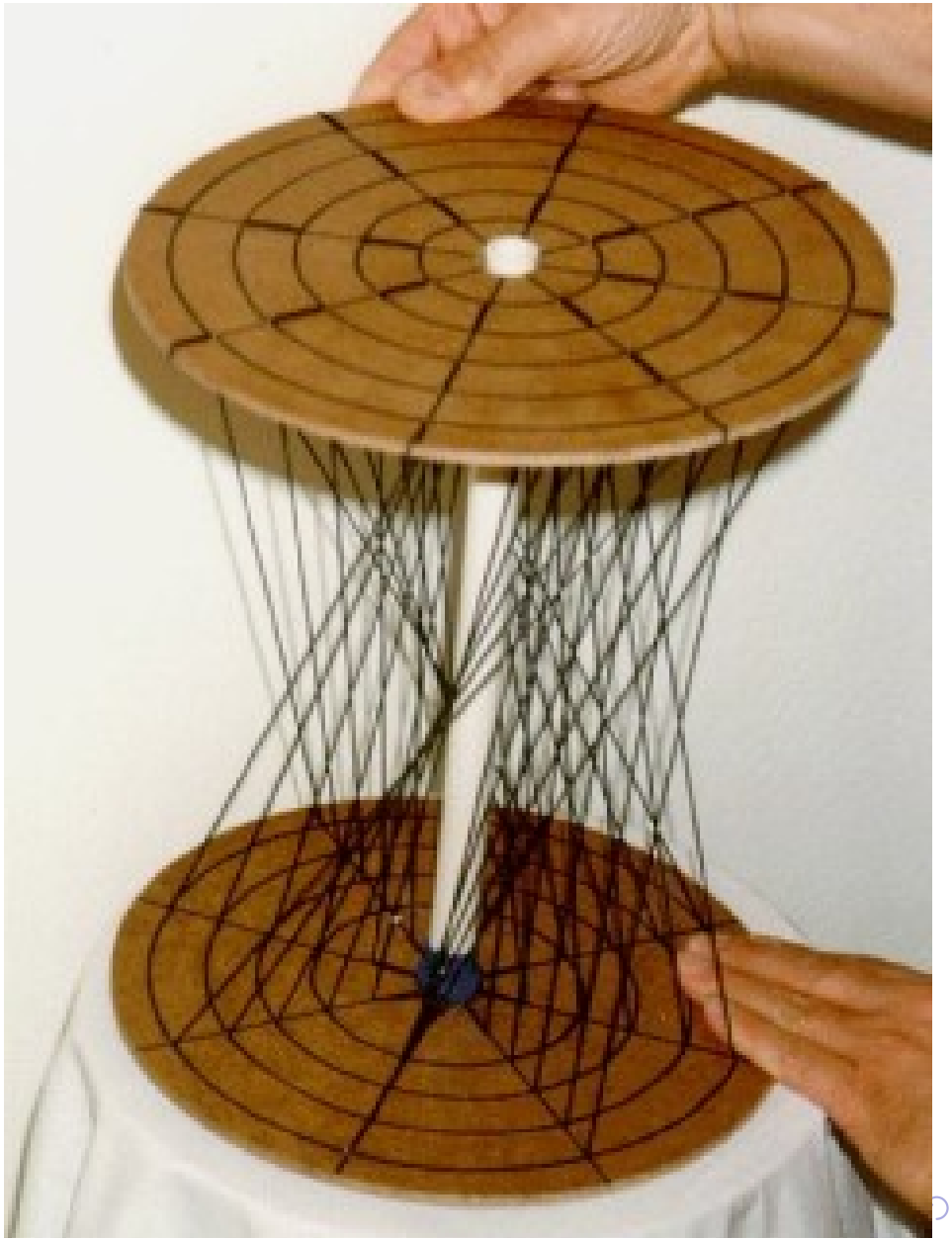
The problem of classification is to find all pairwise non-isomorphic objects of a certain kind (for instace, by making a list).

Related problems are that of recognition and identification:

If an object is given, identify the one in the list that it is isomorphic to (for instance by finding a group element that maps one to the other).

Spreads and Packings in $\mathrm{PG}(3, q)$

A spread of $\mathrm{PG}(3, q)$ is a partition of the points by lines:



Spreads and Packings in $\mathrm{PG}(3, q)$

Every $\mathrm{PG}(3, q)$ has (up to isomorphism) at least one spread, the regular spread.

It can be thought of a being obtained by field reduction from $\mathrm{PG}(1, q^2)$:

Let

$$\mathbb{F}_{q^2} = \mathbb{F}_q + \alpha\mathbb{F}_q$$

and consider the mapping

$$(a + b\alpha, c + d\alpha) \mapsto (a, b, c, d)$$

Under this mapping, the points of $\mathrm{PG}(1, q^2)$ become lines of $\mathrm{PG}(3, q)$ and give a spread.

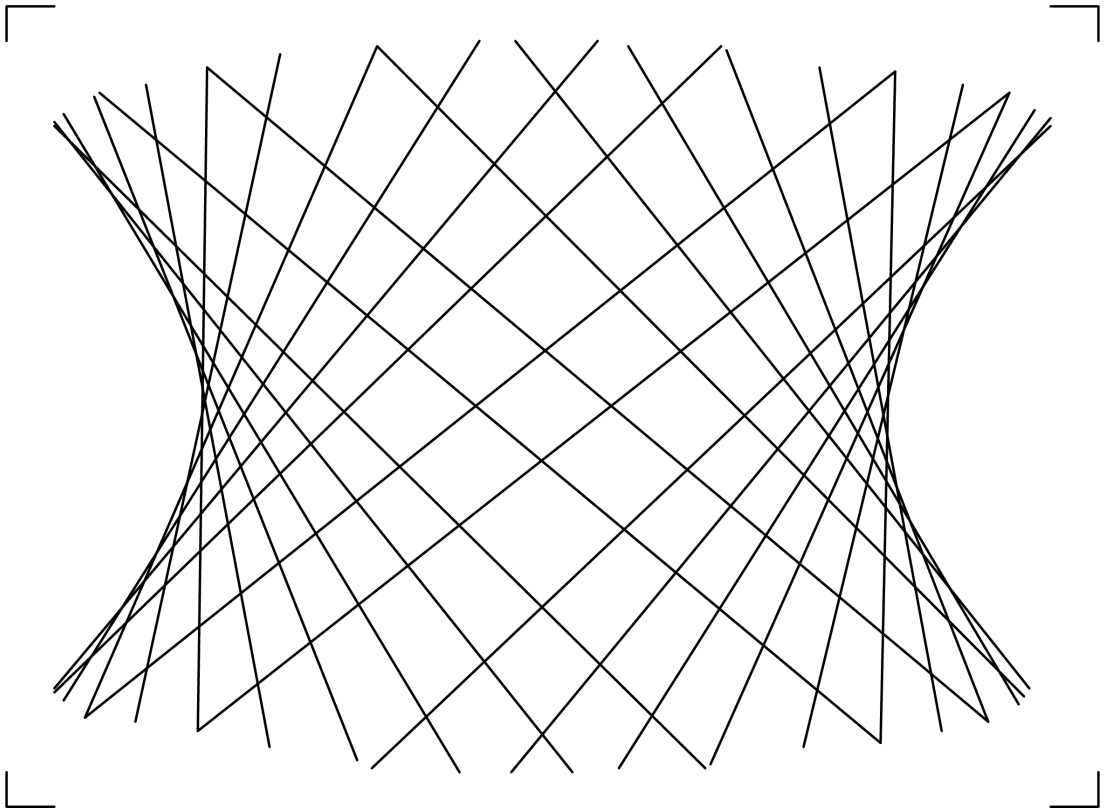
Spreads and Packings in $\mathrm{PG}(3, q)$

A regulus is a set of $q + 1$ mutually skew lines with the property:

> Any line intersecting three of its lines must intersect all of its lines.

The set of reguli defines a 3-design in the set of lines of $\mathrm{PG}(3, q)$.

A regulus partitions the set of points of a hyperbolic quadric $Q^+(3,q)$ (there are two reguli associated with any given $Q^+(3,q)$):



Spreads and Packings in $\mathrm{PG}(3, q)$

A spread is regular if with any three lines of it, the regulus determined by these three lines is contained as well.

Transation planes arise from spreads, hence the interest in spreads.

1. André, Johannes (1954). Über nicht-Dessarguessche Ebenen mit transitiver Translationsgruppe. pp. 156-186.
2. Bruck, R. H.; R. C. Bose (1964). The Construction of Translation Planes from Projective Spaces. pp. 85-102.

Regular spreads are associated with Pappian (Desarguesian if finite) projective planes, hence the interest.

Spreads and Packings in $\mathrm{PG}(3, q)$

Using the Hiramine/Matsumoto/Oyama-construction, each spread gives an infinite family of spreads and hence of translation planes.

Spreads and Packings in $\mathrm{PG}(3, q)$

A packing is a set of spreads, pairwise disjoint, such that every line of $\mathrm{PG}(3, q)$ belongs to exactly one of the chosen spreads.

Other names:

1. Resolution,
2. Parallelism,
3. Large set.

Spreads and Packings in $\mathrm{PG}(3, q)$

It is not clear when packings exist.

A packing is regular if it is made up solely of regular spreads.

A family of regular packings has been described by Penttila and Williams 1998.

We need a congruence on q for this.

Spreads and Packings in $\mathrm{PG}(3, q)$

Open questions:

1. What kinds of packings exist?
2. Do there exist other regular packings that the ones of Penttila and Williams?

It would be nice to classify spreads and packings of $\mathrm{PG}(3, q)$ for small q.

Spreads and Packings in $\mathrm{PG}(3, q)$

Some counting yields:

A spread has $q^2 + 1$ lines. A packing consists of $q^2 + q + 1$ spreads.

Applications

Packings are related to an old problem in Combinatorics, namely Kirkman's 15 schoolgirls, from 1850:

The 15 Schoolgirls

Kirkman's schoolgirl problem:
Fifteen young ladies in a school walk out three abreast for seven days in succession: it is required to arrange them daily, so that no two walk twice abreast.

The packings of $\mathrm{PG}(3,2)$ provide solutions to this problem:
The points correspond to the schoolgirls.
The lines play the role of the rows of 3 girls.
The packing partitions the rows so that we can "parade" the girls over the seven days.

The 15 Schoolgirls

One solution is:

$$\left[\begin{array}{l|lllll} \text{Monday} & 5 & 8 & 14 & 27 & 31 \\ \text{Tuesday} & 3 & 16 & 20 & 26 & 28 \\ \text{Wednesday} & 2 & 11 & 19 & 21 & 33 \\ \text{Thursday} & 6 & 7 & 24 & 25 & 32 \\ \text{Friday} & 0 & 10 & 15 & 23 & 34 \\ \text{Saturday} & 1 & 9 & 13 & 18 & 29 \\ \text{Sunday} & 4 & 12 & 17 & 22 & 30 \end{array}\right]$$

The numbers $0, \ldots, 34$ represent the 35 lines of $\mathrm{PG}(3, 2)$.

