Fourier Transforms in Computer Science

Can a function $[0,2\pi] \to \mathbb{R}$ be expressed as a linear combination of $\sin nx$, $\cos nx$?

If yes, how do we find the coefficients?

If $f(x) = \sum_{n \in Z} a_n \exp(2\pi i\, n\, x)$

Fourier's recipe

then

$$a_n = \int_0^1 f(x) \exp(-2\pi i\, n\, x)\, dx$$

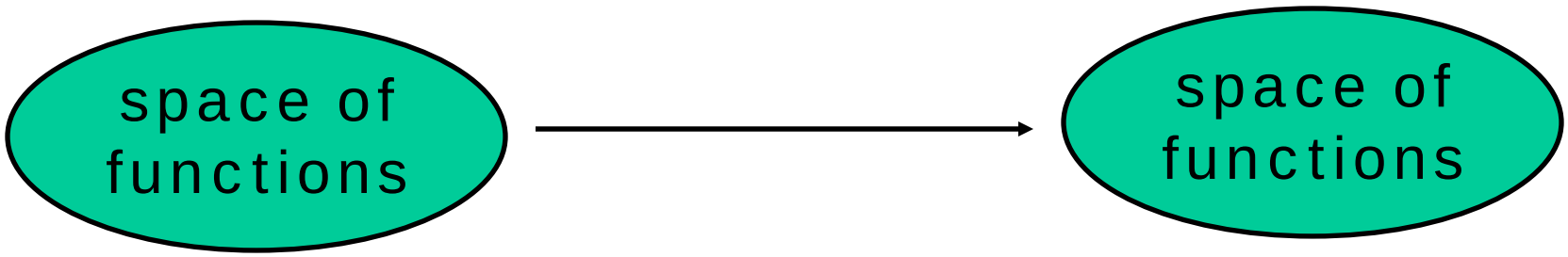
The reason that this works is that

the $\exp(-2\pi i\, nx)$ are orthonormal with respect to the inner product

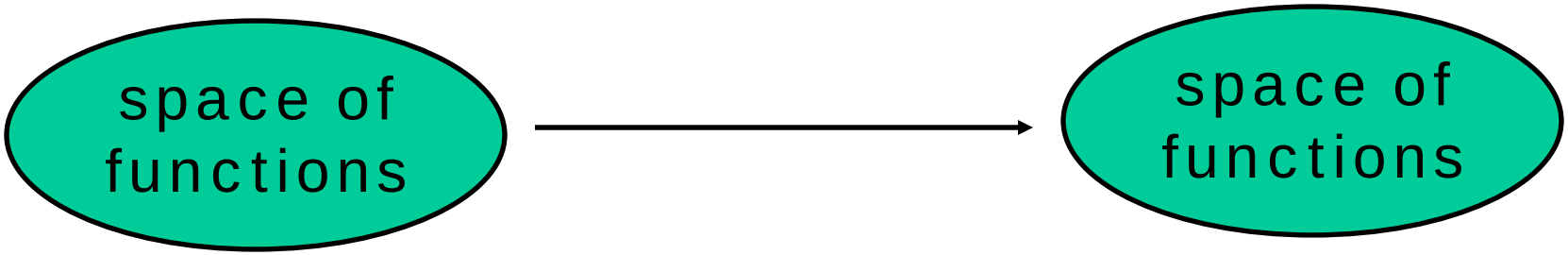
$$\langle f, g \rangle = \int_0^1 f(x) \overline{g(x)}\, dx$$

