Finite Geometries, Mod 2-Geometries and a new weighing matrix $W(23, 16)$

Assaf Goldberger[1] Yossi Strassler[2] Giora Dula[3]

[1]School of Mathematical Sciences
Tel-Aviv University

[2]Dan Yishay

[3]Department of Computer Science and Mathematics
Netanya College

15.03.2016 Braude Colloquium

Definition

Let $n \geq k$ be two positive integers. A weighing matrix W of size n and weight k is a $\{0, 1, -1\}$-matrix that is orthogonal of square-norm k. That is,

$$WW^T = W^T W = kI_n.$$

We use the notation: "W is a $W(n, k)$ matrix".

Applications: Chemistry, Spectroscopy, Quantum Computing and Coding Theory.

Examples

- Signed Permutation matrices are $W(n, 1)$.
- This is a $W(2, 2)$:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- This is a $W(4, 3)$:

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 \\ 1 & -1 & 0 & 1 \\ -1 & -1 & 1 & 0 \end{pmatrix}$$

- Direct (Block) sums:

$$W(n_1, k) \oplus W(n_2, k) \oplus \cdots \oplus W(n_t, k) = W(n, k).$$

Examples

- Tensor Products:

$$W(n_1, k_1) \otimes W(n_2, k_2) = W(n_1 n_2, k_1 k_2).$$

- Orthogonal Designs: Suppose that $A, B \in \{-1, 0, 1\}^{n \times n}$ and $AB = BA$. Assume further that $AA^T + BB^T = kI_n$. Then

$$\begin{pmatrix} A & B \\ -B^T & A^T \end{pmatrix}$$

is a $W(n, k)$.

- There are 4×4, 8×8 and higher orthogonal designs with similar properties.

"Statistically", weighing matrices shouldn't exist

- Let $v, w \in \{-1, 0, 1\}^n$ be two random vectors of norm $\sqrt{k}$.
- The orthogonality probability:

$$Prob(vw^T = 0) \;=\; \sum_{0 \le 2t \le k} \binom{k}{2t} \binom{n-k}{k-2t} \binom{2t}{t} \binom{n}{k}^{-1} \left(\frac{1}{2}\right)^{2t}$$

- And when $k, n \gg 0$ and $k/n = \alpha$,

$$Prob(vw^T = 0) \approx \frac{1}{2\pi\alpha\sqrt{k(1-\alpha)}}$$

- Assuming independency: If v_i are m such random vectors, then

$$Prob(v_i \text{ are mutually orthogonal}) \approx (2\pi\alpha\sqrt{k(1-\alpha)})^{-m(m-1)/2}$$

"Statistically", weighing matrices shouldn't exist

- The number of the $W(n,k)$ is therefore estimated by

$$\binom{n}{k}^{n} 2^{nk}(2\pi\alpha\sqrt{k(1-\alpha)})^{-n(n-1)/2} \ll 1,$$

- Therefore, a $W(n,k)$ is unlikely to exist.
- However, there is an abundance of weighing matrices, such as those given by the constructions above, and many more...

Special Cases of Interest

- $W(n, n)$ are called Hadamard Matrices
- $W(n, n-1)$ are called Conference Matrices
- Symmetric weighing matrices
- Circulant weighing matrices leading to cyclotomic algebraic number theory.

Hadamard Matrices

Conjecture (Hadamard Conjecture)

For every $n \equiv 0 \pmod 4$ there exists a Hadamard matrix of size n.

- The condition $n \equiv 0 \pmod 4$ is necessary (except for $n = 2$).
- The smallest unsolved case is $n = 668$.
- They exist for any power of 2 (by tensor powers).
- They exist for any order $p + 1$ when $p \equiv 3 \pmod 4$ is prime (Payley Matrices).

Payley Matrices

- Let p be a prime, $p \equiv 3 (\mod 4)$.
- The Legendre symbol is the function

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a (\mod p) \text{ has a solution} \\ -1 & \text{otherwise} \end{cases}$$

- This is the Payley matrix of order $p+1$

$$\left(\begin{array}{c|c} 1 & -1 \cdots -1 \\ \hline 1 & \\ \vdots & \left(\frac{i-j}{p}\right)_{1 \leq i,j \leq p} \\ 1 & \end{array}\right)$$

Weighing Matrices

- The smallest unknown weighing matrix was $W(23,16)$. This is now solved by Dula,Goldberger and Strassler (2015).
- The next unknown matrix is $W(25,16)$.

Theorem

If $W = W(n,k)$ is a weighing matrix, then n odd $\implies$ k is a perfect square.

Proof.

$\det W = \pm k^{n/2} \in \mathbb{Z}$ □

-

Weighing Matrices

- The smallest unknown weighing matrix was $W(23, 16)$. This is now solved by Dula,Goldberger and Strassler (2015).
- The next unknown matrix is $W(25, 16)$.