The Lines of $\mathrm{PG}(3,2)$

$$L_0 = \begin{bmatrix} 1000 \\ 0100 \end{bmatrix} \quad L_9 = \begin{bmatrix} 1010 \\ 0101 \end{bmatrix} \quad L_{18} = \begin{bmatrix} 1001 \\ 0010 \end{bmatrix} \quad L_{27} = \begin{bmatrix} 1110 \\ 0001 \end{bmatrix}$$

$$L_1 = \begin{bmatrix} 1000 \\ 0110 \end{bmatrix} \quad L_{10} = \begin{bmatrix} 1010 \\ 0111 \end{bmatrix} \quad L_{19} = \begin{bmatrix} 1001 \\ 0011 \end{bmatrix} \quad L_{28} = \begin{bmatrix} 0100 \\ 0010 \end{bmatrix}$$

$$L_2 = \begin{bmatrix} 1000 \\ 0101 \end{bmatrix} \quad L_{11} = \begin{bmatrix} 1100 \\ 0010 \end{bmatrix} \quad L_{20} = \begin{bmatrix} 1010 \\ 0001 \end{bmatrix} \quad L_{29} = \begin{bmatrix} 0100 \\ 0011 \end{bmatrix}$$

$$L_3 = \begin{bmatrix} 1000 \\ 0111 \end{bmatrix} \quad L_{12} = \begin{bmatrix} 1100 \\ 0011 \end{bmatrix} \quad L_{21} = \begin{bmatrix} 1011 \\ 0100 \end{bmatrix} \quad L_{30} = \begin{bmatrix} 0100 \\ 0001 \end{bmatrix}$$

$$L_4 = \begin{bmatrix} 1000 \\ 0010 \end{bmatrix} \quad L_{13} = \begin{bmatrix} 1100 \\ 0001 \end{bmatrix} \quad L_{22} = \begin{bmatrix} 1011 \\ 0110 \end{bmatrix} \quad L_{31} = \begin{bmatrix} 0101 \\ 0010 \end{bmatrix}$$

$$L_5 = \begin{bmatrix} 1000 \\ 0011 \end{bmatrix} \quad L_{14} = \begin{bmatrix} 1001 \\ 0100 \end{bmatrix} \quad L_{23} = \begin{bmatrix} 1011 \\ 0101 \end{bmatrix} \quad L_{32} = \begin{bmatrix} 0101 \\ 0011 \end{bmatrix}$$

$$L_6 = \begin{bmatrix} 1000 \\ 0001 \end{bmatrix} \quad L_{15} = \begin{bmatrix} 1001 \\ 0110 \end{bmatrix} \quad L_{24} = \begin{bmatrix} 1011 \\ 0111 \end{bmatrix} \quad L_{33} = \begin{bmatrix} 0110 \\ 0001 \end{bmatrix}$$

$$L_7 = \begin{bmatrix} 1010 \\ 0100 \end{bmatrix} \quad L_{16} = \begin{bmatrix} 1001 \\ 0101 \end{bmatrix} \quad L_{25} = \begin{bmatrix} 1101 \\ 0010 \end{bmatrix} \quad L_{34} = \begin{bmatrix} 0010 \\ 0001 \end{bmatrix}$$

$$L_8 = \begin{bmatrix} 1010 \\ 0110 \end{bmatrix} \quad L_{17} = \begin{bmatrix} 1001 \\ 0111 \end{bmatrix} \quad L_{26} = \begin{bmatrix} 1101 \\ 0011 \end{bmatrix}$$

The Lines of $\mathrm{PG}(3, q)$

A convenient way to encode the lines of $\mathrm{PG}(3, q)$ is by means of the Klein correspondence.

Lines in $\mathrm{PG}(3, q)$ correspond to points on the Klein quadric

$$x_1x_2 + x_3x_4 + x_5x_6 = 0.$$

We will say something about polar spaces below.

The 15 Schoolgirls

The schoolgirls appear as binary vectors of length 4:

$\text{Girl}_0 = (1,0,0,0)$
$\text{Girl}_1 = (0,1,0,0)$
$\text{Girl}_2 = (0,0,1,0)$
$\text{Girl}_3 = (0,0,0,1)$
$\text{Girl}_4 = (1,1,1,1)$
$\text{Girl}_5 = (1,1,0,0)$
$\text{Girl}_6 = (1,0,1,0)$
$\text{Girl}_7 = (0,1,1,0)$
$\text{Girl}_8 = (1,1,1,0)$
$\text{Girl}_9 = (1,0,0,1)$
$\text{Girl}_{10} = (0,1,0,1)$
$\text{Girl}_{11} = (1,1,0,1)$
$\text{Girl}_{12} = (0,0,1,1)$
$\text{Girl}_{13} = (1,0,1,1)$
$\text{Girl}_{14} = (0,1,1,1)$

A Generalization

Following Hirschfeld, let us generalize Kirkman:

> *If* $(q^2+1)(q+1)$ *schoolgirls go walking each day in* q^2+1 *rows of* $q+1$*, they can walk for* q^2+q+1 *days so that each girl has walked in the same row as has every other girl and hence with no girl twice.*

The packings of $\mathrm{PG}(3,q)$ provide solutions to this problem.

Let us look at $q=3$.

The 40 Schoolgirls

One solution is:

Monday	6	14	43	60	61	80	90	94	114	119
Tuesday	0	29	47	54	88	97	100	109	115	124
Wednesday	2	17	33	39	58	68	79	96	112	129
Thursday	7	16	28	45	57	66	76	87	103	118
Friday	12	18	22	32	52	69	75	98	106	123
Saturday	9	40	59	70	77	81	99	101	104	127
Sunday	5	20	49	55	73	84	102	108	116	117
Day 8	8	24	26	42	51	67	82	111	113	126
Day 9	10	21	27	38	41	63	71	85	91	121
Day 10	3	15	36	44	64	65	89	95	105	125
Day 11	11	19	23	30	35	46	53	78	107	128
Day 12	1	31	50	56	62	72	74	86	93	120
Day 13	4	13	25	34	37	48	83	92	110	122

The numbers $0, \ldots, 129$ represent the 130 lines of $\mathrm{PG}(3,3)$.

The 40 Schoolgirls

This particular solution is special.

It has a symmetry group that is A_6 (of order 360).

What is known about Spreads and Packings?

- In $\mathrm{PG}(3,2)$ there is only the Desarguesian spread.
- There are exactly two packings of $\mathrm{PG}(3,2)$, they are dual to each other.
- In $\mathrm{PG}(3,3)$ there are exactly two spreads: The Desarguesian spread and the Hall spread.
- Prince 1997 finds 7 packings of $\mathrm{PG}(3,3)$ invariant under a group of order 5.
- It has been known for some time (Dennistion 1973, Prince 1997) that there are no regular packings in $\mathrm{PG}(3,3)$ (packings that consist only of the Desarguesian spread).

What is known about Spreads and Packings?

- Prince 1998 finds 2 transitive regular packings in $\mathrm{PG}(3,5)$. (in the paper, he claims that he has 45, but this has been pointed out to be incorrect by Penttila).
- Denniston 1972 finds regular packings in $\mathrm{PG}(3,8)$.
- Penttila and Williams 1998 find two infinite families of regular packings in $\mathrm{PG}(3,q)$ with $q \equiv 2 \bmod 3$. The two families are dual to each other. These examples generalize the Prince packings in $\mathrm{PG}(3,5)$ and the Denniston packings in $\mathrm{PG}(3,8)$. They do not arise for $\mathrm{PG}(3,3)$.

Packings in $\mathrm{PG}(3,3)$

B. 2013

There are 73343 packings in $\mathrm{PG}(3,3)$.

The distribution of the orders of the automorphism groups is:

$$360,\ 288^2,\ 48^2,\ 36^3,\ 32^6,\ 24^{12},\ 18^2,\ 16^{16},\ 12^8,\ 10^2,\ 8^{131},\ 6^{20},\ 5^4,\ 4^{554},\ 3^{54},\ 2^{2904},\ 1^{69622}.$$

Packings in $\mathrm{PG}(3,3)$

An Invariant:

Let j count the number of Desarguesian spreads in the packing.

Then $13 - j$ is the number of Hall spreads.

We consider $(j, 13 - j)$ the *type* of a packing in $\mathrm{PG}(3,3)$.

Our classification by type is as follows (The 7 packings of Prince are marked red in the table):

Type	Packings	Distribution of Automorphism Group Orders
(13, 0)	0	
(12, 1)	0	
(11, 2)	6	$10,\ 2,\ 1^{4}$
(10, 3)	12	$2^{2},\ 1^{10}$
(9, 4)	392	$16^{2},\ 8^{2},\ 4^{15},\ 2^{85},\ 1^{288}$
(8, 5)	574	$8^{2},\ 2^{54},\ 1^{518}$
(7, 6)	2406	$2^{48},\ 1^{2358}$
(6, 7)	4190	$10,\ 2^{79},\ 1^{4110}$
(5, 8)	9670	$4^{13},\ 2^{230},\ 1^{9427}$
(4, 9)	14391	$8^{4},\ 4^{26},\ 3^{32},\ 2^{311},\ 1^{14018}$
(3, 10)	15452	$4^{4},\ 2^{78},\ 1^{15370}$
(2, 11)	13395	$4^{24},\ 2^{270},\ 1^{13101}$
(1, 12)	9995	$360,\ 288^{2},\ 48^{2},\ 36^{3},\ 32^{2},\ 24^{12},\ 18^{2},\ 16^{10},\ 12^{8},\ 8^{104},\ 6^{20},\ 5^{4},\ 4^{369},\ 3^{22},\ 2^{1374},\ 1^{8060}$
(0, 13)	2860	$32^{4},\ 16^{4},\ 8^{19},\ 4^{103},\ 2^{372},\ 1^{2358}$

Subobjects

On Monday, professor Zhelezova discussed partial packings.

A partial packing is a set of pairwise line-disjoint spreads.

We consider as subobjects the partial packings of a certain size s, say.

The idea is to classify partial packings and then to somehow “lift” these to the packings.

Each partial packing must be lifted.

This lifting is done using a Computer Science primitive (Exact cover, Cliques in graphs, System of equations over the integers etc).

A final isomorph rejection step finishes the job.

Some Theory

So, in this application,

$\mathcal{A} =$ partial packings of size s,

$\mathcal{B} =$ packings (= partial packings of size $q^2 + q + 1$),

$\mathfrak{R}$ = inclusion of spreads.

Step 1: Classification of Subobjects

i	Partial Packings with i Spreads	Distribution of Stabilizer Orders	Average Stabilizer Order
0	1	12130560	12130560
1	2	5760, 1920	3840
2	17	$240, 120, 96, 48, 32^2, 24, 16^2, 12^2, 10, 8^2, 6, 4^2$	$40 + \frac{8}{17} = 40.471$
3	1,274	$240, 96, 72, 48^2, 32^2, 24^7, 16^8, 12^8, 10^2, 8^{32}, 6^{12}, 4^{85}, 3^{12}, 2^{341}, 1^{760}$	$2 + \frac{578}{1274} = 2.454$
4	219,066	$72, 64, 48^3, 40, 36, 32^3, 24^{11}, 18, 16^{11}, 12^{20}, 10, 8^{127}, 6^{31}, 4^{848}, 3^{22}, 2^{9312}, 1^{208672}$	$1 + \frac{14050}{219066} = 1.064$

Step 1: Classification of Subobjects

As we can see, the average order of the stabilizer of orbit representatives approaches 1.

