Completing Hadamard and Weighing Matrices Using LLL

Radel Ben-Av[1] Giora Dula[4] Assaf Goldberger[2] Yossi Strassler[3]

ArasuFest, 1 Aug 2019

[1]Holon Institue of Technology rbenav@gmail.com

[2]Tel-Aviv University assafg@post.tau.ac.il

[3] Dan Yishay danyishay@gmail.com

[4] Netanya Accademic College giora@netanya.ac.il

Overview

In this presentation we will discuss

- Given a "1/2"-Hadamard Matrix, How to complete to a full.

Other things that can be done, but will not be discussed

- Creating "1/2"-Hadamard Matrices.
- Solve the equation $XX^T = A$ under 'generic' conditions.

In all items, we will use the famous LLL algorithm. Our results are practical for dimension≤ 200, but no proofs.

The LLL Algorithm

- This algorithm (due to Lenstra,Lenstra and Lovasz, 1982) was invented for factoring polynomials over $\mathbb{Q}$.

The Basic Problem

Given a lattice $L \subset \mathbb{R}^d$, find a nearly orthogonal basis.

- The LLL algorithm solves this problem with partial success:
- Notation: Given a basis $b_1, \ldots, b_d \in \mathbb{R}^d$, let $\{b_i^*\}$ be its Gram-Schmidt vectors, and write

$$b_i = \sum_j \mu_{i,j} b_j^*.$$

The LLL Algorithm

Definition

A basis $b_1, \ldots, b_d$ of a lattice L is LLL-reduced, if
(i) $|\mu_{i,j}| < 0.5$ for all $i \neq j$.
(ii) for all k, $(\delta - \mu_{k,k-1}^2)||b_{k-1}^*||^2 \leq ||b_k^*||^2$. (Lovasz condition)

- The two conditions make LLL-reduced bases be nearly orthogonal, and basis vectors relatively short.
- Fact: We have the norm bounds:

$$||b_1|| \leq 2^{(d-1)/2} \cdot \lambda_1(L),$$

where $\lambda_1(L)$ is the length of the shortest nonzero lattice vector.

LLL in Practice

- In practice, LLL computes the shortest vector within much smaller bounds.
- The Unimodular LLL-Phenomena: For a lattice $L \simeq c\mathbb{Z}^d$, the LLL computes the (unique up to signed permuation) standard basis, in practice for $d \leq 200$.

Our Alogrithm

We are given a matrix $1/2H$ of size $2n \times 4n$ which is partial Hadamard.

1. Let L_0 be the lattice spanned over $\mathbb{Z}$ by the rows of $1/2H$. Compute

$$L_1 = L_0^{\perp} = \{v \in \mathbb{Z}^{4n} \mid \langle v, \ell \rangle = 0 \ \forall \ \ell \in L_0\}.$$

2. Let

$$W = \{v \in \mathbb{Z}^{4n} \mid v_i \equiv v_j \mod 2 \ \forall i, j\}.$$

   Compute the intersection $L_2 = L_1 \cap W$.

3. Compute an LLL basis of L_2. If everything is ok, we get the list of completing vectors.

Smith Normal Form(SNF)

For every integral matrix $M \in M_{m\times n}(\mathbb{Z})$ there exists a decompositon

$$U_L M U_R = D,$$

such that

- D is $m \times n$ diagonal with diagonal $d_i \geq 0$ and $d_1|d_2|\cdots|d_m$ and
- U_L, U_R are unimodular.

d_i are uniquely determined and are called the elementary divisors

Computing $L_1 = L_0^\perp$

Let $1/2H$ be our partial Hadamard matrix.

- Comupte the SNF

$$U_L \cdot 1/2H \cdot U_R = D.$$

- It can be shown that the bottom $n - m$ rows of U_R^T are a basis for $L_0^\perp$.

Unfortunately, the lattice L_1 is too big and the completion is not a basis of L_1.

Intersecting with W

Clearly, the lattice spanned by the completion vectors is contained in

$$W = \{v \in \mathbb{Z}^{4n} \mid v_i \equiv v_j \mod 2 \ \forall i, j\}.$$

So we may form the lattice $L_2 = L_1 \cap W$.

Method

1) Let $B = \{b_1, \dots, b_{2n}\}$ be a basis for L_1.
2) We compute the lattice spanned by vectors λ s.t. $\sum_i \lambda_i b_i \in W$. This gives linear equations mod 2 on λ.
3) Solve the linear system and let $\Omega_1, \dots, \Omega_r \in \mathbb{Z}^{2n}$ be lifts to $\mathbb{Z}$ be a basis to the solution space.
4) Then L_2 is spanned by $\Omega_i B$ and the rows of $2B$.
5) Use SNF to compute a basis of L_2.

Final Stage

Now, compute an LLL-reduced basis to L_2.

- Hopefully, L_2 is the lattice spanned by the completion vectors.
- This happens when $vol(L_2) = vol(L_0) = (4n)^n$. In general, all we can say is $vol(L_2) | (4n)^n$.

Defintion-Theorem

A lattice L spanned by Hadamard vectors is called regular if

$$span_{\mathbb{Q}}(L) \cap W = L \iff L \text{ has elementary divisors } 1, 2, 2, \ldots, 2.$$

If the first half $1/2H$ is regular, then we can prove that L_2 is spanned by the completion.

- In this case, the Unimodular LLL Phenomena on L_2 will produce the (Unique) completion basis.

Summary

- We presented a practical algorithm for completing Hadamard matrices from the half.
- We do not have proofs, but it works for sizes up to 200.
- Even more important: If we are given a 1/2-Hadamard matrix, this algorithm practically shows that it is (not) completable.