Theorem

If $W = W(n, k)$ is a weighing matrix, then n odd $\implies$ k is a perfect square.

Proof.

$\det W = \pm k^{n/2} \in \mathbb{Z}$ □

-

Circulant Weighing Matrices

Theorem

If $W = W(n,k)$ is a Circulant weighing matrix, then k is a perfect square (regardless of the order).

Proof.

Let $\mathbf{j} = [1, 1, \ldots, 1]$. Then $\mathbf{j}W = [s, s, \ldots, s] = s\mathbf{j}$ for some $s \in \mathbb{Z}$. Hence

$$nk = \mathbf{j}(kI_n)\mathbf{j}^T = \mathbf{j}(WW^T)\mathbf{j}^T = (s\mathbf{j})(s\mathbf{j})^T = ns^2.$$

So $k = s^2$. □

-

Circulant Weighing Matrices

Theorem

If $W = W(n,k)$ is a Circulant weighing matrix, then k is a perfect square (regardless of the order).

Proof.

Let $\mathbf{j} = [1, 1, \ldots, 1]$. Then $\mathbf{j}W = [s, s, \ldots, s] = s\mathbf{j}$ for some $s \in \mathbb{Z}$. Hence

$$nk = \mathbf{j}(kI_n)\mathbf{j}^T = \mathbf{j}(WW^T)\mathbf{j}^T = (s\mathbf{j})(s\mathbf{j})^T = ns^2.$$

So $k = s^2$. □

-

Circulant weighing matrices and cyclotomic algebra

Consider the problem of finding a circulant weighing matrix $W(n,k)$, such that $WW^T = kI_n$.

- The nth cyclotomic algebra is $C_n = \mathbb{Z}[x]/(x^n - 1)$.
- It carries an involution $C_n \to C_n$ given by $x \mapsto \bar{x} := x^{-1}$ (complex conjugation).
- Solving for $W \iff$ Solving the equation $z\bar{z} = k$ in C_n.
- There is a factorization to cyclotomic polynomials

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

$\Phi_1(x) = x-1;\ \Phi_2(x) = x+1;\ \Phi_3(x) = x^2+x+1; \Phi_6(x) = x^2-x+1;$ etc.

The Cyclotomic Method

- Accordingly,

$$C_n \otimes \mathbb{Q} \simeq \bigoplus_{d|n} \mathbb{Q}[x]/(\Phi_d(x)),$$

  and $K_d := \mathbb{Q}[x]/(\Phi_d(x))$ are the cyclotomic fields $\mathbb{Q}(\exp(2\pi i/d))$.
- Solution Strategy: Find a solution $z_d \in K_d$ for $z_d \bar{z}_d = k$ and let $z = \sum z_d \in C_n \otimes \mathbb{Q}$.
- Advantage: Usually not many candidates for z_d.
- Notice: z may not be integral even if z_d are integral for all $d|n$.
- There is an efficient way to sort out the integral $z \in C_n$.
- This is efficient in finding or disproving existence of circulant weighing matrices $W(n,k)$ for $n < 100$.

The Cyclotomic Method

- For large n, we expect that circulant weighing matrices will be rare due to the large class number of the K_d.
- it is easy to show that some cases don't exist, for instance, circulant $W(17, 9)$.
- If we try to solve $z_{17}\bar{z_{17}} = 9$ in $K_{17} = \mathbb{Q}(\exp(2\pi i/17)$, we encounter a problem:
- The ideal (3) in $\mathbb{Z}[\exp(2\pi i/17)]$ is prime. This means that z_{17} must be divisible by 3.
- For any $\{-1, 0, 1\}$-polynomial $h(x) \in C_{17}(x)$, the projection $h(x)$ mod $\Phi_{17}(x)$ is has coefficients bounded by 2.
- Hence, $z_{17} = h(x) \mod \Phi_{17}(x)$ cannot be divisible by 3, a contradiction.

The Cyclotomic Method - Augmented Circulant Matrices

- Example: Let $p \equiv 3 \mod 4$ be a prime. The Gauss sum $z_p = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \exp(2\pi ij/p)$ satisfies $z_p\bar{z_p} = p + 1$.
- There is no solution in K_1 to $z_1\bar{z_1} = z_1^2 = p + 1$, Hence no rational circulant $p \times p$ matrix W with $WW^T = (p+1)I_p$.
- However, taking $z_1 = 0$ will result in a matrix W for which $WW^T = (p+1)I_p - J$ for $J = (1)_{p \times p}$.
- By adding extra row and column, we can turn this into a $W(p+1, p+1)$. This is the Payley matrix!
- This type of construction is called augmented circulant weighing matrix
- In general one can construct thicker augmentations by combining solutions z_d for all but few small $d|n$.

