Plan for today

- Proof of Schwartz-Zippel Lemma
- Polynomial multiplication
- The FFT Fast Fourier Transform

Polynomials

Let R be a ring. A *polynomial* over R is an expression of the form

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \qquad a_n \neq 0.$$

- a_i are in R are called coefficients
- x is the indeterminate
- n is the *degree*.

Multvariate polynomials

- *Monomial:* $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$
- *Polynomial:* $f(x) = \sum_{\alpha \in \mathbb{N}_0^n} a_\alpha x^\alpha$ only finitely many $\alpha \neq 0 \in \mathbb{R}[x_1, \ldots, x_n]$
- *Total degree:* $D(f) = \max_{\alpha \in \mathbb{N}_0^n} \|\alpha\|_1$

$p(x_1, x_2, x_3) = 3x_1 x_2^2 x_3 + 4 x_2 x_3^6 + 2 x_1 x_2$

$D(p) = 7$

Motivation

We were interested in $\det(T_X) \equiv 0$

$$T_X(i,j) = \begin{cases} X_{ij} & \text{if } ij \in E,\ i<j \\ -X_{ji} & \text{" } \quad i>j \\ 0 & \text{otherwise.} \end{cases}$$

$\det(T_X) \in \mathbb{Z}[X_e : e \in E]$

$G=(V,E)$ We don't want to write down $p(x) = \det(T_X)$ explicitly.

Question: Is there a way to determine $p(x) \equiv 0$ by performing evaluations? Answer: YES.

Can do: Efficiently evaluate i.e. compute $p(x^*)$ for some $x^* \in \mathbb{Z}^{|E|}$

Schwartz-Zippel Theorem

Theorem (Schwartz-Zippel Theorem)

Let K be a field and $Q(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ be a multivariate polynomial of total degree d. Fix a finite set $S \subseteq K$, and let $r_1, \ldots, r_n$ be chosen independently and uniformly at random from S. Then

$$P[Q(r_1, \ldots, r_n) = 0 \mid Q(x_1, \ldots, x_n) \not\equiv 0] \leq d/|S|.$$

Why useful?: $p(x)$ has total degree $\leq |V|$

$S = \{1, 2, 3, 4, 5, 6, \ldots 2|V|\}$

on integer matrix with small entries.

$\forall e = ij$ pick $v_e \in S$ at random. compute $p(v) = \det(\widetilde{T_v})$

$P[p(v)=0 \mid p(x) \not\equiv 0] \leq \frac{1}{2}$. Repeat i times: $P_S(\text{all eval.} = 0 \mid p(x) \not\equiv 0) \leq (1/2)^i$

Schwartz-Zippel Theorem

$Q(x_1, x_2) = 2x_1^2 x_2 + 3x_2^3 + 2x_1 x_2$

$f_2(x_2) = 2 \cdot x_2$

Theorem (Schwartz-Zippel Theorem)

Let K be a field and $Q(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ be a multivariate polynomial of total degree d. Fix a finite set $S \subseteq K$, and let $r_1, \ldots, r_n$ be chosen independently and uniformly at random from S. Then (non-empty)

$|S| \geq d$

$$P[Q(r_1, \ldots, r_n) = 0 \mid Q(x_1, \ldots, x_n) \not\equiv 0] \leq d/|S|.$$

Proof: Induction on n. $n=1$) if $p(x_1) \not\equiv 0$ then # roots of p is $\leq d$

choose $r_1 \in S$ at random. $P_r(p(r_1)=0 \mid p \not\equiv 0) \leq \frac{d}{|S|}$

$n > 1$: Write $Q(x_1, \ldots, x_n) = \sum_{i=0}^{k} x_1^i \cdot f_i(x_2, \ldots, x_n)$ if $f_0, \ldots, f_k \not\equiv 0$

Chose $r_1, \ldots, r_n$ indep. and uniformly at random. I.H. $Pr(f_k(r_2, \ldots, r_n) = 0) \leq \frac{d-k}{|S|}$

$Pr(Q(r_1, \ldots, r_n) = 0 \mid f_k(r_2, \ldots, r_n) \neq 0) \leq \frac{k}{|S|}$ $\quad D(f_k) = d - k$ $\quad Pr(A) \leq Pr(A \mid \bar{B}) + Pr(B)$

B event: $f_k(r_2, \ldots, r_n) = 0$

Polynomial multiplication

$f, g \in F[X]$, F is a field.