This is how we choose s.

Some experimenting many be necessary.

Step 2: Liftings

Let $P_1, \ldots, P_m$ be representatives for the partial packings of size s under the action of $G = \mathrm{P\Gamma L}(4, q)$.

So,

$$\mathcal{A} = \bigcup_{i=1}^{m} G(P_i).$$

It remains to compute the liftings for each P_i.

$$N_{\mathcal{B}}(P_i) = \{(P_i, Q) \mid Q \text{ is a packing of } \mathrm{PG}(3, q) \text{ containing } P_i\}$$

This problem can be formulated as an Exact Cover Problem:

Exact Cover

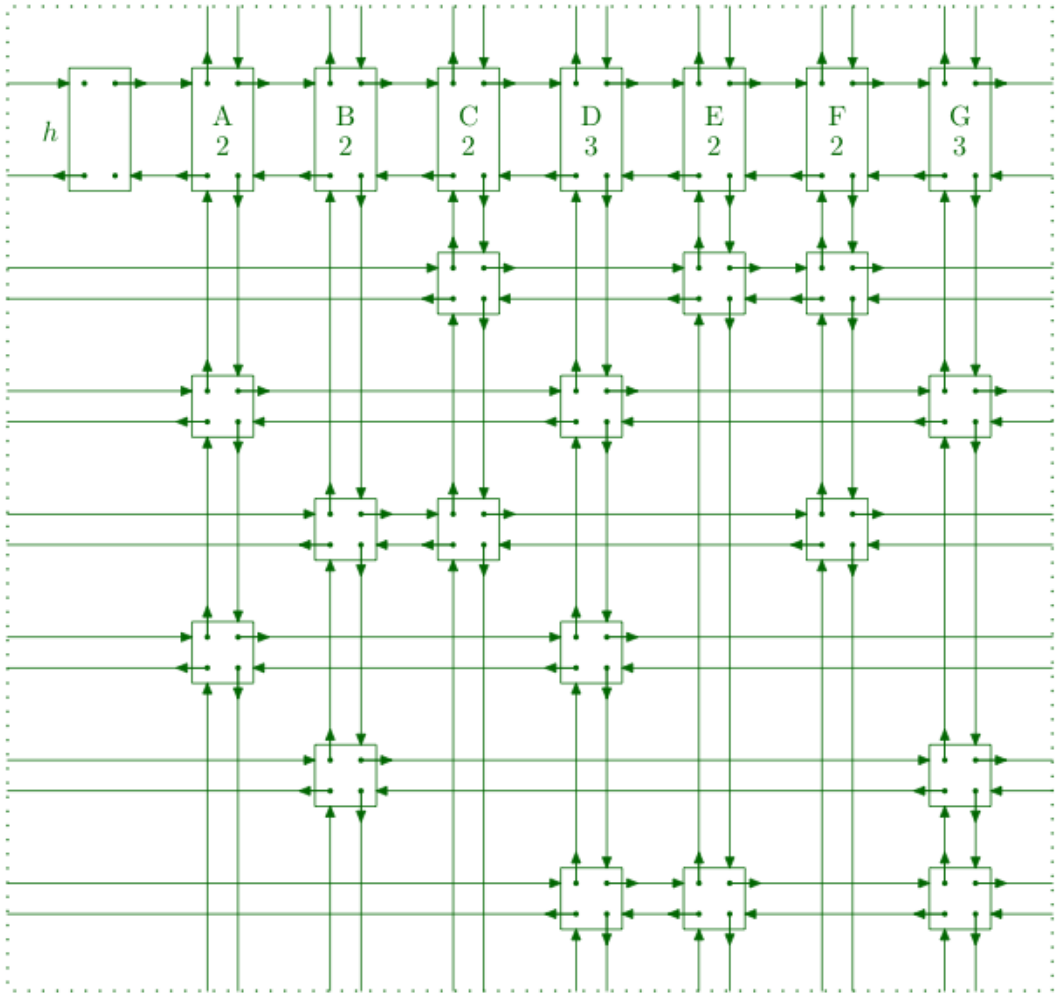
Given a 0/1 matrix:

$$\begin{bmatrix} 0&0&1&0&1&1&0 \\ 1&0&0&1&0&0&1 \\ 0&1&1&0&0&1&0 \\ 1&0&0&1&0&0&0 \\ 0&1&0&0&0&0&1 \\ 0&0&0&1&1&0&1 \end{bmatrix}$$

Find a selection of the rows such that each column (inside the selection) sums up to one:

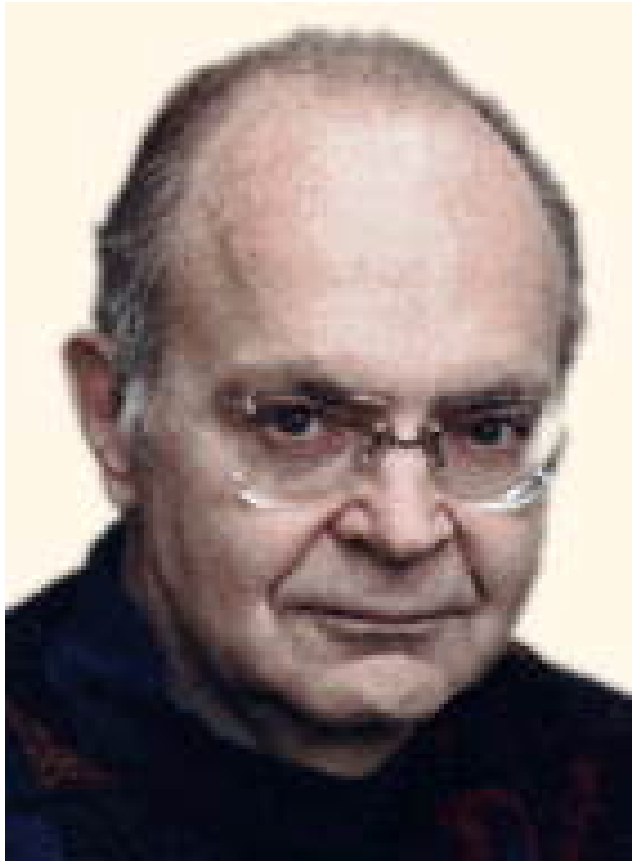
$$\begin{bmatrix} 0&0&1&0&1&1&0 \\ 1&0&0&1&0&0&1 \\ 0&1&1&0&0&1&0 \\ 1&0&0&1&0&0&0 \\ 0&1&0&0&0&0&1 \\ 0&0&0&1&1&0&1 \end{bmatrix}$$

Represent the coefficient matrix as a 2-dimensional doubly linked list:



Exact Cover

Don Knuth



uses this data structure to realize an efficient search algorithm, known under the name Dancing Links.

Step 3: Isomorph Rejection

Once the lifting is done, we move on to Step 3, the final isomorph rejection part.

For the isomorph rejection part, we use the LEMMA.

Orbits on Ordered Pairs

We would like to compute the classification

$$\mathcal{B} = \bigcup_{j=1}^{n} G(Q_j)$$

for some representatives $Q_1, \ldots, Q_m$ (yet to be determined).

The isomorph classification establishes the bijection ψ from the LEMMA.

This furnishes the representatives $Q_1, \ldots, Q_n$ such that

$$\mathcal{B} = \bigcup_{j=1}^{n} G(Q_j).$$

Summary

- We have classified packings for the field of order $q = 3$.
- We have data that can be analyzed to find new constructions of interesting planes.
- We have transformed the mathematical problem into a Computer Science problem (exact cover).

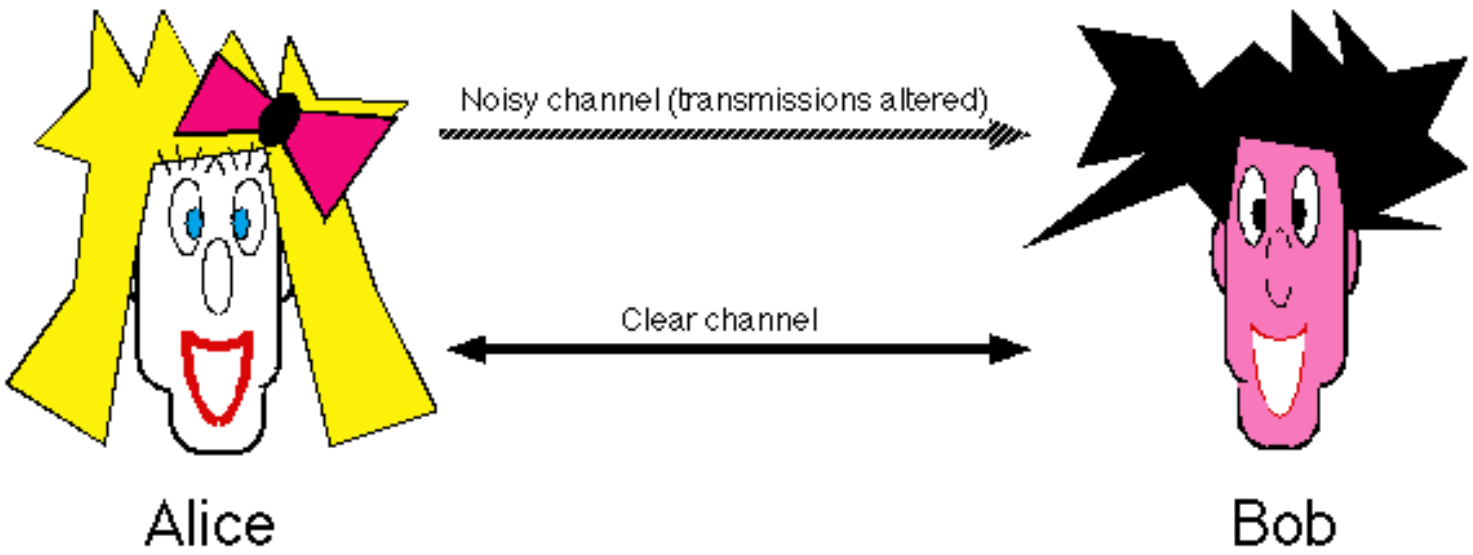
Topic # 3

Optimal Linear Codes

Why Codes?

Suppose Alice and Bob want to communicate.