Mod 2 Geometries

Philosophy: Break the construction of a weighing matrix into two stages:

1. Geometrizing: Find a $\{0,1\}$-matrix $\bar{W}$ such that $\bar{W}\bar{W}^T \equiv kI_n$ mod 2.
2. Coloring: Add signs (colors) to each "1" in $\bar{W}$ to obtain a true $W = W(n,k)$.

Definition

The matrix $\bar{W}$ is called the support matrix of W.
The complementary matrix $S = J_n - \bar{W}, J_n := (1)_{n\times n}$, is called the shadow matrix of W.

They satisfy

$$\bar{W}\bar{W}^T \equiv \bar{W}^T\bar{W} \equiv kI_n \mod 2 \text{ and}$$
$$SS^T \equiv S^TS \equiv kI_n + nJ_n \mod 2.$$

Mod 2 Geometries

Philosophy: Break the construction of a weighing matrix into two stages:

1. Geometrizing: Find a $\{0,1\}$-matrix $\bar{W}$ such that $\bar{W}\bar{W}^T \equiv kI_n$ mod 2.
2. Coloring: Add signs (colors) to each "1" in $\bar{W}$ to obtain a true $W = W(n,k)$.

Definition

The matrix $\bar{W}$ is called the support matrix of W.
The complementary matrix $S = J_n - \bar{W}, J_n := (1)_{n\times n}$, is called the shadow matrix of W.

They satisfy

$$\bar{W}\bar{W}^T \equiv \bar{W}^T\bar{W} \equiv kI_n \mod 2 \text{ and}$$
$$SS^T \equiv S^TS \equiv kI_n + nJ_n \mod 2.$$

Mod 2 Geometries

Definition

let i, n, p be integers, $i = 0, 1$ and $p \leq n$. A mod 2 Geometry of characteristic (i, n, p) is a pair (G, L) where G a finite set G and a finite collection Λ of subsets of G such that

- The elements of G are called points, and those of L are called lines.
- $|L| = |G| = n$
- Each line contains p points.
- Each point is contained in p lines.
- Every two lines intersect at $i \mod 2$ points.
- Every two points are contained in $i \mod 2$ lines.
- The incidence matrix $I(G)$ is the $\{0, 1\}$ matrix such that $I(G)_{i,j} = 1$ iff the ith point is on the jth line.

Examples

- The support and shadow matrices of a weighing matrix are incidence matrices of mod 2 Geometries.
- Finite Plane Geometries:

Definition

A finite Geometry of order q is a mod 2 geometry where
(a) Every two distinct lines intersect at exactly one point;
(b) Every two distinct points lie on exactly one line;
(c) The Geoemtry consists of $q^2 + q + 1$ points and lines;
(d) Every line consists of $q + 1$ points, and vice-versa.

- Example of finite plane geometries: projective planes $\mathbb{P}^2(\mathbb{F}_q)$ for a finite field $\mathbb{F}_q$.
- Projective spaces $\mathbb{P}^d(\mathbb{F}_q)$, where the lines are hyperplanes, form mod 2 Geometries.

Circulant Structure of Projective Geometries

Theorem

For every projective geometry $G = \mathbb{P}^d(\mathbb{F}_q)$, there exists an ordering of the points such that the incidence matrix $I(G)$ is circulant.

Proof.

There is an identification $\mathbb{P}^d(\mathbb{F}_q) = \mathbb{F}^{\times}_{q^{d+1}}/\mathbb{F}^{\times}_q$. The latter is a cyclic group with generator a. Ordering the points by $1, a, a^2$,etc. gives the circulant Structure. □

Example

There is a circulant weighing matrix $W(31, 16)$ due to Strassler. It corresponds to the (circulant) shadow geometry $\mathbb{P}^4(\mathbb{F}_2)$.

Mod 2 Geometries

Two easy equations

Let (G, L) be a mod 2 geometry with characteristic (i, n, p). Fix a line $\ell \in L$ and for each t, let z_t be the number of lines that intersect ℓ at t points. Then

$$\sum_t z_t = n - 1 \tag{1}$$

$$\sum_t t z_t = p(p-1). \tag{2}$$

-
  - A line ℓ together with the intersecions $\ell' \cap \ell$ for all lines ℓ' is called a local mod 2 Geomtry.

Example: $W(21,16)$

- A matrix $W = W(21,16)$ is known to exist. It's shadow geometry is of characteristic $(1,25,5)$. Let's look at a local geoemtry:
- We have $z_1 + z_3 + z_5 = 20$ and $z_1 + 3z_3 + 5z_5 = 20$. Consequently $z_1 = 20, z_3 = z_5 = 0$.
- Conclusion: All intersections are of cardinality 1. This is a finite plane geometry.
- It is known that the only example is $\mathbb{P}^2(\mathbb{F}_4)$.