- $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ $\quad \deg(f \cdot g) \leq n$
- $(f \cdot g)(x) = \sum_{i=0}^{2n} \left(\sum_{i=k+\ell} a_k b_\ell \right) x^i$
- Number of field-operations: multiplications $\Theta(n^2)$ Additions $\Theta(n^2)$

Another representation:

- f is represented uniquely by $(x_0, f(x_0)), \ldots, (x_n, f(x_n))$

$(2 + 4x + 7x^2)(1 + 2x + x^2)$

$= 2 \cdot 1 + (2 \cdot 2 + 4 \cdot 1)x + (2 \cdot 1 + 2 \cdot 4 + 7 \cdot 1) \cdot x^2 + (4 \cdot 1 + 7 \cdot 2)x^3 + (7 \cdot 1)x^4$

$n + n-1 + \ldots = \Theta(n^2)$

$n \times n$ pairs. n Result

$(n-1) \simeq n-1$ pairs $n-1$ Mi

Fast polynomial multiplication: The idea

2 ways to represent a polynomial:

1.) $f(x) = a_0 + a_1 x + \cdots + a_n x^n \leftrightsquigarrow [a_0, a_1, \ldots, a_n]$

2.) $f(x)$ is uniquely represented by: $(x_0, f(x_0)), \ldots (x_n, f(x_n))$ x_i distinct.

1.) $\rightarrow$ 2.) evaluation: $O(n^2)$ running time.

$$\begin{bmatrix} f(x_0) \\ \vdots \\ f(x_n) \end{bmatrix} = \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ & & \vdots & & \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix} \cdot \begin{bmatrix} a_0 \\ \vdots \\ a_n \end{bmatrix}$$

A invertible.

2.) $\rightarrow$ 1.) Interpolation $A^{-1} \cdot f = a$.

Fast polynomial multiplication: The idea

Suppose now: $\deg(f), \deg(g) \leq n$.

f, g are represented by $(x_0, f(x_0)), \ldots, (x_{2n}, f(x_{2n})) \simeq f$

$(x_0, g(x_0)), \ldots (x_{2n}, g(x_{2n})) \simeq g$.

How fast can I multiply now? $\Theta(n)$ mult. Since

$$f \cdot g \simeq \left(x_0, f(x_0) \cdot g(x_0)\right), \ldots, \left(x_{2n}, f(x_{2n}) \cdot g(x_{2n})\right)$$

Discrete and fast Fourier transform

- In the following R denotes a *commutative ring with* 1.
- Recall that an element $0 \neq r \in R$ is a *zero divisor* if there exists ~~another~~ an element $0 \neq s \in R$ such that $r \cdot s = 0$.

$\mathbb{Z}_9$ $\quad 3 \neq 0$

$3 \cdot 3 = 0$

$\mathbb{Z}_{12}$ $\quad 4 \neq 0, \ 3 \neq 0$

$4 \cdot 3 = 0$

n-th root of unity

$f(x)$ $x_0, x_1, \ldots, x_n$

$1 \quad \omega \quad \omega^2 \quad \omega^n$

Definition

Let $n \in \mathbb{N}_{\geq 1}$ and $\omega \in R$.

i) ω is an *n-th root of unity* if $\omega^n = 1$.

$\underbrace{1+1+\cdots+1}_{n\text{-times}}$ is a unit in R

ii) ω is a *primitive* n-th *root of unity* if $\omega^n = 1$, n is a unit in R, $\omega^{n/t} - 1$ is not a zero divisor for, for any prime $t \in \mathbb{P}$ dividing n and $\omega^k \neq 1$ for all $k = 1, \ldots, n-1$.

t could also be n

Example: $R = \mathbb{C}$ $\quad e^{\frac{2\pi i}{n}}$ is primitive n-th root of unity.