Given “good” f:[0,1] C we define its Fourier transform as f:Z C

$$f(n) = \int_0^1 f(x)\exp(-2\pi i\, n\, x)\, dx$$



Fourier Transform

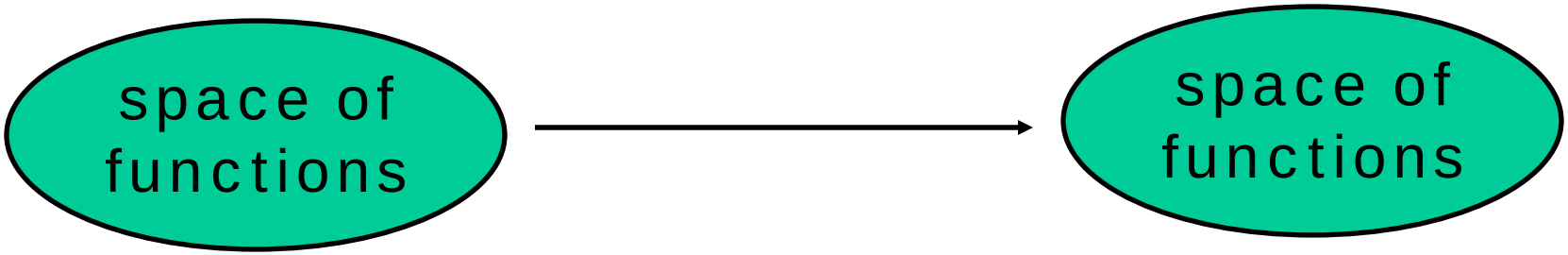


Fourier Transform

$L^2[0,1]$ isometry $L^2(Z)$

Plancherel formula $\langle f,g \rangle = \langle f,g \rangle$

Parseval's identity $\|f\|_2 = \|f\|_2$



Fourier Transform

convolution ⟶ pointwise multiplication

$f * g \longrightarrow \widehat{f}\,\widehat{g}$

$$(f*g)(x)=\int_0^1 f(y)g(x-y)\,dy$$

Can be studied in a more general setting:

interval [0,1] → LCA group G

Lebesgue measure and integral → Haar measure and integral

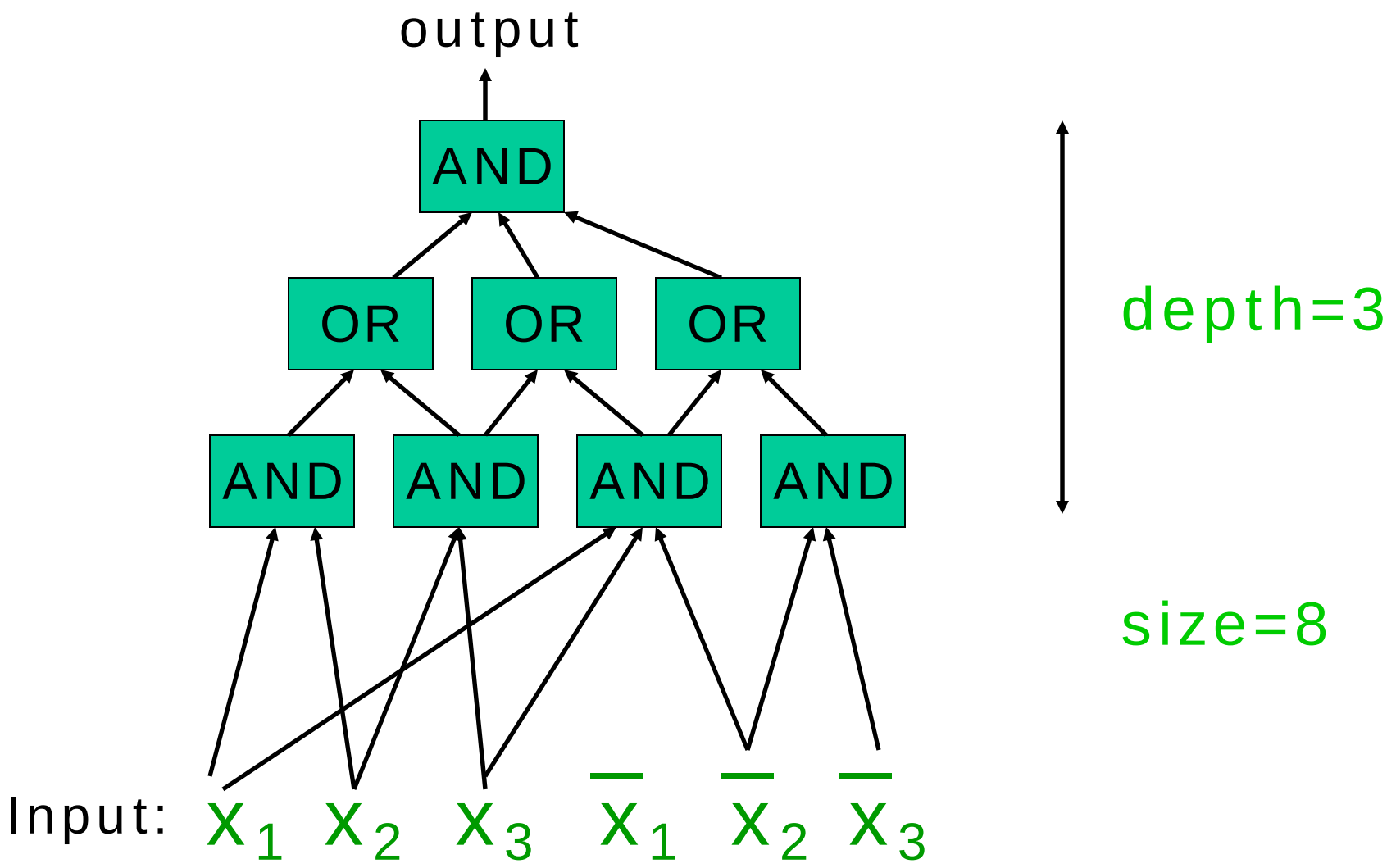
$\exp(2\pi i\, n\, x)$ → characters of G