The same logic can lead the more general.

Theorem

A) If a weighing $W(n^2+n+1, n^2)$ exists, then its support geometry is a finite plane geometry, with lines of cardinality $n+1$ and intersect each other at a single point.

B) A weighing matrix $W(m,k)$ does not exist if $m = x^2+x+1$ is odd (x real), and $k > x^2$.

We see that k has an upper bound in $W(m,k)$. But what if k is close but below the upper bound?

Example: $W(23,16)$

- This was recently open until current work.
- Looking at the local shadow geometry (of characteristic $(1,23,7)$) reveals that

$$\begin{aligned} z_1 + z_3 + z_5 + z_7 &= 22 \\ z_3 + 2z_5 + 3z_7 &= 10. \end{aligned}$$

- Conclusion: $z_1 \geq 12$. In particular:

Observation

There are 23 lines, of cardinality 7 each, and more that 50% of the pairs intersect at a single point. All this is packed in a set of cardinality 23.

- It seems unlikely that all this could happen!?

A geometry for $W(23, 16)$

- Surprisingly, a geometry for $W(23, 16)$ has been found!
- This was done by first guessing a local geometry.
- From this we studied the conditions imposed on the entire geometry.
- Then we found the full geometry.
- Finally, we found a connection to the projective geometry $\mathbb{P}^2(\mathbb{F}_4)$ of the shadow of $W(21, 16)$.
- This allows us to generalize to an infinite family of mod 2 geometries.

- To construct a local geometry for $W(23,16)$, we begin with a baseline ℓ.
- The local geometry should satisfy:
  1. If z_t is the number of lines intersecting ℓ at t-points, then

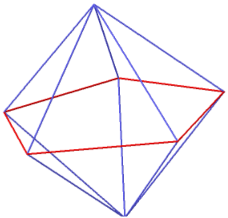
$$\begin{aligned} z_1 + z_3 + z_5 + z_7 &= 22 \\ z_3 + 2z_5 + 3z_7 &= 10 \\ z_t &= 0 \text{ for } t \equiv 0 \mod 2 \end{aligned}$$

  2. Each point of ℓ must be covered by exactly six other lines,
  3. Every pair of points in ℓ must be covered by an even number of lines.

Below are two examples of (incidence matrices) of local geometries, with $(z_1, z_3, z_5, z_7) = (12, 10, 0, 0)$ and $(z_1, z_3, z_5, z_7) = (16, 4, 0, 2)$.

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

Visualization of the type $(z_1, z_3, z_5, z_7) = (12, 10, 0, 0)$



- The vertices correspond to the points of ℓ.
- The faces correspond to the 10 lines that intersect ℓ at 3 points, these intersection points being vertices of the triangle.

The Frame Matrix for $W(23, 16)$

The local and dual-local incidence matrices form the green part of the matrix

1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

The Core Matrix

- The (missing) white part of the matrix is the core matrix
- This is a 16×16 matrix arranged as a 4×4 array of 4×4 blocks.

$$\begin{bmatrix} t_{1,1} & t_{1,2} & t_{1,3} & t_{1,4} \\ t_{2,1} & t_{2,2} & t_{2,3} & t_{2,4} \\ t_{3,1} & t_{3,2} & t_{3,3} & t_{3,4} \\ t_{4,1} & t_{4,2} & t_{4,3} & t_{4,4} \end{bmatrix}$$

- To make a mod 2 geometry, the core must satisfy:
  1. Each block $t_{i,j}$ has odd weight in each row & column.
  2. The inner product of two rows that belong to same block layer must be $0 \mod 2$.
  3. The inner product of two rows that belong to a different block layer must be $1 \mod 2$.
  4. Each row has total weight 6
  5. Ditto for columns.

The blocks in the core matrix

- As said above, each block $t_{i,j}$ has odd weight in each row & column
- There are $2^9 = 512$ possible 4×4 blocks.
- There are only 7 possible blocks up to isomorphism (= row & column permutations). These are (labelled by total weight):

$$T_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, T_{6,1} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$T_{6,2} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, T_8 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$T_{10,i} = J - T_{6,i}, T_{12} = J - T_4$$

The search for the core matrix

- The core matrix was obtained by a combination of linear algebra and exhaustive search.
- It was done layer by layer. Each layer satisfies linear equations (mod 2) relative to previous layers, plus the linear conditions for each block.
- We search the solution space and sort out all solutions with row weight 6.
- The total number of combinations at each stage did not exceed 10^7.
- Finally, we have found 144 solutions to the core matrix, comprised of 2 isomorphism classes.