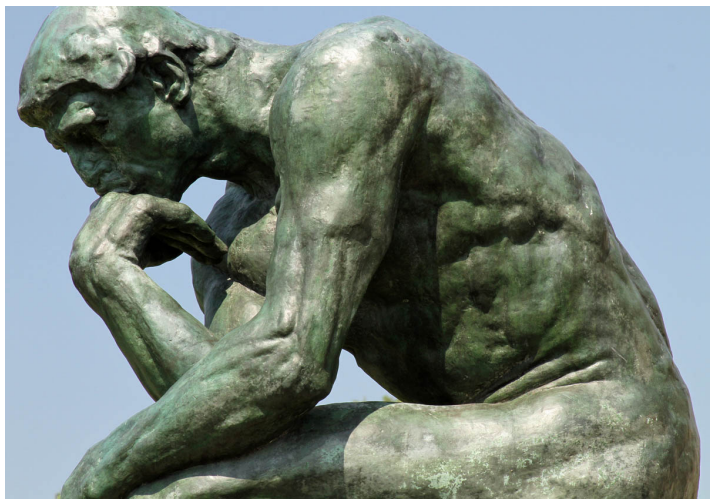
Suppose that the channel they use is 'noisy': bits can flip at any time.



Why Codes?

Bob may not recieve exactly what Alice has sent.

Is it still possible that Bob can figure out exactly what Alice was trying to say?



The thinker, by Rodin

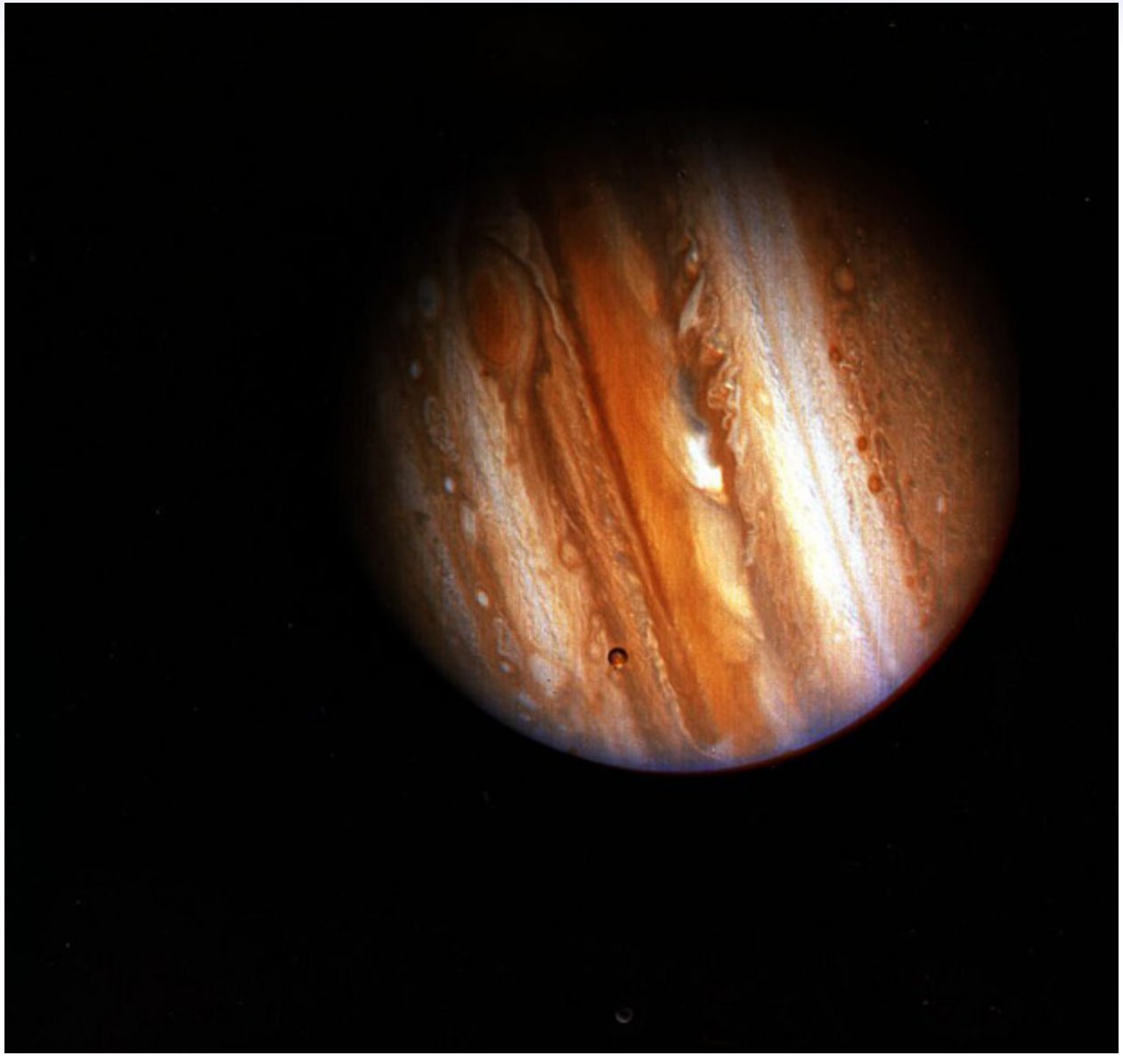
Why Codes?

"Very Large Array, Socorro, NM" photo by John Fowler 2012.

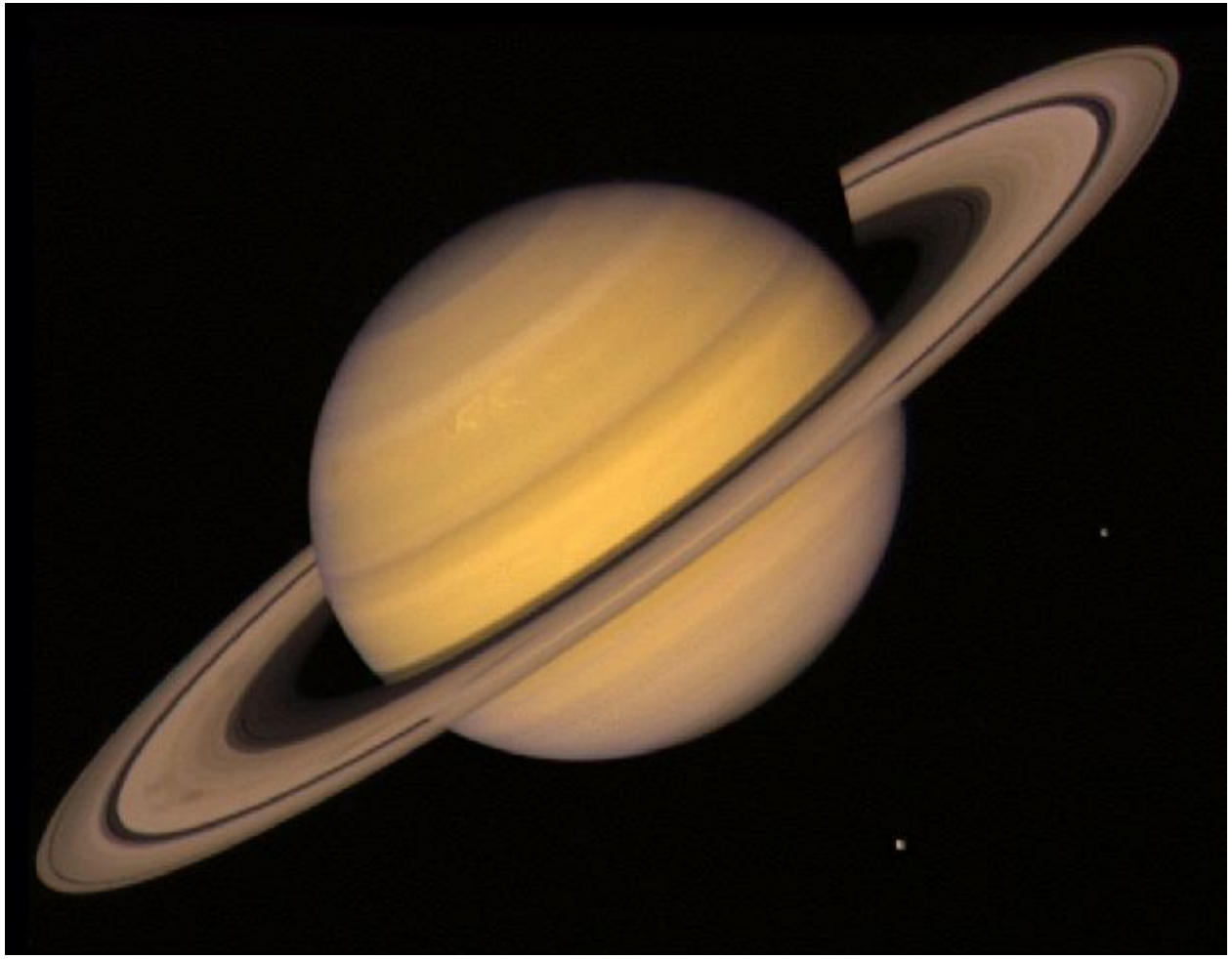
Why Codes?

Coding allows us to receive the pictures that were sent from the spacecraft even though some of the information is corrupted.

Coding is even more important if compressed files are sent.



Jupiter: Voyager flyby February 5, 1979



Saturn: Voyager 2 flyby, July 21, 1981.

Optimal Linear Codes

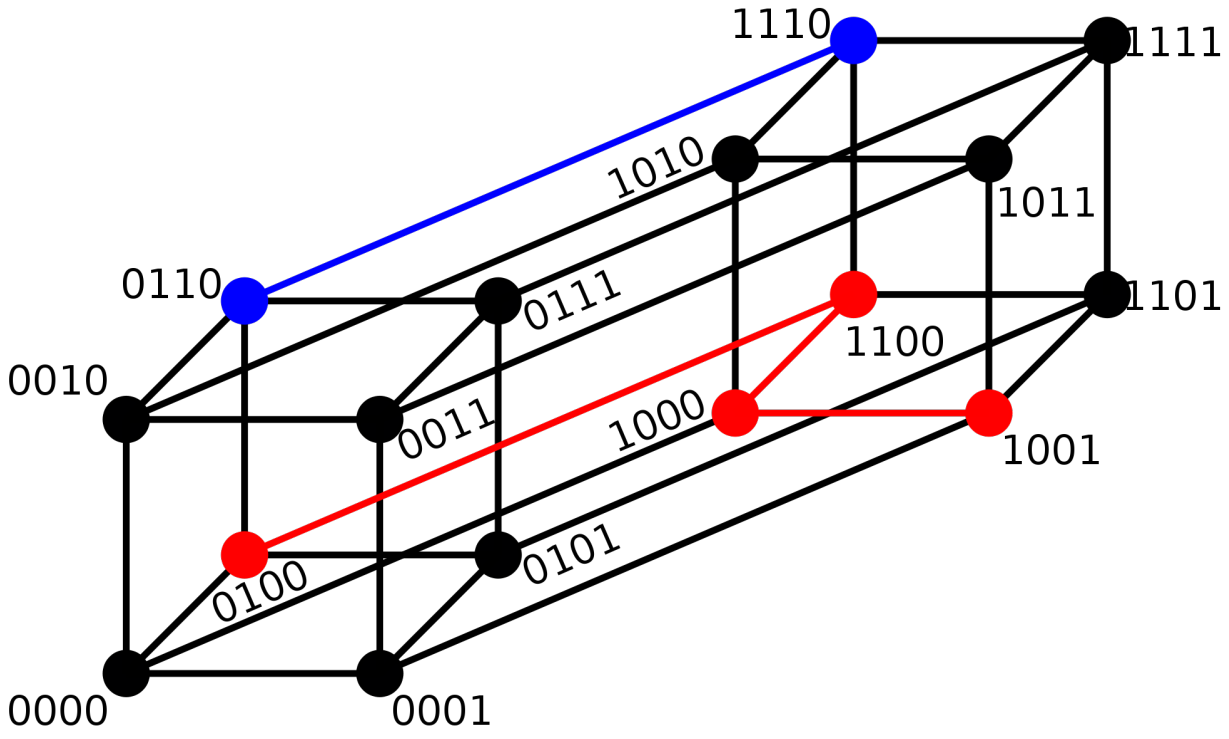
Recall: the Hamming distance between two vectors:

For two elements $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ in $V = \mathbb{F}_q^n$, let

$$d(\mathbf{x}, \mathbf{y}) = \#i : x_i \neq y_i$$

be the number of places where $\mathbf{x}$ and $\mathbf{y}$ differ.