form a topological group G, dual of G → continuous homomorphisms G → C

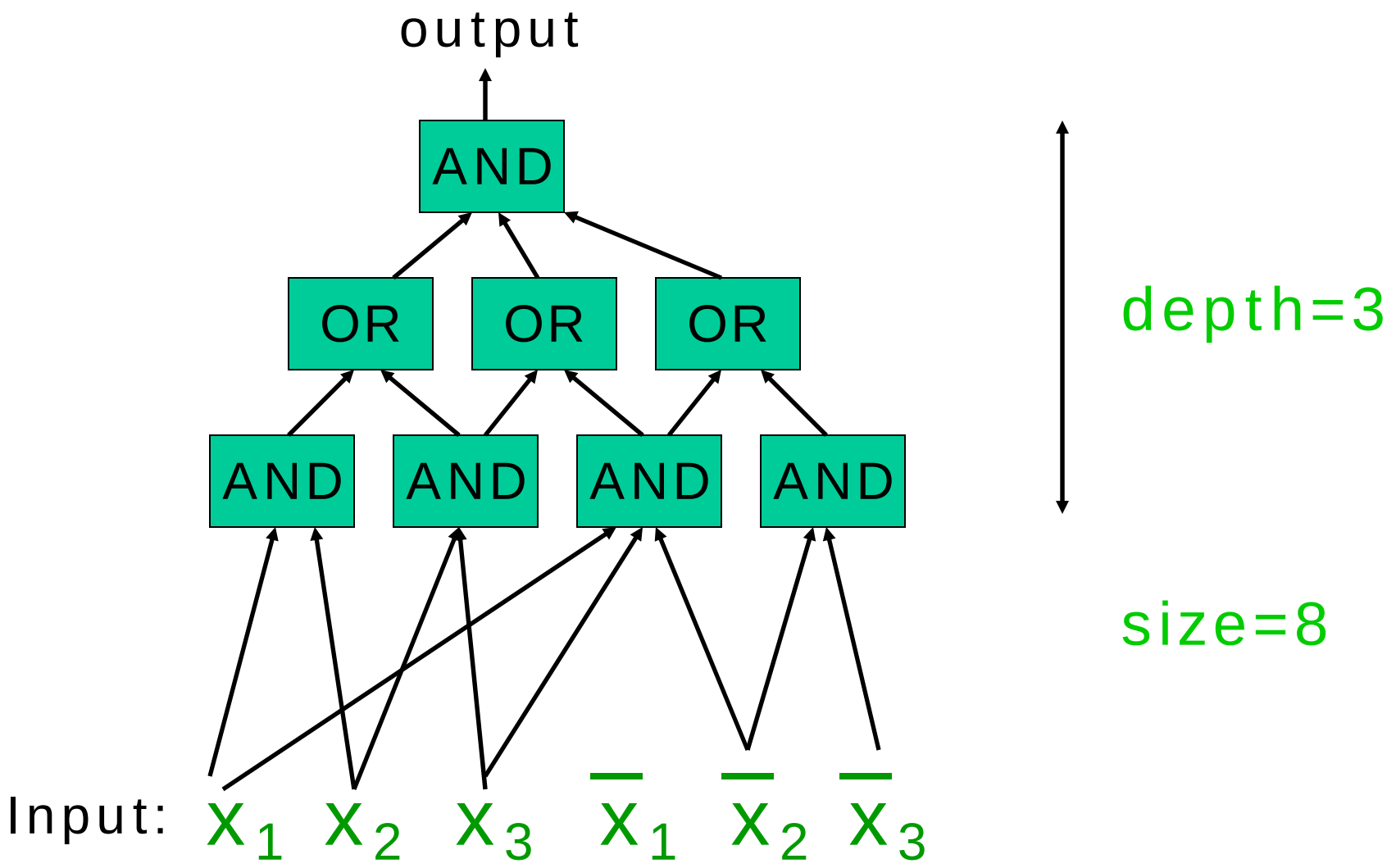
Fourier coefficients of AC^0 functions

Linial, Mansour, Nisan ‘93

circuit

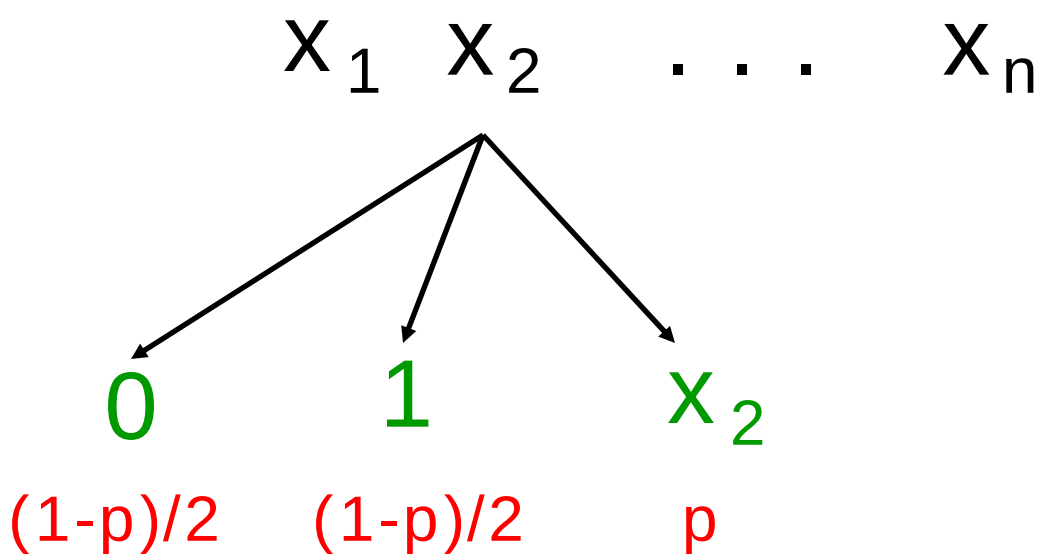

output
AND
OR
OR
OR
AND
AND
AND
AND
depth=3
size=8
Input:
x_1 x_2 x_3 $\overline{x}_1$ $\overline{x}_2$ $\overline{x}_3$

AC^0 circuits ⟶ constant depth, polynomial size



Random restriction of a function

$$f : \{0,1\}^n \quad \{0,1\}$$



Fourier transform over Z_2^n

characters

$$\chi_A(x) = \prod_{i \in A} (-1)^{x_i}$$

for each subset of {1,...,n}

Fourier coefficients

$$f(A) = P(f(x)=\chi_A(x)) - P(f(x)\neq\chi_A(x))$$

Håstad switching lemma

$f \in AC^0$ high Fourier coefficients of a random restriction are zero with high probability

All coefficients of size >s are 0 with probability at least

$$1-M(5p^{1/d}s^{1-1/d})^s$$

size of the circuit

depth

We can express the Fourier coefficients of the random restriction of f using the Fourier coefficients of f

$$E[r(x)] = p^{|x|} f(x)$$

$$E[r(x)^2] = p^{|x|} \sum_{y \supseteq \bar{x}} f(x+y)^2 (1-p)^{|y|}$$

Sum of the squares of the high Fourier coefficients of an AC^0 Function is small