The core matrix of a finite plane geometry

- Let's take a finite plane geometry of order 4 (That is, of cardinality $21 = 4^2 + 4 + 1$).
- The local geometry looks like

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

- There is a core matrix K_{21} of the sort

$$\begin{bmatrix} t_{1,1} & t_{1,2} & t_{1,3} & t_{1,4} \\ t_{2,1} & t_{2,2} & t_{2,3} & t_{2,4} \\ t_{3,1} & t_{3,2} & t_{3,3} & t_{3,4} \\ t_{4,1} & t_{4,2} & t_{4,3} & t_{4,4} \end{bmatrix}$$

  where each $t_{i,j}$ is a 4×4 permutation matrix.
- The inner products of the K_{21} rows are exactly the same as was with the $W(23, 16)$ core!

J-twisting

- Let J be the matrix of 1's (of a suitable order).
- Denote K_{23} the 16×16 core of the desired $W(23, 16)$ matrix.

Definition (J-twist)

Let $\pi \in S_4$ be permutation, and C a core matrix. The J-twist of $C = (t_{i,j})$ along the permutation π is the matrix $C' = (t'_{i,j})$ such that

$$\begin{cases} t'_{i,j} = J - t_{i,j} & \text{for } j = \pi(i) \\ t'_{i,j} = t_{i,j} & \text{otherwise} \end{cases}$$

Theorem

Let $\pi \in S_4$ be a permutation. A 16×16 matrix is a K_{21} if and only if its J-twist along π is a K_{23}.

-

J-twisting

Corollary

We can construct a mod 2 shadow geoemtry of a $W(23, 16)$ by J-twisting on a finite plane geometry of order 4, such as $\mathbb{P}^2(\mathbb{F}_4)$.

- We can apply further J-twisting and obtain shadow geometries for $W(25, 16), W(27, 16)$ and $W(29, 16)$. However, we do not know if these weighing matrices exist.
- Our constuction is more general, namely:

Theorem

Starting from the projective geometry $\mathbb{P}^2(\mathbb{F}_{2^m})$, we can apply the method of J-twisting and obtain shadow geometries for $W(2^{2m} + 2^m + (2^m - 2)j + 1, 2^{2m})$ for $j = 0, 1, \ldots, 2^m$.

J-twisting - Example

This is a K_{21} coming from projective geometry:

$$\left[\begin{array}{cccc|cccc|cccc|cccc}
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\
\hline
1&0&0&0&0&0&0&1&0&1&0&0&0&0&1&0\\
0&1&0&0&0&0&1&0&1&0&0&0&0&0&0&1\\
0&0&1&0&0&1&0&0&0&0&0&1&1&0&0&0\\
0&0&0&1&1&0&0&0&0&0&1&0&0&1&0&0\\
\hline
1&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0\\
0&1&0&0&0&0&0&1&0&0&1&0&1&0&0&0\\
0&0&1&0&1&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&1&0&1&0&0&1&0&0&0&0&0&1&0\\
\hline
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
0&1&0&0&1&0&0&0&0&0&0&1&0&0&1&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&0&0&1&0&0&1&0&0&1&0&0&1&0&0&0
\end{array}\right]$$

J-twisting - Example

And this is a K_{23} obtained by J-twisting along $\pi = (12)(34)$:

$$
\left[\begin{array}{cccc|cccc|cccc|cccc}
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
\hline
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
\hline
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0
\end{array}\right]
$$

Coloring

- By "Coloring" we mean adding signs to a support matrix so that it becomes orthogonal.
- Coloring is still premature technology. We don't know much about it.
- The two main tools we use for coloring are:
  1. Max-Clique Algorithm (Ostergard's algorithm)
  2. Lattice Basis Reduction (The LLL algorithm)