$\underbrace{\omega, \omega^2, \ldots, \omega^{n-1}}_{\neq 1} \quad \underbrace{\omega^n}_{=1}$

Example

1. $\omega = e^{2\pi i/8} \in \mathbb{C}$ is a primitive 8-th root of unity.
2. $\mathbb{Z}_8$ does not have a primitive square root of unity. (Why?)

because 2 is not in $\mathbb{Z}_p^*$

The matrix V_ω

$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$

Let ω be a primitive n-th root of unity. The matrix V_ω is defined as

$$V_\omega = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)^2} \end{pmatrix} \cdot \begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} \qquad (1)$$

$$= \begin{bmatrix} f(1) \\ f(\omega) \\ f(\omega^2) \\ \vdots \\ f(\omega^{n-1}) \end{bmatrix}$$

The discrete Fourier transform

Definition

Let ω be a primitive n-th root of unity. The mapping

$$\begin{array}{rccc} \mathbf{DFT}_\omega : & R^n & \longrightarrow & R^n \\ & a & \longmapsto & V_\omega a \end{array},$$

which evaluates a polynomial $f = a_0 + \cdots + a_{n-1}x^{n-1}$ of degree at most $n-1$ at the powers of ω is called the *Discrete Fourier Transform*.

Algorithm

$f(x) = f^e(x^2) + x \cdot f^o(x^2)$

$f^e(x) = 1 + 3x + 4x^2$

$f^o(x) = 2 + 2x$

$f(x) = 1 + 2x + 3x^2 + 2x^3 + 4x^4$

Input: $f(x) = [a_0, \ldots, a_{n-1}]$ and primitive n-th root of unity ω where n is a power of 2

Output: $\mathbf{DFT}_\omega(a) = [y_0, \ldots, y_{n-1}]$

Suppose: ω is 8-th root of unity.

Split f into even and odd part: $f(x) = f_e(x^2) + x \cdot f_o(x^2)$

$y^e = \mathbf{DFT}_{\omega^2}(f_2)$, $y^o = \mathbf{DFT}_{\omega^2}(f_o)$

$h = 1$

for $k = 0$ to $n/2 - 1$ do

$y_k = y_k^e + h \cdot y_k^o$

$y_{k+n/2} = y_{k-n/2}^e - h \cdot y_{k-n/2}^o$

$h = h \cdot \omega$

return $[y_0, \ldots, y_{n-1}]$

compute $f(\omega^0), f(\omega^1), \ldots, f(\omega^7)$.

$f^e((\omega^5)^2) = f^e(\omega^{10}) = f^e(\omega^2)$

$f^o((\omega^5)^2) = f^o(\omega^{10}) = f^o(\omega^2)$

$f(\omega^5) = \omega^5 + f^e(\omega^2) + \omega^5 f^o(\omega^2)$

Running time in terms of ring-operations

$$T(n) = 2 \cdot T(n/2) + O(n)$$

$$= O(n \cdot \log(n))$$

DFT runs in time $O(n \cdot \log n)$.

DFT_ω : $\begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} \to \underbrace{\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \omega^{2(n-1)} \\ & & \vdots & \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)^2} \end{bmatrix}}_{A_\omega} \cdot \begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix}$