$$\sum_{|x|>s} f(x)^2 < 2M \exp\left(-\frac{1}{5e}(t/2)^{1/d}\right)$$

Learning of AC^0 functions

Influence of variables on Boolean functions

Kahn, Kalai, Linial ‘88

The Influence of variables

$I_f(x_i)$

The influence of x_i on $f(x_1, x_2, \ldots, x_n)$

set the other variables randomly

the probability that change of x_i will change the value of the function

Examples: for the AND function of n variables
each variable has influence $1/2^n$

for the XOR function of n variables
each variable has influence 1

The Influence of variables

$I_f(x_i)$

The influence of x_i in $f(x_1, x_2, \ldots, x_n)$

set the other variables randomly

the probability that change of x_i will change the value of the function

For balanced f there is a variable with influence > (c log n)/n

We have a function f_i such that $I(x_i)=\|f_i\|_p^p$, and the Fourier coefficients of f_i can be expressed using the Fourier coefficients of f

$$f_i(x)=f(x)-f(x+i)$$

$$f_i(x) = 2f(x) \quad \text{if } i \text{ is in } x$$
$$= 0 \quad \text{otherwise}$$

We can express the sum of the influences using the Fourier coefficients of f

$$\sum I(x_i) = 4 \sum |x| \, f(x)^2$$

if f has large high Fourier coefficients then we are happy

How to inspect small coefficients?