Measuring the number of entries in which two vectors differ is the fundamental idea which leads to the *Hamming metric.*



This is a reference to Richard Hamming, another pioneer of coding theory.

Optimal Linear Codes

Example:
Using the binary expression of integers to denote vectors of zeros and ones, we write

$$d(0110011, 1010101) = 4,$$

since 0110011 and 1010101 differ in exactly 4 positions:

$$\begin{array}{ccccccc} 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \updownarrow & \updownarrow & & & \updownarrow & \updownarrow & \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}$$

Codes

A code $\mathcal{C}$ is a subset of $V = \mathbb{F}_q^n$.

A linear code is a code that is a linear subspace of $V = \mathbb{F}_q^n$.

The minimum distance of a code $\mathcal{C}$ is

$$d(\mathcal{C}) = \min\left\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{C},\ \mathbf{x} \neq \mathbf{y}\right\}.$$

Linear Codes

For a linear code, one can show that

$$d(\mathcal{C}) = \min_{\mathbf{x} \in \mathcal{C} \setminus \{0\}} \mathrm{wt}(\mathbf{x})$$

where

$$\mathrm{wt}(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$$

is the number of nonzero entries of $\mathbf{x}$.

Suppose that a codeword $\mathbf{c}$ was sent and $\mathbf{c}'$ was received.

Under the assumption that a bit flip on the channel is less likely than a correct transmission, it make sense to correct $\mathbf{c}'$ to the nearest codeword $\mathbf{c}$.

This is known as maximum likelihood decoding.

It leads us to consider the metric balls around codewords.

We choose the largest radius such that all metric balls centered at codewords are disjoint.

We say that a code

$$\mathcal{C} = \{\mathbf{c}_1, \ldots, \mathbf{c}_N\}$$

can correct e errors if the metric balls of radius e centered around codewords are disjoint.

Theorem: A code $\mathcal{C}$ can correct e errors if any two codewords are at least $2e + 1$ apart.

Linear Codes

A linear code of length n and dimension k and minimum distance d is denoted as a

$$[n, k, d]$$

code.

Theorem: A code with minimum distance d can correct $\lfloor \frac{d-1}{2} \rfloor$ errors.

Linear Codes

Let $\mathcal{C}$ be a linear code.

Let $\mathcal{C}^{\perp}$ be the dual subspace (dual code).

A generator matrix Γ for $\mathcal{C}$ is a $k \times n$ matrix whose rows form a basis for $\mathcal{C}$.

Linear Codes

A check matrix Δ is a $(n-k) \times n$ matrix whose rows form a basis for the dual code $C^{\perp}$.

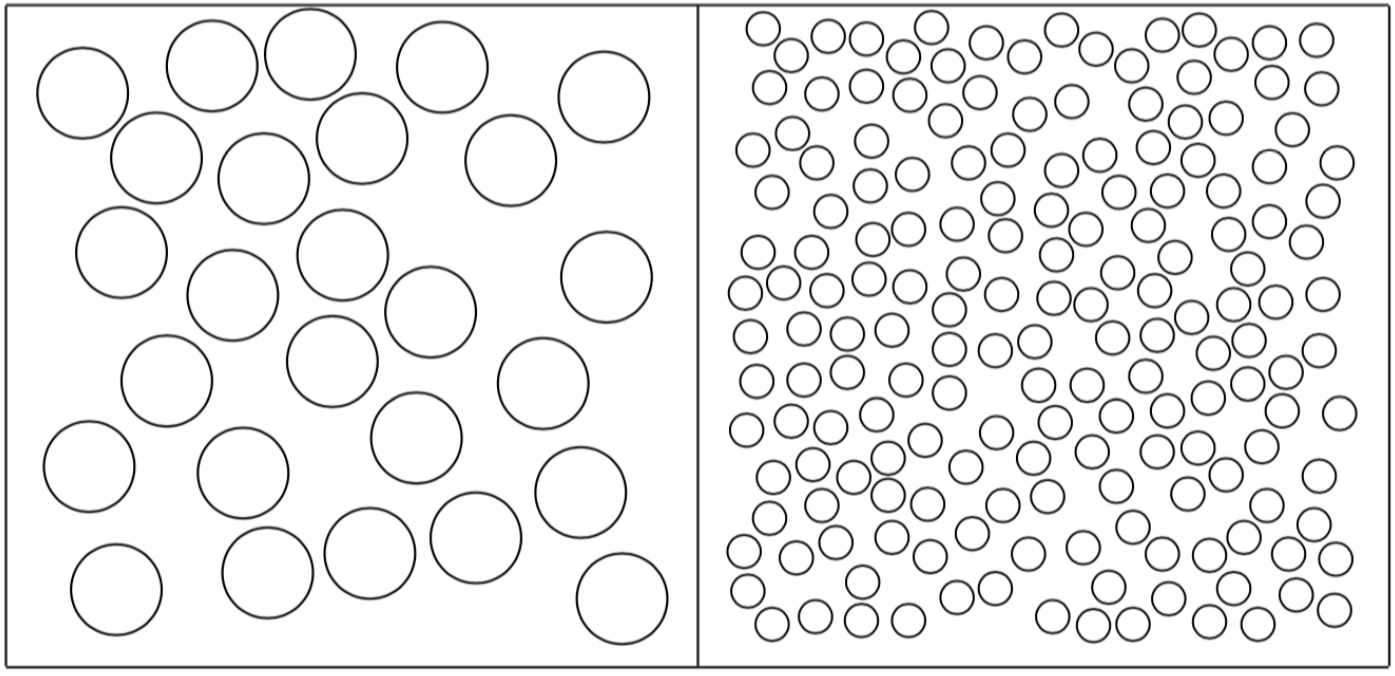
Thus, $\Gamma \cdot \Delta^{\top} = 0$.

Linear Codes

What we want is:

- n should be small,
- k should be large,
- d should be large.

These are contradicting aims.



You cannot fill a fixed size box with very many balls if the balls are supposed to be large.

Linear Codes

The *Singleton bound*:

$$d \leq n - k + 1$$

for any $[n, k, d]$ code.

A code whose parameters $[n, k, d]$ attain equality in the Singleton bound is called MDS-code (maximum distance separable).

Example: Reed Solomon codes.

Optimal Linear Codes

The *Hamming bound*:

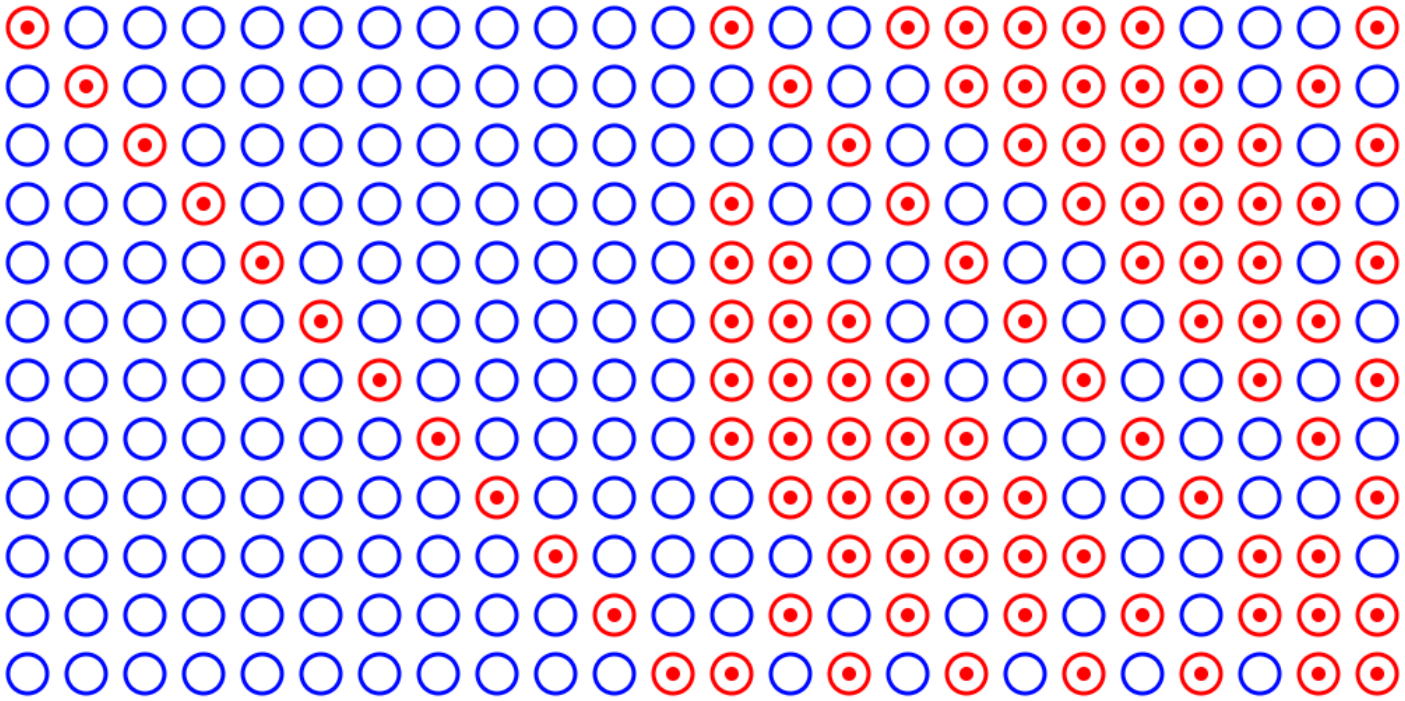
$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} (q-1)^i \binom{n}{i} \leq q^{n-k}.$$

A code whose parameters $[n, k, d]$ attain equality in the Hamming bound is called perfect.

Unfortunately, there are not many perfect codes.

Good Codes

Some good codes pop out of nowhere:



The binary Golay code. Shown is the 12×24 generator matrix. The code is the rowspan of this matrix.