$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$

$\downarrow$ $\qquad \uparrow (DFT_\omega)^{-1}$

$(x_0, p(x_0)) \cdots (x_{n-1}, p(x_{n-1}))$

$(DFT_\omega)^{-1}$

Goal: Show that

$(DFT_\omega)^{-1} = \frac{1}{n} \cdot (DFT_{\omega^{-1}})$

$A_\omega \cdot A_{\omega^{-1}} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \cdots & \omega^{2(n-1)} \\ & & \vdots & \\ 1 & \omega^{n-1} & & \omega^{(n-1)^2} \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & & \omega^{-(n-1)} \\ & & \vdots & \\ 1 & \omega^{-(n-1)} & \cdots & \omega^{-(n-1)^2} \end{bmatrix}$

i-th row $\cdot$ i-th column: $\sum_{j=0}^{n-1} (\omega^i)^j \cdot (\omega^{-i})^j = n$ ← should be a unit, we want it in R

i-th row $\times$ j-th column: $\sum_{k=0}^{n-1} (\omega^i)^k \cdot (\omega^{-j})^k = \sum_{k=0}^{n-1} (\omega^{i-j})^k = 0$

$i \neq j$

IF R is a field: $(\omega^{i-j} - 1) \cdot \sum_{k=0}^{n-1} (\omega^{i-j})^k = (\omega^{i-j})^n - 1 = 0$

± 0 $\qquad$ $\neq 0$

Preparations for the inverse of the **DFT**

Exercise: extend this to $-n < \ell < -1$.

Lemma

Let $\ell, n \in \mathbb{N}_{\geq 1}$ such that $1 < \ell < n$ and let $\omega \in R$ be a primitive n-th root of unity, then

1. $\omega^\ell - 1$ *is not a zero divisor of* R,
2. $\sum_{0 \leq j < n} \omega^{\ell j} = 0$.

Assuming 1.) let us show 2.) :

$$\left(\sum_{0 \leq j < n} \omega^{\ell \cdot j}\right)\left(\omega^\ell - 1\right) = \omega^{\ell \cdot n} - 1 = (\omega^n)^\ell - 1 = 0$$

$\Rightarrow = 0$ since

is not a zero divisor.

Preparations for the inverse of the **DFT**

Lemma

Let $\ell, n \in \mathbb{N}_{\geq 1}$ such that $1 \leqslant \ell < n$ and let $\omega \in R$ be a primitive n-th root of unity, then

1. *$\omega^\ell - 1$ is not a zero divisor of R,*
2. *$\sum_{0 \leq j < n} \omega^{\ell j} = 0$.*

Proof of 1.) First case: $\ell \mid n$. Then there exist $p \in \mathbb{P}$ such that ($\ell \cdot x = \frac{n}{p}$) $\ell \mid \frac{n}{p}$. From Def. we have that $(\omega^{n/p} - 1)$ is not a zero divisor. $(\omega^{n/p} - 1) = (\omega^\ell - 1) \sum_{j=0}^{x-1} \omega^{j \cdot \ell}$ if $(\omega^\ell - 1)$ was a zero divisor, then $(\omega^{n/p} - 1)$ was a zero divisor as well.

Second case: $\ell \nmid n$. Let $d = \gcd(\ell, n)$. $d \mid n$, thus $(\omega^d - 1)$ is not a zero divisor. $d = x \cdot \ell + y \cdot n$. $(\omega^d - 1) = (\omega^{x\ell} - 1) = (\omega^\ell - 1) \sum_{j=0}^{x-1} \omega^{\ell \cdot j}$

$\Rightarrow$ equation: if $\omega^\ell - 1$ was a zero div., then $\omega^d - 1$ was a zero divisor.

Preparations for the inverse of the **DFT**

Lemma

Let $\omega \in R$ be a primitive n-th root of unity, $k \in \mathbb{Z}$ and $d = n/\gcd(n,k)$. Then ω^k is a primitive d-th root of unity.

Actually: we only need to show this:

$\omega \in R$ be a primitive $2n$-th root of unity, then ω^2 is a primitive n-th root of unity. (Need for FFT Algo.)

Since $2n$ is a unit in R, also n is a unit in R. The ord of ω^2 is n.

And $\forall\ t \in \mathbb{P}$ s.th. $t \mid n$: $\omega^{n/t} \neq 1$ is not a zero divisor, follows from previous lemmmma.

The matrix $V_{\omega^{-1}}$

Lemma

Let $\omega \in R$ be a primitive n-th root of unity. Then

$$V_\omega V_{\omega^{-1}} = n \cdot I,$$

where I is the $n \times n$ identity matrix.