Basic Coloring Scheme

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

- The uncolored matrix

Basic Coloring Scheme

0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	−1	−1	−1	−1	−1	−1	−1	−1
0	0	0	0	0	0	0	1	1	1	1	−1	−1	−1	−1	1	1	1	1	−1	−1	−1	−1
0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1
0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0
1	1	1	0	1	1	1	1	0	0	0	0	1	1	1	0	1	1	1	0	1	1	1
1	1	1	0	1	1	1	0	1	0	0	1	0	1	1	1	0	1	1	1	0	1	1
1	1	1	0	1	1	1	0	0	1	0	1	1	0	1	1	1	0	1	1	1	0	1
1	1	1	0	1	1	1	0	0	0	1	1	1	1	0	1	1	1	0	1	1	1	0
1	1	1	1	0	1	1	0	1	1	1	0	0	0	1	1	0	1	1	1	1	0	1
1	1	1	1	0	1	1	1	0	1	1	0	0	1	0	0	1	1	1	1	1	1	0
1	1	1	1	0	1	1	1	1	0	1	0	1	0	0	1	1	1	0	0	1	1	1
1	1	1	1	0	1	1	1	1	1	0	1	0	0	0	1	1	0	1	1	0	1	1
1	1	1	1	1	0	1	0	1	1	1	1	1	0	1	0	0	0	1	1	0	1	1
1	1	1	1	1	0	1	1	0	1	1	1	1	1	0	0	0	1	0	0	1	1	1
1	1	1	1	1	0	1	1	1	0	1	0	1	1	1	0	1	0	0	1	1	1	0
1	1	1	1	1	0	1	1	1	1	0	1	0	1	1	1	0	0	0	1	1	0	1
1	1	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	1	0	0	0	1
1	1	1	1	1	1	0	1	0	1	1	0	1	1	1	1	1	1	0	0	0	1	0
1	1	1	1	1	1	0	1	1	0	1	1	1	1	0	0	1	1	1	0	1	0	0
1	1	1	1	1	1	0	1	1	1	0	1	1	0	1	1	0	1	1	1	0	0	0

- We color the fisrt 3 rows (an intelligent guess; respects the blocks)

Basic Coloring Scheme

$$
\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0
\end{pmatrix}
$$

- We color the fisrt 3 rows (an intelligent guess; respects the blocks)
- We also color a 4×4 Hadamard block

Basic Coloring Scheme

$$
\begin{pmatrix}
0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&-1&-1&-1&-1&-1&-1&-1&-1\\
0&0&0&0&0&0&0&1&1&1&1&-1&-1&-1&-1&1&1&1&1&-1&-1&-1&-1\\
0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1\\
0&0&0&-1&-1&1&1&1&1&1&1&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&1&-1&1&-1&1&1&1&1&1&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&-1&1&1&-1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0\\
1&1&1&0&1&1&1&1&0&0&0&0&1&1&1&0&1&1&1&0&1&1&1\\
1&1&1&0&1&1&1&0&1&0&0&1&0&1&1&1&0&1&1&1&0&1&1\\
1&1&1&0&1&1&1&0&0&1&0&1&1&0&1&1&1&0&1&1&1&0&1\\
1&1&1&0&1&1&1&0&0&0&1&1&1&1&0&1&1&1&0&1&1&1&0\\
1&1&1&1&0&1&1&0&1&1&1&0&0&0&1&1&0&1&1&1&1&0&1\\
1&1&1&1&0&1&1&1&0&1&1&0&0&1&0&0&1&1&1&1&1&1&0\\
1&1&1&1&0&1&1&1&1&0&1&0&1&0&0&1&1&1&0&0&1&1&1\\
1&1&1&1&0&1&1&1&1&1&0&1&0&0&0&1&1&0&1&1&0&1&1\\
1&1&1&1&1&0&1&0&1&1&1&1&1&0&1&0&0&0&1&1&0&1&1\\
1&1&1&1&1&0&1&1&0&1&1&1&1&1&0&0&0&1&0&0&1&1&1\\
1&1&1&1&1&0&1&1&1&0&1&0&1&1&1&0&1&0&0&1&1&1&0\\
1&1&1&1&1&0&1&1&1&1&0&1&0&1&1&1&0&0&0&1&1&0&1\\
1&1&1&1&1&1&0&0&1&1&1&1&0&1&1&1&1&0&1&0&0&0&1\\
1&1&1&1&1&1&0&1&0&1&1&0&1&1&1&1&1&1&0&0&0&1&0\\
1&1&1&1&1&1&0&1&1&0&1&1&1&1&0&0&1&1&1&0&1&0&0\\
1&1&1&1&1&1&0&1&1&1&0&1&1&0&1&1&0&1&1&1&0&0&0
\end{pmatrix}
$$

- We find all pairs (row3,row4) that are orthogonal to row1–row3). We get a list $\mathcal{P}_{34}$