The Golay code has minimum distance 8 and therefore can correct 3 errors.

Optimal Linear Codes

A code is optimal if the minimum distance is best possible among all codes of equal length and dimension.

Idea: Use computers to search for optimal linear coders.

THEOREM

Let C be a linear code over $\mathbb{F}_q$ with check matrix Δ. The following are equivalent:

- C has minimum distance d
- In Δ, any $d-1$ columns are linearly independent and there exist d columns that are linearly dependent.

Projective Codes

A code is called projective if

- No coordinate is always zero.
- No two coordinates are linearly dependent.

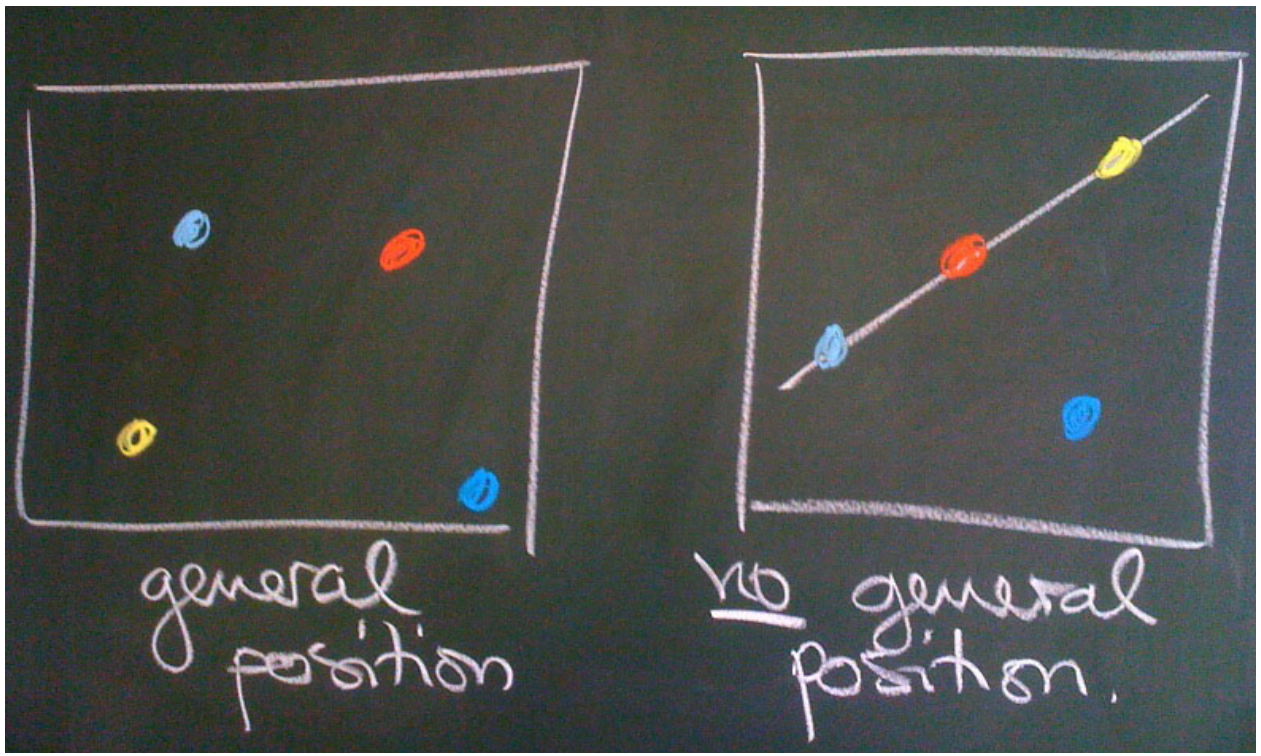
Let C be a projective code with $k \times n$ generator matrix Γ.

$$\mathbf{x}_0, \ldots, \mathbf{x}_{n-1} \text{ the columns of } \Gamma.$$

$$\Updownarrow$$

$$\mathbf{P}(\mathbf{x}_0), \ldots, \mathbf{P}(\mathbf{x}_{n-1}) \text{ a set of points in } \mathrm{PG}(k-1, q).$$

A set of points in $\mathrm{PG}(s, q)$ is *r-independent* if any r elements are in general position (i.e., span a subspace of algebraic dimension r).



4 points in a plane

Recipe for Finding Good Codes

In order to find $[n, k, \geq d]_q$ codes, we have to find n points in $\mathrm{PG}(n-k-1, q)$ with the property that

Any $d-1$ are independent.

In order to reduce excess searching, we need to talk about Code Isomorphism.

Let's create good codes:

Motivating example:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \omega & \omega^2 \\ 0 & 0 & 1 & 1 & \omega^2 & \omega \end{bmatrix}$$

corresponds to the set of size 6 in $\mathrm{PG}(2,4)$

$$P(1,0,0),\ P(0,1,0),\ P(0,0,1),\ P(1,1,1),\ P(1,\omega,\omega^2),\ P(1,\omega^2,\omega).$$

No three points are collinear. The minimum distance is 4.

Vector Spaces over Finite Fields

$\mathbb{F}_{q^s}^k$ the k-dimensional vector space over $\mathbb{F}_{q^s}$.

Two types of subspaces:

- $\mathbb{F}_{q^s}^i$ for $i \leq k$ is called subspace
- $\mathbb{F}_{q^i}^k$ for $i \mid s$ is called subfield subspace

A basis is a set of linearly independent vectors that spans the subspace over

- $\mathbb{F}_{q^s}$
- $\mathbb{F}_{q^i}$

Cyclic Codes

A code C is cyclic if

$$(c_0, c_1, \ldots, c_{n-1}) \in C \iff (c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

Example: BCH codes, Reed-Solomon codes.

Remark:

- Cyclic codes are in 1 to 1 correspondence to the ideals in the ring $\mathbb{F}_q[X]/(X^n - 1)$ (provided $\gcd(n, q) = 1$).

Constacyclic Codes

A code C is constacyclic if

$$(c_0, c_1, \ldots, c_{n-1}) \in C \iff (\kappa c_{n-1}, c_0, \ldots, c_{n-2}) \in C$$

for some $\kappa \in \mathbb{F}_q^\times$ (the same κ for every $\mathbf{c} \in C$).

A constacyclic code is cyclic if $\kappa = 1$.

Example: see below

Permutational, Monomial and Semilinear Isometry

Isometric Codes: Different codes may behave the same way with respect to the Hamming metric.

There are three types of code isometries:

- Permutational isometries (permuting the coordinates),
- Monomial isometries (permuting the coordinates and multiplying non-zero constants),
- Semilinear isometries (all of the above plus field automorphisms).

When we say 'Code', we often mean the *equivalence class of isometric codes*.

In this sense, a code can be cyclic / constacyclic in many different ways, according to different arrangements of the coordinates.

Permutational, Monomial and Semilinear Automorphism Groups

An automorphism is a isometry (of the Hamming space) that maps the code to itself.

There are three types of automorphism groups:

- Permutational automorphism group PAut,
- Monomial automorphism group MAut,
- Semilinear automorphism group $\Gamma\mathrm{Aut}$.

$$\mathrm{PAut} \leq \mathrm{MAut} \leq \Gamma\mathrm{Aut}.$$

Automorphisms of Projective Space

We need to understand the automorphisms of projective space.

An automorphism of projective space is an

incidence preserving isomorphism

(also called collineation).

Two sets A and B in $\mathrm{PG}(n, q)$ are projectively equivalent if there is an automorphism α of $\mathrm{PG}(n, q)$ with $\alpha(A) = B$.

Some One-to-One Correspondences

There is a one-to-one correspondence

$$\left\{ \begin{array}{c} \text{isometry classes} \\ \text{of projective} \\ [n,k]_q\text{-codes} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{projective equivalence} \\ \text{classes of } n\text{-point-sets} \\ \text{in } \mathrm{PG}(n-k-1,q) \end{array} \right\}$$

There is a one-to-one correspondence

$$\left\{ \begin{array}{c} \text{isometry classes} \\ \text{of projective} \\ [n,k,\geq d]_q\text{-codes} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{projective equivalence} \\ \text{classes of } n\text{-point-sets} \\ \text{in } \mathrm{PG}(n-k-1,q) \\ \text{any } d-1 \text{ independent} \end{array} \right\}$$

Using an algorithm to classify orbit on subsets, optimal codes can be classified.

Tables of optimal linear codes have been computed (and put on the web).

	k=1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
n=1															
2															
3															
4	4^1														
5	5^1	3^1													
6	6^1	$4^1\ 3^1$	3^1												
7	7^1	$4^2\ 3^1$	$4^1\ 3^3$	3^1											
8	8^1	$5^1\ 4^2$	$4^3\ 3^6$	$4^1\ 3^4$											
9	9^1	$6^1\ 5^2\ 4^2$	4^8	$4^4\ 3^{18}$	3^5										
10	10^1	$6^2\ 5^2\ 4^2$	$5^2\ 4^{18}$	4^{19}	$4^4\ 3^{36}$	3^4									
11	11^1	$7^1\ 6^3\ 5^2$	$6^1\ 5^8\ 4^{29}$	$5^1\ 4^{66}$	4^{30}	$4^2\ 3^{58}$	3^3								
12	12^1	$8^1\ 7^2\ 6^3\ 5^2$	$6^6\ 5^{19}$	$6^1\ 5^{12}\ 4^{201}$	4^{214}	4^{41}	$4^2\ 3^{84}$	3^2							
13	13^1	$8^2\ 7^3\ 6^3$	$7^1\ 6^{16}\ 5^{37}$	$6^6\ 5^{72}$	$5^{15}\ 4^{1159}$	4^{580}	4^{45}	$4^1\ 3^{109}$	3^1						
14	14^1	$9^1\ 8^3\ 7^3$	$8^1\ 7^5\ 6^{37}$	$7^1\ 6^{39}\ 5^{292}$	$6^6\ 5^{261}$	$5^{11}\ 4^{6704}$	4^{1488}	4^{48}	$4^1\ 3^{126}$	3^1					
15	15^1	$10^1\ 9^2\ 8^4\ 7^3$	$8^3\ 7^{17}$	$8^1\ 7^5\ 6^{195}$	$7^1\ 6^{91}\ 5^{2547}$	$6^5\ 5^{995}$	$5^6\ 4^{41037}$	4^{3473}	4^{43}	$4^1\ 3^{142}$	3^1				
16	16^1	$10^2\ 9^3\ 8^4$	$8^{12}\ 7^{41}$	$8^4\ 7^{37}$	$8^1\ 7^5\ 6^{1145}$	$6^{180}\ 5^{29826}$	$6^3\ 5^{4010}$	$5^1\ 4^{268258}$	4^{7456}	4^{47}	$4^1\ 3^{143}$				
17	17^1	$11^1\ 10^3\ 9^4\ 8^4$	$9^2\ 8^{32}$	$8^{18}\ 7^{241}$	$8^4\ 7^{84}$	7^3	6^{377}	$6^1\ 5^{13757}$	5^1	4^{14390}	4^{39}	3^{129}			
18	18^1	$12^1\ 11^2\ 10^4\ 9^4$	$10^1\ 9^{11}\ 8^{71}$	8^{108}	$8^{34}\ 7^{1777}$	$8^2\ 7^{108}$	7^2	6^{918}	$6^1\ 5^{29371}$		4^{25024}	4^{33}	3^{113}		
19		$12^2\ 11^3\ 10^5$	$10^6\ 9^{33}$	$9^7\ 8^{550}$	8^{411}	$8^{28}\ 7^{19021}$	$8^1\ 7^{81}$	7^1	6^{1700}	5^{31237}		4^{39302}	4^{25}	3^{91}	
20			$11^1\ 10^{21}$	$10^3\ 9^{81}$	$9^3\ 8^{6480}$	8^{1833}	8^{26}	$8^1\ 7^{33}$	7^1	6^{1682}	5^{14135}			4^{24}	3^{67}
21				10^{27}	$10^2\ 9^{178}$			8^{12}	$8^1\ 7^{20}$	7^1	6^{739}	5^{2373}			4^{16}
22					10^{37}	9^{248}			8^9	$8^1\ 7^{15}$	7^1	6^{128}	5^{128}		
23						10^{29}	9^{29}			8^8	$8^1\ 7^{15}$	7^1	6^8	5^1	
24							10^6				8^9	$8^1\ 7^{11}$		6^1	
25												8^7			
26															

Families of new codes have been found.