Proof: See previous slides.

Theorem

Let $\omega \in R$ be a primitive n-th root of unity. For each $y = (y_0, \ldots, y_{n-1})^T$, there exists exactly one polynomial $f = a_0 + \ldots + a_{n-1}x^{n-1}$ with $f(\omega^i) = y_i$, for $i = 0, \ldots, n-1$. This polynomial is given by

$$a = \frac{1}{n} V_{\omega^{-1}} y.$$

Remark

Notice that $1/n \in R$. We insured this in our Definition 29. In fact this is the only place where the requirement $n \in R^*$ matters.

Exercise: Let $p(x) = a_0 + \ldots + a_{n-1}x^{n-1} \in \mathbb{Z}[x]$ with $M \geq \|a\|_\infty, \|b\|_\infty$

$q(x) = b_0 + \ldots + b_{n-1}x^{n-1}$

How long should N be (in terms of n, M) to identify $p \cdot q$ from $p \cdot q \bmod \mathbb{Z}_N$? $N = O(M^2 \cdot n)$

Modular DFT

$L \in \mathbb{N}_+$

In the following we consider the Ring $\mathbb{Z}_M$ for $M = 2^L + 1$.

Lemma

Addition and subtraction in $\mathbb{Z}_M$ can be done with $O(L)$ bit-operations.

Lemma

Let $K = 2^k$ divide L, then

$$\omega = 2^{L/K} \in \mathbb{Z}_M$$

$L = 2^\ell$, $K = 2^k$, $1 \le k < \ell$

is a primitive $2K$-th root of unity.

$\omega^{2K} = 2^{2 \cdot L} = 2^L \cdot 2^L = (-1)(-1) = 1$, $2K$ is power of 2.

$\Rightarrow 2K \in \mathbb{Z}_M^*$

$\gcd(2K, M) = 1 \Rightarrow 2K$ is a unit.

Also: $\omega^j \neq 1$ for $j = 1, \dots, 2K-1$

$(\omega^K - 1)$ is not a zero divisor. $(\omega^K - 1)$ is even a unit $(\omega^K - 1) = (2^L - 1) = -2$

$\gcd(2, M) = 1$

Exercise

Let $a \in \mathbb{Z}_M$, where $M = 2^L + 1$ and let j, $1 \leq j \leq L$ be a natural number. Show that the product $a \cdot 2^j$ can be computed with $\mathrm{O}(L)$ bit-operations. *Hint: This is not just shifting to the left but a little bit more*

Running time

in Algorithm $n = 2K$

Theorem

$L = 2^{\ell}$

Let $M = 2^L + 1$ and $K = 2^k$ divide L and let $\omega = 2^{L/K}$. The mappings $\mathbf{DFT}_\omega$ and $(\mathbf{DFT}_\omega)^{-1}$ can be computed with $O(K\,L \log K)$ bit-operations.

$$T(K, L) = 2 \cdot T\left(\frac{K}{2}, L\right) + O(K \cdot L)$$

$$= O(K \cdot L \cdot \log K)$$

Running time

Corollary

Let $f(x)$ and $g(x)$ be two polynomials in $\mathbb{Z}_M$, $M = 2^L + 1$, of degree at most $2K - 1$, where $K = 2^k$ divides L. Then their product $(f \cdot g)(x)$ can be computed with $O(K L \log K + K\, M(L))$ bit-operations, where $M(s)$ is the bit-complexity of s-bit integer multiplication.

(in bit-operations)

Exercise: How fast can you multiply two polynomials f, g in terms of their degree and $\|\cdot\|_\infty$-norm?

Exercise

You are to multiply two n-degree polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$. For this you want to use the modular DFT approach. Thus you want to translate the problem into a suitable problem of polynomial multiplication in $\mathbb{Z}_M[x]$ using the following scheme. The polynomials f and g are mapped into $\mathbb{Z}_M[x]$ via the canonical homomorphism. In there they are multiplied using the modular FFT. From this product, the original product $f \cdot g \in \mathbb{Z}[x]$ is to be reconstructed.