Basic Coloring Scheme

0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	−1	−1	−1	−1	−1	−1	−1	−1
0	0	0	0	0	0	0	1	1	1	1	−1	−1	−1	−1	1	1	1	1	−1	−1	−1	−1
0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	−1	−1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	1	−1	1	−1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1
0	0	0	−1	1	1	−1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0
1	1	1	0	1	1	1	1	0	0	0	0	1	1	1	0	1	1	1	0	1	1	1
1	1	1	0	1	1	1	0	1	0	0	1	0	1	1	1	0	1	1	1	0	1	1
1	1	1	0	1	1	1	0	0	1	0	1	1	0	1	1	1	0	1	1	1	0	1
1	1	1	0	1	1	1	0	0	0	1	1	1	1	0	1	1	1	0	1	1	1	0
1	1	1	1	0	1	1	0	1	1	1	0	0	0	1	1	0	1	1	1	1	0	1
1	1	1	1	0	1	1	1	0	1	1	0	0	1	0	0	1	1	1	1	1	1	0
1	1	1	1	0	1	1	1	1	0	1	0	1	0	0	1	1	1	0	0	1	1	1
1	1	1	1	0	1	1	1	1	1	0	1	0	0	0	1	1	0	1	1	0	1	1
1	1	1	1	1	0	1	0	1	1	1	1	1	0	1	0	0	0	1	1	0	1	1
1	1	1	1	1	0	1	1	0	1	1	1	1	1	0	0	0	1	0	0	1	1	1
1	1	1	1	1	0	1	1	1	0	1	0	1	1	1	0	1	0	0	1	1	1	0
1	1	1	1	1	0	1	1	1	1	0	1	0	1	1	1	0	0	0	1	1	0	1
1	1	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	1	0	0	0	1
1	1	1	1	1	1	0	1	0	1	1	0	1	1	1	1	1	1	0	0	0	1	0
1	1	1	1	1	1	0	1	1	0	1	1	1	1	0	0	1	1	1	0	1	0	0
1	1	1	1	1	1	0	1	1	1	0	1	1	0	1	1	0	1	1	1	0	0	0

- We find all row8 which is orthogonal to rows 1–3 and to some (row4,row5) $\in \mathcal{P}_{34}$. Get a list $\mathcal{R}_8$. $\#\mathcal{R}_8 \approx 90$

Basic Coloring Scheme

$$
\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0
\end{pmatrix}
$$

- We find all row9 which is orthogonal to rows 1–3 and to some (row4,row5) $\in \mathcal{P}_{34}$. Get a list $\mathcal{R}_9$. $\#\mathcal{R}_9 \approx 90$

Basic Coloring Scheme

0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	−1	−1	−1	−1	−1	−1	−1	−1
0	0	0	0	0	0	0	1	1	1	1	−1	−1	−1	−1	1	1	1	1	−1	−1	−1	−1
0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	−1	−1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	1	−1	1	−1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1
0	0	0	−1	1	1	−1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0
1	1	1	0	1	1	1	1	0	0	0	0	1	1	1	0	1	1	1	0	1	1	1
1	1	1	0	1	1	1	0	1	0	0	1	0	1	1	1	0	1	1	1	0	1	1
1	1	1	0	1	1	1	0	0	1	0	1	1	0	1	1	1	0	1	1	1	0	1
1	1	1	0	1	1	1	0	0	0	1	1	1	1	0	1	1	1	0	1	1	1	0
1	1	1	1	0	1	1	0	1	1	1	0	0	0	1	1	0	1	1	1	1	0	1
1	1	1	1	0	1	1	1	0	1	1	0	0	1	0	0	1	1	1	1	1	1	0
1	1	1	1	0	1	1	1	1	0	1	0	1	0	0	1	1	1	0	0	1	1	1
1	1	1	1	0	1	1	1	1	1	0	1	0	0	0	1	1	0	1	1	0	1	1
1	1	1	1	1	0	1	0	1	1	1	1	1	0	1	0	0	0	1	1	0	1	1
1	1	1	1	1	0	1	1	0	1	1	1	1	1	0	0	0	1	0	0	1	1	1
1	1	1	1	1	0	1	1	1	0	1	0	1	1	1	0	1	0	0	1	1	1	0
1	1	1	1	1	0	1	1	1	1	0	1	0	1	1	1	0	0	0	1	1	0	1
1	1	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	1	0	0	0	1
1	1	1	1	1	1	0	1	0	1	1	0	1	1	1	1	1	1	0	0	0	1	0
1	1	1	1	1	1	0	1	1	0	1	1	1	1	0	0	1	1	1	0	1	0	0
1	1	1	1	1	1	0	1	1	1	0	1	1	0	1	1	0	1	1	1	0	0	0

- . . . We find all row23 which is orthogonal to rows 1–3 and to some (row4,row5) $\in \mathcal{P}_{34}$. Get a list $\mathcal{R}_{23}$. $\#\mathcal{R}_{23} \approx 90$

Basic Coloring Scheme

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0
\end{pmatrix}$$

- We create a graph $G = (V, E)$ where $V = \bigcup_{i=8}^{23} \mathcal{R}_i$ and edges connect rows in $\mathcal{R}_i$ with rows in $\mathcal{R}_j$ if they are mutually orthogonal.
- We compute the max-clique of G. If of size 16, we have a colored the green part.

Basic Coloring Scheme

$$
\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0
\end{pmatrix}
$$

- We use the LLL completion algorithm to complete the yellow part.