Beckner's linear operators

$f(x) \longrightarrow a^{|x|} f(x) \qquad a<1$

Norm 1 linear operator

from $L^{1+a^2}(Z_2^n)$ to $L^2(Z_2^n)$

Can get bound ignoring high FC

$$\sum I(x_i)^{4/3} > 4 \sum |x|\, f(x)^2\, (1/2)^{|x|}$$

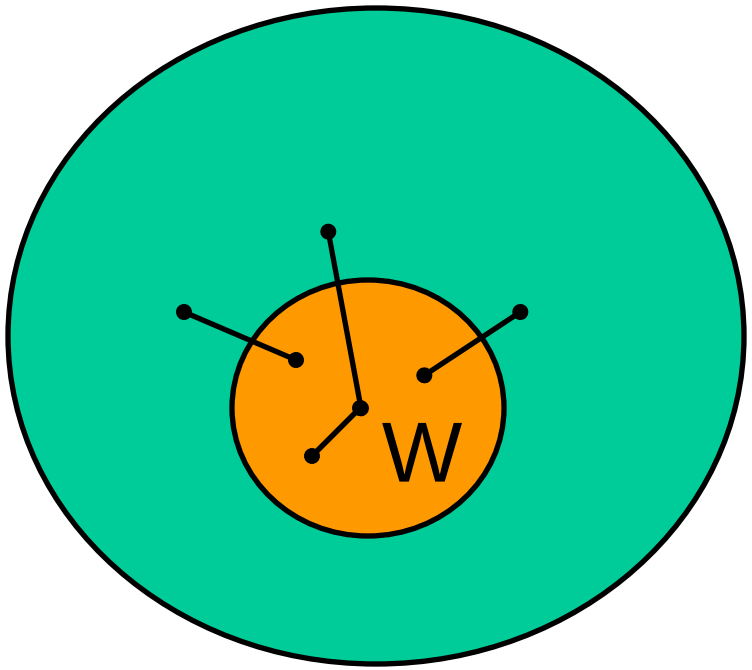
Explicit Expanders

Gaber, Galil ’79 (using Margulis ’73)

Expander

Any (not too big) set of vertices W
has many neighbors (at least $(1+a)|W|$)

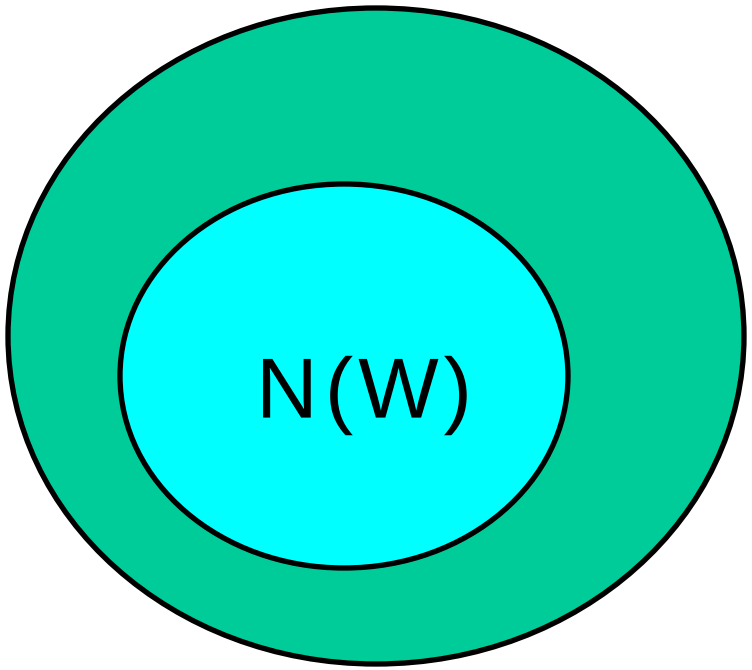
positive
constant



Expander

Any (not too big) set of vertices W
has many neighbors (at least (1+a)|W|)

positive
constant



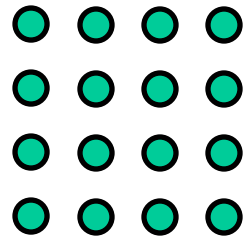
|N(W)|>(1+a)|W|

Why do we want explicit expanders of small degree?

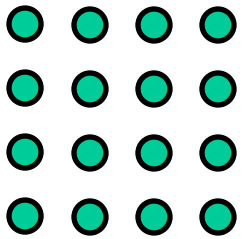
extracting randomness

sorting networks

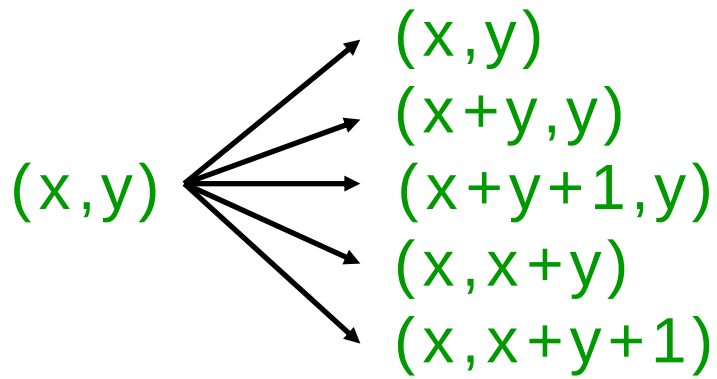
Example of explicit bipartite expander of constant degree:



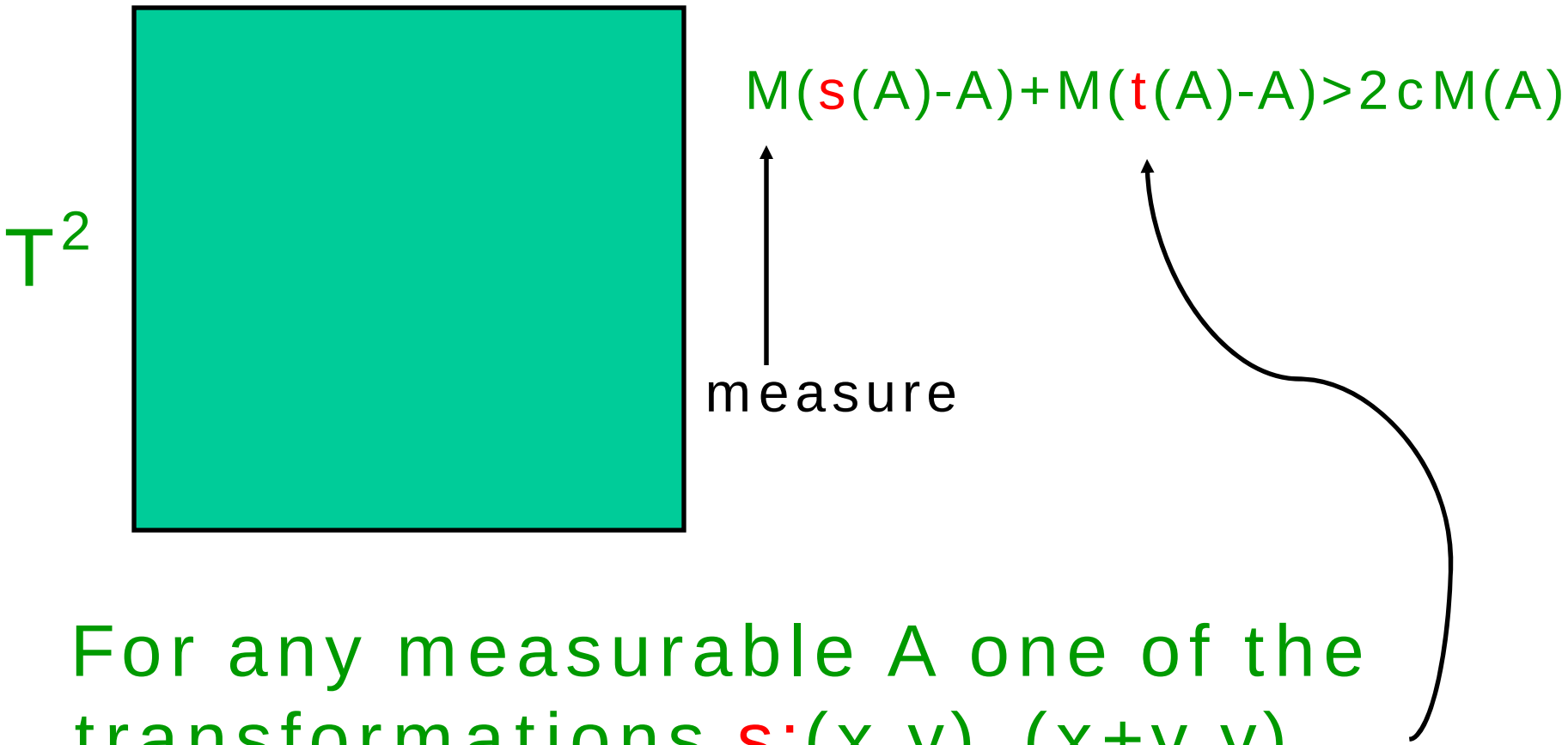
$Z_m \times Z_m$



$Z_m \times Z_m$



Transform to a continuous problem



For any measurable A one of the transformations s:(x,y) (x+y,y) and t:(x,y) (x,x+y) “displaces” it