1. Let a be an upper bound on the absolute values of the coefficients of f and g. Determine an $M \in \mathbb{N}_+$ such that the reconstruction of the product $f \cdot g \in \mathbb{Z}_M[x]$ is unique. Derive a lower bound on M. (These bounds should not be far apart! I don't want anybody to write 1 and ∞ here!)
2. Derive an upper bound on the bit-complexity of this modular approach in terms of n and $\mathrm{size}(a)$. (Give your best for that too!)

Exercise

Consider the polynomials $f(x) = 5x^3 + 3x^2 - 4x + 3$ and $g(x) = 2x^3 - 5x^2 + 7x - 2$ in $\mathbb{Z}_{17}$.

1. Compute $f \cdot g$ the naive way.
2. Show that $\omega = 2$ is a primitive 8th root of unity and compute the inverse $\omega^{-1} = 2^{-1}$.
3. Compute the matrices V_ω and $V_{\omega^{-1}}$ and their product.
4. Trace Algorithm **??** on input ω, f and ω, g and compute with the result $(y_0, \ldots, y_7) = \mathbf{DFT}_\omega(f) \cdot \mathbf{DFT}_\omega(g)$.
5. Trace Algorithm **??** on input ω^{-1}, y an compare your result with 1.

Exercise

Consider the polynomials $f(x) = 5x^3 + 3x^2 - 4x + 3$ and $g(x) = 2x^3 - 5x^2 + 7x - 2$ in $\mathbb{Z}_{17}$.

1. Compute $f \cdot g$ the naive way.
2. Show that $\omega = 2$ is a primitive 8th root of unity and compute the inverse $\omega^{-1} = 2^{-1}$.
3. Compute the matrices V_ω and $V_{\omega^{-1}}$ and their product.
4. Trace Algorithm **??** on input ω, f and ω, g and compute with the result $(y_0, \ldots, y_7) = \mathbf{DFT}_\omega(f) \cdot \mathbf{DFT}_\omega(g)$.
5. Trace Algorithm **??** on input ω^{-1}, y an compare your result with 1.

Exercise

Consider the polynomials $f(x) = 5x^3 + 3x^2 - 4x + 3$ and $g(x) = 2x^3 - 5x^2 + 7x - 2$ in $\mathbb{Z}_{17}$.

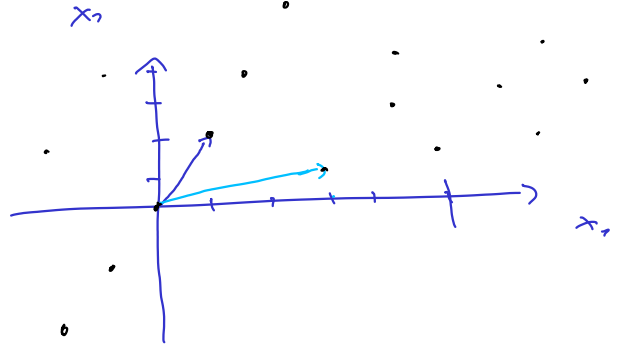
1. Compute $f \cdot g$ the naive way.
2. Show that $\omega = 2$ is a primitive 8th root of unity and compute the inverse $\omega^{-1} = 2^{-1}$.
3. Compute the matrices V_ω and $V_{\omega^{-1}}$ and their product.
4. Trace Algorithm **??** on input ω, f and ω, g and compute with the result $(y_0, \ldots, y_7) = \mathbf{DFT}_\omega(f) \cdot \mathbf{DFT}_\omega(g)$.
5. Trace Algorithm **??** on input ω^{-1}, y an compare your result with 1.

Lattices & Geometry of Numbers and Algorithmic Consequences.

Def: A lattice is a set of the Form $\Lambda(A) = \{A \cdot x : x \in \mathbb{Z}^n\}$

$A \in \mathbb{Z}^{d \times n}$ of full row-rank.