This is the $W(23,16)$

$$
\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 \\
0 & 0 & 0 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\
0 & 0 & 0 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & -1 & 1 \\
0 & 0 & 0 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 & 1 & -1 & -1 & 0 & -1 & -1 & 1 & 0 & -1 & 1 & 1 \\
1 & 1 & 1 & 0 & -1 & 1 & 1 & 0 & 1 & 0 & 0 & -1 & 0 & -1 & 1 & 1 & 0 & -1 & -1 & 1 & 0 & 1 & -1 \\
1 & 1 & 1 & 0 & -1 & -1 & 1 & 0 & 0 & 1 & 0 & 1 & -1 & 0 & -1 & -1 & 1 & 0 & -1 & -1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & -1 & 0 & 0 & 0 & 1 & -1 & -1 & 1 & 0 & -1 & -1 & 1 & 0 & 1 & 1 & -1 & 0 \\
1 & 1 & -1 & 1 & 0 & -1 & 1 & 0 & -1 & 1 & -1 & 0 & 0 & 0 & 1 & -1 & 0 & 1 & 1 & 1 & -1 & 0 & -1 \\
1 & 1 & -1 & -1 & 0 & 1 & -1 & 1 & 0 & -1 & -1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & -1 & -1 & -1 & 1 & 0 \\
1 & 1 & -1 & -1 & 0 & -1 & -1 & -1 & -1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & -1 & 0 & 0 & 1 & -1 & -1 \\
1 & 1 & -1 & 1 & 0 & 1 & 1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 & 0 & -1 & 1 \\
1 & -1 & -1 & -1 & 1 & 0 & 1 & 0 & 1 & 1 & -1 & -1 & 1 & 0 & -1 & 0 & 0 & 0 & -1 & 1 & 0 & -1 & 1 \\
1 & -1 & -1 & 1 & -1 & 0 & -1 & -1 & 0 & 1 & 1 & -1 & -1 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & 1 & 1 \\
1 & -1 & -1 & -1 & 1 & 0 & 1 & 1 & -1 & 0 & 1 & 0 & -1 & -1 & 1 & 0 & -1 & 0 & 0 & -1 & 1 & 1 & 0 \\
1 & -1 & -1 & 1 & -1 & 0 & -1 & 1 & 1 & -1 & 0 & 1 & 0 & -1 & -1 & -1 & 0 & 0 & 0 & 1 & 1 & 0 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & 0 & 0 & -1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 & 0 & -1 \\
1 & -1 & 1 & 1 & 1 & -1 & 0 & 1 & 0 & -1 & -1 & 0 & -1 & 1 & 1 & 1 & 1 & -1 & 0 & 0 & 0 & -1 & 0 \\
1 & -1 & 1 & 1 & 1 & 1 & 0 & -1 & -1 & 0 & 1 & 1 & 1 & -1 & 0 & 0 & 1 & 1 & -1 & 0 & -1 & 0 & 0 \\
1 & -1 & 1 & -1 & -1 & -1 & 0 & -1 & 1 & -1 & 0 & -1 & 1 & 0 & 1 & -1 & 0 & 1 & 1 & -1 & 0 & 0 & 0
\end{pmatrix}
$$

The Max-Clique Algorithm

- Ostergard's algorithm (2003) is an algorithm to find all maximum cliques in an undirected simple graph.
- It uses a backtracking and prunning procedure to search for the max-cliques.
- At every stage it computes the max-cliques of a full subgraph and then adds another vertex.
- Some simple test is used to prune the new vertices that cannot be used to create a clique of the same size or larger.
- It has a very effcient implementation is Sage. It could find a max-clique in a graph of 3000 vertices in just few seconds!

The LLL Algorithm

- The Lenstra-Lenstra-Lovasz (LLL, 1984) algorithm was designed to factor polynomials over $\mathbb{Q}$ in polynomial time.
- Given a lattice $L \subset \mathbb{R}^n$, the LLL algorithm outputs a basis which is 'close' to being orthogonal.
- An empirical observation (Conjecture?): For orthogonal lattices of dimension < 100, the algorithm always outputs an orthogonal basis.
- The orthogonal basis is unique up to signs.

The LLL Completion Algorithm

- Suppose that we have a partial $m \times n$ weighing matrix, $m > n/2$.
- Assume for simplicity that the weight k is odd and n is even.
- Let $L \subset \mathbb{Z}^n$ be the sublattice of all integral vectors v such that $Wv^T = 0$.
- Under mild assumptions (the $n/2 \times n/2$ minors of W have no common divisor > 1), the volume of L equals $k^{(n-m)/2}$.
- Assume that W can be completed to a full weighing matrix.
- Then $L =$ the lattice spanned by the (orthogonal basis of the) missing
- The LLL applied to L will most likely find the desired completion.
- This has been tested and implemented in Sage.

Questions?