We call them twisted tensor product codes.

In the Number Theory community, the construction is known as Weil descent.

Results

THEOREM 1 (B. 2008)

A) There exist constacyclic $[q^2+1, q^2-8, \geq 6]_q$ for any $q \geq 3$. They are cyclic if and only if q is even.

B) There exist $[q^2+2, q^2-7, \geq 6]_q$ codes for any $q \geq 4$ even.

In both cases, the codes are invariant under $\mathrm{P\Gamma L}(2, q^2)$.

THEOREM 2 (B. 2008)

There exist constacyclic $[q^3+1, q^3-7, \geq 5]_q$ for any $q \geq 3$. The codes are invariant under $\mathrm{P\Gamma L}(2, q^3)$.

$q = p^h$, p prime.

$$\mathbb{F}_q = \{\alpha^i \mid i = 0, \ldots, q-2\} \cup \{0\}.$$

α a primitive element over $\mathbb{F}_p$.

$\Phi : t \mapsto t^p$ the Frobenius automorphism.

The Construction

Let $V_n = \mathbb{F}_{q^s}^n$ be an n-dimensional vector space over $\mathbb{F}_{q^s}$.

Consider

$$\otimes_s V_n := V_n \otimes V_n \otimes \cdots \otimes V_n \quad (s \text{ times})$$

Define a mapping

$$\iota_s : V_n \to \otimes_s V_n,$$

$$x \mapsto x \otimes \phi_s(x) \otimes \phi_s^2(x) \otimes \cdots \otimes \phi_s^{s-1}(x).$$

This induces a mapping between the corresponding projective spaces:

$$\iota_s : \mathbf{P}(V_n) \to \mathbf{P}(\otimes_s V_n)$$

The Construction

The points of $\mathrm{PG}(1,q)$ are often identified as follows:

$$\mathbf{P}(1,t) \leftrightarrow t, \quad \mathbf{P}(0,1) \leftrightarrow \infty$$

The Veronese map

$$\nu_k : \mathrm{PG}(1,q) \to \mathrm{PG}(k-1,q), \quad \mathbf{P}(a,b) \mapsto \mathbf{P}(a^k, a^{k-1}b, \ldots, b^k)$$

$\nu_2(\mathrm{PG}(1,q))$ is the conic

$$\{\mathbf{P}(1,t,t^2), \quad t \in \mathbb{F}_{q^2}\} \cup \{\mathbf{P}(0,0,1)\}.$$

The Construction

Consider

- $\iota_2 \circ \nu_3(\mathrm{PG}(1, q^2)) \Rightarrow n = q^2 + 1$ points in $\mathrm{PG}(8, q^2)$
- $\iota_3(\mathrm{PG}(1, q^3)) \Rightarrow n = q^3 + 1$ points in $\mathrm{PG}(7, q^3)$

The image lies in an $\mathbb{F}_q$-subfield subspace.

- $\mathrm{PG}(8, q)$
- $\mathrm{PG}(7, q)$

The codes are projective codes whose point sets are the subspace bases. For Theorem 1 B, add the nucleus to the conic $\nu_2(\mathrm{PG}(1, q))$ (recall that $2 \mid q$ in this case).

Example: Theorem 1

Using $t = 0, 1, \ldots, \infty$ for the points of the projective line, the ν_2 image of $\mathrm{PG}(1, q^2)$ is the conic

$$\{\mathbf{P}(1, t, t^2), \quad t \in \mathbb{F}_{q^2}\} \cup \{\mathbf{P}(0, 0, 1)\}.$$

The ι_2-image of this set is

$$\{\mathbf{P}\underbrace{(1, t^{q+1}, t^{2q+2}, t^q, t, t^{2q}, t^2, t^{2q+1}, t^{q+2})}_{=:\mathbf{y}_t}, \quad t \in \mathbb{F}_{q^2}\}$$

together with $\mathbf{P}\underbrace{(0, 0, 1, 0, 0, 0, 0, 0, 0)}_{\mathbf{y}_\infty}$.

$\otimes$	$\phi(1)$ 1	$\phi(t)$ t^q	$\phi(t^2)$ t^{2q}
1	1	t^q	t^{2q}
t	t	t^{q+1}	t^{2q+1}
t^2	t^2	t^{q+2}	t^{2q+2}

ordering of basis elts.

0	3	5
4	1	7
6	8	2

Example $q = 16$ (with $\alpha^4 = \alpha + 1$):

$$M = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & \alpha^5 & \alpha^5 & \alpha^{10} & \alpha^{10} & \alpha^{10} & \alpha^5 & 1 & \alpha^{10} & 1 & \alpha^5 & 1 & \alpha^5 & \alpha^{10} & 1 & 0 & 1 \\
0 & 1 & \alpha^{10} & \alpha^{10} & \alpha^5 & \alpha^5 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & 1 & \alpha^{10} & 1 & \alpha^{10} & \alpha^5 & 1 & 1 & 0 \\
0 & 1 & \alpha^4 & \alpha & \alpha^8 & \alpha^2 & \alpha^5 & \alpha^{10} & \alpha^{12} & \alpha^{11} & \alpha^6 & \alpha^{13} & \alpha^9 & \alpha^7 & \alpha^{14} & \alpha^3 & 0 & 0 \\
0 & 1 & \alpha & \alpha^4 & \alpha^2 & \alpha^8 & \alpha^5 & \alpha^{10} & \alpha^3 & \alpha^{14} & \alpha^9 & \alpha^7 & \alpha^6 & \alpha^{13} & \alpha^{11} & \alpha^{12} & 0 & 0 \\
0 & 1 & \alpha^8 & \alpha^2 & \alpha & \alpha^4 & \alpha^{10} & \alpha^5 & \alpha^9 & \alpha^7 & \alpha^{12} & \alpha^{11} & \alpha^3 & \alpha^{14} & \alpha^{13} & \alpha^6 & 0 & 0 \\
0 & 1 & \alpha^2 & \alpha^8 & \alpha^4 & \alpha & \alpha^{10} & \alpha^5 & \alpha^6 & \alpha^{13} & \alpha^3 & \alpha^{14} & \alpha^{12} & \alpha^{11} & \alpha^7 & \alpha^9 & 0 & 0 \\
0 & 1 & \alpha^9 & \alpha^6 & \alpha^3 & \alpha^{12} & 1 & 1 & \alpha^{12} & \alpha^6 & \alpha^6 & \alpha^3 & \alpha^9 & \alpha^{12} & \alpha^9 & \alpha^3 & 0 & 0 \\
0 & 1 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^3 & 1 & 1 & \alpha^3 & \alpha^9 & \alpha^9 & \alpha^{12} & \alpha^6 & \alpha^3 & \alpha^6 & \alpha^{12} & 0 & 0
\end{bmatrix}$$

This is a generator matrix of an $[18, 9, 8]$ code over $\mathbb{F}_{16}$ (with automorphism group $\mathrm{P\Gamma L}(2, 16)$).

Example: Theorem 1

The image lies in an $\mathbb{F}_q$-subfield subspace.

Need: Base change.

Observe that for $\mathbb{F}_q^2 = \mathbb{F}_q(\beta)$ we have

$$\begin{bmatrix} 1 & 1 \\ \beta & \beta^q \end{bmatrix} \cdot \begin{bmatrix} t \\ t^q \end{bmatrix} = \begin{bmatrix} t + t^q \\ \beta t + \beta^q t^q \end{bmatrix} = \begin{bmatrix} T_2(t) \\ T_2(\beta t) \end{bmatrix}$$

which is in the (quadratic) subfield $\mathbb{F}_q$.

Apply this trick in general:

Example: Theorem 1

$$S_\beta \mathbf{y}_t^\top = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & 1 & & & \\ & & \beta^q & & \beta & & & \\ & & & & & 1 & 1 & \\ & & & & & \beta^q & \beta & \\ & & & & & & & 1 \ 1 \\ & & & & & & & \beta^q \beta \end{pmatrix} \begin{pmatrix} 1 \\ t^{q+1} \\ t^{2q+2} \\ t^q \\ t \\ t^{2q} \\ t^2 \\ t^{2q+1} \\ t^{q+2} \end{pmatrix} = \begin{pmatrix} 1 \\ t^{q+1} \\ t^{2q+2} \\ t^q + t \\ \beta^q t^q + \beta t \\ t^{2q} + t^2 \\ \beta^q t^{2q} + \beta t^2 \\ t^{2q+1} + t^{q+2} \\ \beta^q t^{2q+1} + \beta t^{q+2} \end{pmatrix} = \begin{pmatrix} 1 \\ N_2(t) \\ N_2(t^2) \\ T_2(t) \\ T_2(\beta t) \\ T_2(t^2) \\ T_2(\beta t^2) \\ T_2(t^{q+2}) \\ T_2(\beta t^{q+2}) \end{pmatrix} = \mathbf{x}_t^\top$$

Let Δ be the check matrix whose columns are the $\mathbf{x}_t$, $t \in \mathbb{F}_{q^2}$ and $\mathbf{x}_\infty = \mathbf{y}_\infty$. This defines the code.

Example: Theorem 1

Here, the image lies in an $\mathbb{F}_4$ subspace.

