Optimisation (Batching)

Fausse bonne idée

Soient
$$B = \begin{pmatrix} b_{11} & \dots & b_{n1} \\ \vdots & \ddots & \vdots \\ b_{1n} & \dots & b_{nn} \end{pmatrix}, \quad x^i = \begin{pmatrix} x_1^i \\ \vdots \\ x_n^i \end{pmatrix}$$
 on peut calculer $\begin{pmatrix} p_1^i \\ \vdots \\ p_n^i \end{pmatrix} = Bx^i$

L'idée était de construire une matrice avec n vecteurs coefficients: $X = \begin{pmatrix} x_1^1 & \dots & x_1^n \\ \vdots & \ddots & \vdots \\ x_n^1 & \dots & x_n^n \end{pmatrix}$

- Il devrait être plus rapide de calculer n points par BX (Strassen) plutôt que n fois Bx^i
- En pratique moins performant (pour des *n* relativement petits), probablement dû aux allocations supplémentaire requises

Approximation

Par réduction de base (Algorithme LLL)

• LLL est un algorithme polynomial qui, étant donné une base B et un facteur $0.25 < \delta < 1$, retourne une nouvelle base \tilde{B} engendrant le même espace et dite δ -LLL réduite

Si
$$\tilde{B}$$
 est δ -LLL réduite, alors $\|\tilde{b}_1\| \leq \left(\frac{2}{\sqrt{4\delta-1}}\right)^{n-1} \lambda$

- Fonctionne par raffinements successifs de la base via l'algorithme de Gram-Schmidt
- En arrondissant les coefficients de projections aux entiers les plus près, pour obtenir une nouvelle base "presque orthogonale"
- Donne une base excellente pour l'énumération si on veut une solution exacte