Estimating the Rayleigh quotient of an operator on X $L^2(T^2)$

Functions with f(0)=0

$$(T\ f)\ (x,y)=f(x-y,y)+f(x,y-x)$$

$$r(T)=\sup\ \{\ |\langle Tx,x\rangle|\ ;\ \|x\|=1\}$$

It is easier to analyze the corresponding linear operator in Z^2

$$(S\ f)(x,y)=f(x+y,y)+f(x,x+y)$$

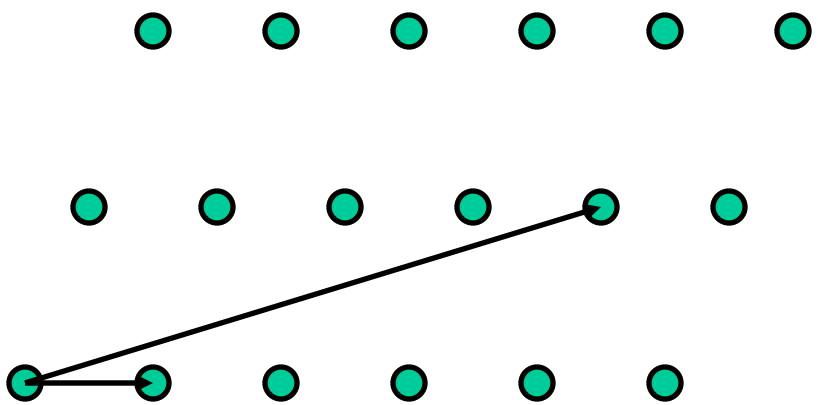
Let L be a labeling of the arcs of the graph with vertex set Z x Z and edges (x,y) (x+y,y) and (x,y) (x,x+y) such that L(u,v)=1/L(v,u). Let C be maximum over all vertices of sum of the labels of the outgoing edges. Then r(S) C.

Lattice Duality: Banaszczyk's Transference Theorem

Banaszczyk '93

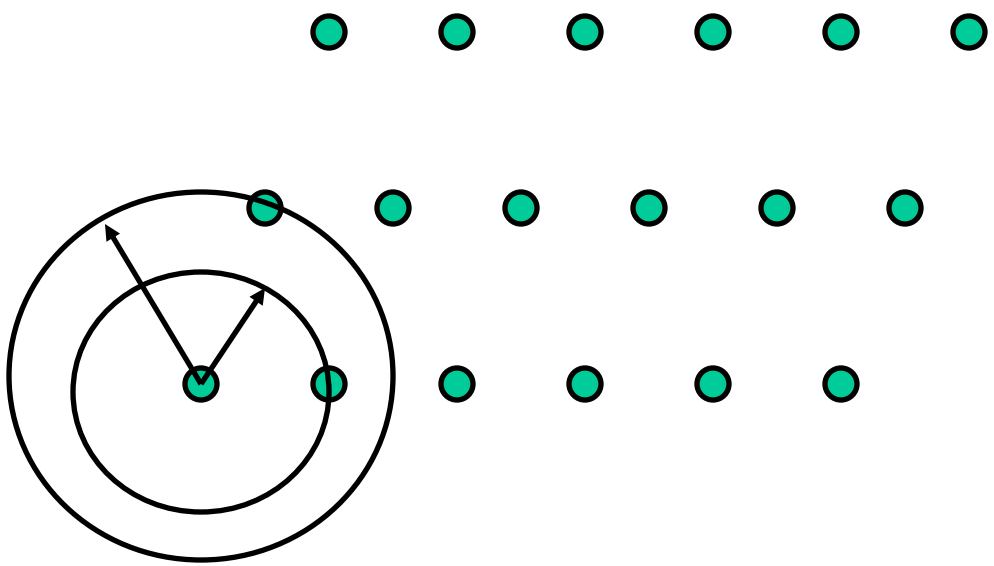
Lattice:

given n x n regular matrix B,
a lattice is $\{ Bx;\ x \in Z^n \}$



Successive minima:

λ_k smallest r such that a ball centered in 0 of diameter r contains k linearly independent lattice points



Dual lattice:

Lattice L^* with matrix B^{-T}

Transference theorem:

$$\lambda_k \lambda^*_{n-k+1} \quad n$$

can be used to show that O(n) approximation of the shortest lattice vector in 2-norm is not NP-hard unless NP=co-NP

(Lagarias, H.W. Lenstra, Schnorr' 90)

Poisson summation formula:

For “nice” f:R C

$$\sum_{x \in Z} f(x) = \sum_{x \in Z} f(x)$$

Define Gaussian-like measure on the subsets of R^n

$$r(A)=\sum_{x\in A} \exp(-\pi \|x\|^2)$$

Prove using Poisson summation formula:

$$r((L+u)\backslash B)<0.285\ r(L)$$

a ball of diameter $(3/4)n^{1/2}$ centered around 0

Define Gaussian-like measure on the subsets of R

$$p(A) = r(A \cap L)/r(L)$$

Prove using Poisson summation formula:

$$p(u) = r(L^{*}+u)/r(L^{*})$$

If $\lambda_k \lambda^*_{n-k+1} > n$ then we have

a vector u perpendicular to all lattice points in $L \cap B$ and $L^* \cap B$

outside ball

small + small

inside ball, "moved by u"