Example: $A = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$



Algorithmic Problems: 1.) Given $A \in \mathbb{Z}^{d \times n}$ (full row-rank), $v \in \mathbb{Z}^d$,

determine whether $v \in \mathcal{L}(A)$ and if yes compute $x \in \mathbb{Z}^n$ s.t.

$A \cdot x = v$ (Lattice Membership problem)

2.) Given $A \in \mathbb{Z}^{d \times n}$ of full row-rank, determine

a nonzero vector $v \in \mathcal{L}(A)$ with $\|v\|$ minimal.

(Shortest (Lattice) Vector problem)

Membership Problem: Input $A \in \mathbb{Z}^{d \times n}$ of full row-rank.

$v \in \mathbb{Z}^d$. **Q:** $v \in \mathcal{L}(A)$.

Q: $\exists x \in \mathbb{Z}^n : \quad A \cdot x = v \quad (*)$???

$\exists x \in \mathbb{Q}^n$: Gaussian Algo

OBSERVATION: If $d = n$, then

$\exists! x^* \in \mathbb{Q}^n$ sol. $(*)$, so $v \in \mathcal{L}(A) \Leftrightarrow x^* \in \mathbb{Z}^n$

Q: $\exists\ B \in \mathbb{Z}^{d \times d}$ s.th. $\mathcal{L}(A) = \mathcal{L}(B)$?

IF YES, HOW TO COMPUTE IT ?

Def: $B \in \mathbb{Z}^{d \times d}$ with $\Lambda(B) = \Lambda(A)$ is called a **Basis** of the lattice $\Lambda(A)$.

Lemma: Let $U \in \mathbb{Z}^{n \times n}$ be a unimodular matrix, i.e. $\det(U) = \pm 1$. Then $\Lambda(A) = \Lambda(A \cdot U)$

Proof: Let $v \in \Lambda(A)$. Then $\exists x \in \mathbb{Z}^n$ s.th. $v = A \cdot x$.

But $\exists y \in \mathbb{Z}^n$ s.th. $U \cdot y = x$, since $U^{-1} \in \mathbb{Z}^{n \times n}$.

$\Rightarrow v = A \cdot U \cdot y \Rightarrow v \in \Lambda(A \cdot U) \Rightarrow \Lambda(A) \subseteq \Lambda(A \cdot U)$

Also. $\Lambda(A \cdot U) \subseteq \Lambda(A \cdot U \cdot U^{-1}) = \Lambda(A)$ ∎

Elementary unimodular Transformations:

1.) Swap two columns of A: $\rightarrow A \cdot U$

$$\det(U) = -1$$

$$U = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & & 1 & \\ & & & \ddots & & \\ & & 1 & & 0 & \\ & & & & & 1 \end{bmatrix}$$

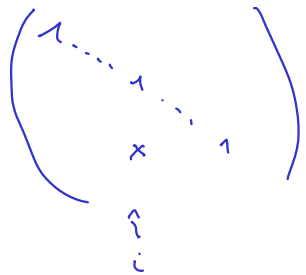
2.) Multiplying a column with (-1): $A := A \cdot U$ with

$$U = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & -1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \quad . \quad \det(U) = -1 .$$

3.) Add an integer multiple of one column from another column of A: $A := A \cdot U$.

$U =$

$j \rightarrow$



x times column j from column i.

$\det(U) = 1$

Def: $A \in \mathbb{Z}^{d \times n}$ of full row-rank is in Hermite Normal Form (HNF) if it is of this form

$$A = d\left(\begin{array}{c|c} B & 0 \end{array}\right)$$

(B is $d \times d$)

- Each entry of B is ≥ 0
- The unique max of every row is on the diagonal.

Example:

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 \end{array}\right)$$

Thm: Let $A \in \mathbb{Z}^{d \times n}$ of full row-rank.

$\exists\, U \in \mathbb{Z}^{n \times n}$ with $\det(U) = \pm 1$ s.th.

$A \cdot U$ is in HNF.