The base change matrix is

$$S_\beta = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^8 & \alpha^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha^8 & \alpha^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^8 & \alpha^2 \end{bmatrix}$$

Example: Theorem 1

$$S_\beta \cdot M = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & \alpha^5 & \alpha^5 & \alpha^{10} & \alpha^{10} & \alpha^{10} & \alpha^5 & 1 & \alpha^{10} & 1 & \alpha^5 & 1 & \alpha^5 & \alpha^{10} & 1 & 0 & 1 \\
0 & 1 & \alpha^{10} & \alpha^{10} & \alpha^5 & \alpha^5 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & 1 & \alpha^{10} & 1 & \alpha^{10} & \alpha^5 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \alpha^{10} & \alpha^{10} & \alpha^5 & \alpha^5 & \alpha^5 & \alpha^5 & \alpha^{10} & \alpha^{10} & 0 & 0 \\
0 & 1 & \alpha^{10} & \alpha^5 & 1 & 0 & \alpha^5 & \alpha^{10} & 0 & 1 & \alpha^{10} & \alpha^5 & 1 & 0 & \alpha^5 & \alpha^{10} & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \alpha^5 & \alpha^5 & \alpha^{10} & \alpha^{10} & \alpha^{10} & \alpha^{10} & \alpha^5 & \alpha^5 & 0 & 0 \\
0 & 1 & 1 & 0 & \alpha^5 & \alpha^{10} & \alpha^{10} & \alpha^5 & 1 & 0 & 0 & 1 & \alpha^{10} & \alpha^5 & \alpha^5 & \alpha^{10} & 0 & 0 \\
0 & 0 & \alpha^5 & \alpha^5 & \alpha^{10} & \alpha^{10} & 0 & 0 & \alpha^{10} & \alpha^5 & \alpha^5 & \alpha^{10} & \alpha^5 & \alpha^{10} & \alpha^5 & \alpha^{10} & 0 & 0 \\
0 & 1 & 1 & \alpha^{10} & \alpha^{10} & 0 & 1 & 1 & 0 & \alpha^{10} & \alpha^{10} & \alpha^{10} & 1 & 0 & 1 & \alpha^{10} & 0 & 0
\end{bmatrix}$$

Example: Theorem 1

Or, with $\omega = \alpha^5$ a primitive element for $\mathbb{F}_4$ with $\omega^2 = \omega + 1$.

$$\left[\begin{array}{cccccccccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & \omega & \omega & \omega^2 & \omega^2 & \omega^2 & \omega & 1 & \omega^2 & 1 & \omega & 1 & \omega & \omega^2 & 1 & 0 & 1 \\
0 & 1 & \omega^2 & \omega^2 & \omega & \omega & \omega & \omega^2 & 1 & \omega & 1 & \omega^2 & 1 & \omega^2 & \omega & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \omega^2 & \omega^2 & \omega & \omega & \omega & \omega & \omega^2 & \omega^2 & 0 & 0 \\
0 & 1 & \omega^2 & \omega & 1 & 0 & \omega & \omega^2 & 0 & 1 & \omega^2 & \omega & 1 & 0 & \omega & \omega^2 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \omega & \omega & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & 0 & 0 \\
0 & 1 & 1 & 0 & \omega & \omega^2 & \omega^2 & \omega & 1 & 0 & 0 & 1 & \omega^2 & \omega & \omega & \omega^2 & 0 & 0 \\
0 & 0 & \omega & \omega & \omega^2 & \omega^2 & 0 & 0 & \omega^2 & \omega & \omega & \omega^2 & \omega & \omega^2 & \omega & \omega^2 & 0 & 0 \\
0 & 1 & 1 & \omega^2 & \omega^2 & 0 & 1 & 1 & 0 & \omega^2 & \omega^2 & \omega^2 & 1 & 0 & 1 & \omega^2 & 0 & 0
\end{array}\right]$$

Or, in standard form...

Example: Theorem 1

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & \omega^2 & \omega \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & \omega & \omega^2 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & \omega & 0 & \omega^2 & 0 & \omega & 1 & \omega & \omega & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & \omega^2 & 0 & \omega & 1 & \omega & 1 & \omega^2 & \omega^2 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & \omega^2 & 0 & \omega^2 & \omega & 0 & \omega^2 & 1 & \omega^2 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \omega & 0 & \omega & 0 & \omega^2 & 0 & \omega^2 & 1 & \omega \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & \omega^2 & \omega & \omega & \omega^2 & \omega & \omega \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \omega^2 & \omega^2 & \omega & \omega & \omega^2 & \omega^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & \omega & \omega & \omega^2 & \omega^2 & \omega^2 & \omega^2
\end{bmatrix}$$

Are The Codes New?

The following question arises:

QUESTION 1

Are the codes of Theorem 1 and 2 new?

Fact 1: There are BCH-codes with the same parameters as the codes in Theorem 1 A (see below).

Fact 2: There are codes with the same parameters as the duals of the codes in Theorem 2

Fact 1: A Class of BCH codes

For $n = q^2 + 1$, take the cyclotomic sets of $0, 1, 2$ mod $q^2 + 1$:

$\{0\}$
$\{1, q, q^2 \equiv -1, -q, -q^2 \equiv 1\}$
$\{2, 2q, 2q^2 \equiv -2, -2q, -2q^2 \equiv 2\}$

9 roots, in order:

$$-2q,\ -q,\ \underbrace{-2,\ -1,\ 0,\ 1,\ 2,}_{\text{consecutive set}}\ q,\ 2q,$$

This yields a $[q^2 + 1, q^2 - 8, \geq 6]_q$ BCH-code.

(minimum distance ≥ 6 b/c we have a consecutive set of size 5)

Are The Codes New?

Since BCH-codes are cyclic, we ask:

QUESTION 2

Are the codes of Theorem 1 and 2 cyclic?

If we can show that the codes of Theorem 1 A are not cyclic, then we have shown that they are not BCH-codes and hence (likely) new.

We ask:

QUESTION 3

Given a projective code, how can we tell if the code is cyclic?

When is a Projective Code Cyclic?

C is constacyclic $\iff$

There exists a code automorphism α with

$$\alpha(\mathbf{x}_0) = \mathbf{x}_1,\ \alpha(\mathbf{x}_1) = \mathbf{x}_2,\ \ldots \alpha(\mathbf{x}_{n-1}) = \kappa\mathbf{x}_0.$$

C is cyclic $\iff$ the above with $\kappa = 1$.

When is a Projective Code Cyclic?

The codes are images of $\mathrm{PG}(1, q)$. Thus we ask:

QUESTION 4

What are the cyclic collineations of $\mathrm{PG}(n, q)$?

Cyclic Collineations of Projective Space

LEMMA: (Hirschfeld 1973)

$\#$ conjugacy classes of cyclic projectivities of $\mathrm{PG}(d-1,q)$

$= \frac{1}{q-1} \cdot \#$ subprimitive polynomials of degree d over $\mathbb{F}_q$

$= \frac{\Phi(\theta_{d-1}(q))}{d}$ (with Φ Euler's totient function)

This answers the question for when a code is constacyclic. We still need the find the answer for when it is cyclic.

When is a Projective Code Cyclic?

C is constacyclic $\iff$

There exists a code automorphism α with matrix T s.t.

$$T^n \mathbf{x}_0 = \kappa \mathbf{x}_0, \quad \kappa \neq 0, \quad \text{and} \quad T^i \mathbf{x}_0 \notin \langle \mathbf{x}_0 \rangle \quad i = 1, \ldots, n-1$$

C is cyclic $\iff$ the above with $\kappa = 1$.

The Exponent of a Polynomial

Definition

Let $m(x) \in \mathbb{F}_q[x]$ be monic, irreducible of degree $d > 1$.

The Exponent e

The Exponent of m, denoted $\mathrm{Exp}(m)$ is the smallest positive integer e such that

$$m(x) \quad \text{divides} \quad x^e - 1$$

If β denotes a root of $m(x)$ in $\mathbb{F}_{q^d}$ then $\mathrm{Exp}(m)$ is the order of β in $\mathbb{F}_{q^d}^{\times}$.

The Subexponent of a Polynomial

Definition

The Subexponent of m, denoted $\mathrm{Subexp}(m)$, is the smallest positive integer s such that

$$m(x) \quad \text{divides} \quad x^s - \kappa$$

for some $\kappa \in \mathbb{F}_q^\times$ (κ is called integral element).

If β denotes a root of $m(x)$, then s is the order of β in the factor group $\mathbb{F}_{q^d}^\times / \mathbb{F}_q^\times$. Therefore,

$$s = \frac{e}{\gcd(q-1, e)}.$$

Primitive and Subprimitive Polynomials

Definition

Let $m(x)$ be a polynomial over $\mathbb{F}_q$.

$m(x)$ is called primitive if $\mathrm{Exp}(m) = q^d - 1$.

$m(x)$ is called subprimitive if

$$\mathrm{Subexp}(m) = \theta_{d-1}(q) = \frac{q^d - 1}{q - 1} = |\mathrm{PG}(d-1, q)|$$

Remarks:

- If $m(x)$ is primitive, multiplication by β is a cyclic collineation of the affine space $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$.
- If $m(x)$ is subprimitive, multiplication by β is a cyclic collineation of the projective space $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$.

Generalizing Hirschfeld's Result

In

$$T^n \mathbf{x}_0 = \kappa \mathbf{x}_0,$$

we need $\kappa = 1$. Thus we need to count subprimitive polynomials with integral element $\kappa = 1$.

Actually, we'll compute the more general counting function

$R_\kappa(d, q) =$ *# of subprimitive polynomials of degree d over* $\mathbb{F}_q$ *with integral element* $\kappa \in \mathbb{F}_q$.

Write $\kappa = \alpha^i$ where α is a primitive element of $\mathbb{F}_q$.

Generalizing Hirschfeld's Result

LEMMA

$$R_\kappa(d,q) = R_{\alpha^i}(d,q) = \begin{cases} \dfrac{g}{\Phi(g)} \cdot \dfrac{\Phi(\theta_{d-1}(q))}{d} & \text{if } \gcd(i,g) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

where $g = \gcd(q-1, \theta_{d-1}(q))$

Remarks:

- The function $R_{\alpha^i}(d,q)$ is periodic in i with period $\gcd(q-1, \theta_{d-1}(q))$.
- The non-zero function values depend only on d and q, but not on i.
- The factor $q-1$ in Hirschfeld's formula is replaced by $\frac{g}{\Phi(g)}$.

Counting Subprimitive Polynomials by Integral Element

COROLLARY

$$R_\kappa(2,q) = \begin{cases} \frac{1}{2}\Phi(q+1) & \text{for all } \kappa \text{ if } 2 \mid q, \\ \Phi(q+1) & \text{if } 2 \nmid q \text{ and } \kappa \text{ is a nonsquare in } \mathbb{F}_q^\times, \\ 0 & \text{if } 2 \nmid q \text{ and } \kappa \text{ is a square in } \mathbb{F}_q^\times. \end{cases}$$

COROLLARY

$$R_1(2,q) = \begin{cases} \frac{1}{2}\Phi(q+1) & \text{if } 2 \mid q, \\ 0 & \text{if } 2 \nmid q. \end{cases}$$

Cyclic Code Automorphisms

COROLLARY

The codes of length $q^2 + 1$ or $q^3 + 1$ are cyclic iff $2 \mid q$

COROLLARY

The codes of length $q^2 + 1$ for $2 \nmid q$ are not BCH-codes

Remark:
If the codes are cyclic, then they are cyclic in $R_1(2, q)$ many ways.