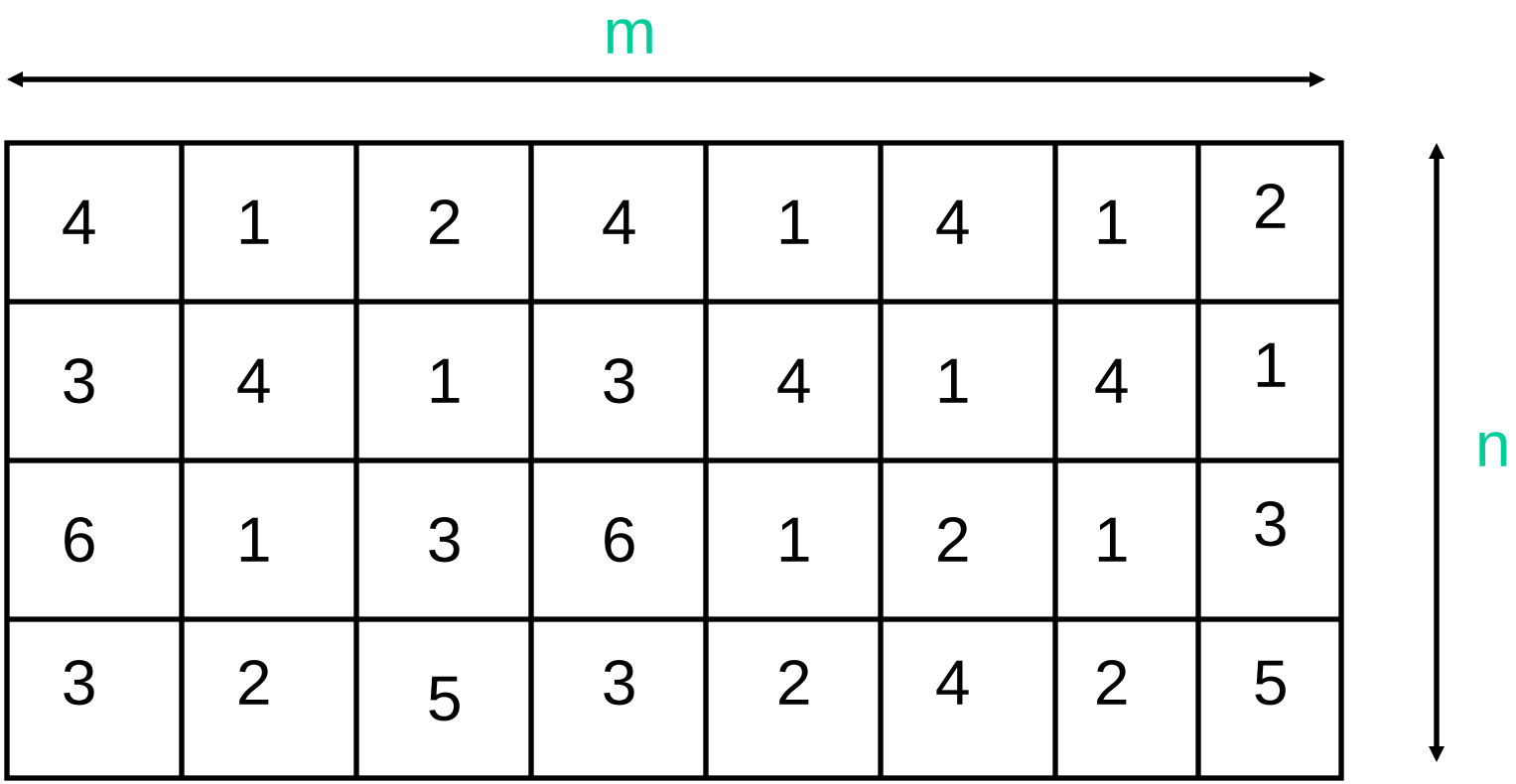
$r(L^*+u)/r(L^*)$

$$p(u)=\sum_{x \in L} r(x)\exp(-2\pi i u^T x)$$

large

Weight of a function – sum of columns (mod m)

Thérien ‘94



Is there a set of columns which sum to the zero column (mod t) ?

If $m > c\, n\, t^{11/2}$ then there always exists a set of columns which sum to zero column (mod t)

wt(f)= number of non-zero Fourier coefficients

$w(fg) \quad w(f)w(g)$

$w(f+g) \quad w(f)+w(g)$

t+1 is a prime

$$f_i(x) = g^{x_1 a_{i,1} + \ \cdots \ + x_m a_{i,m}}$$

If no set of columns sums to the zero column mod t then

$$g = \prod (1-(1-f_i)^t)$$

restricted to $B=\{0,1\}^m$ is 1_0

$$t^m = wt(g\ 1_B)\ \ t^n\ (t-1)^m$$