What is in this class ?

II Function spaces:

The example of fast multiplication of large integers using methods from signal processing

A contribution by Dora Ganter, 2020

MAST 10007 Linear Algebra

Integer multiplication in time $O(n \log n)$

David Harvey and Joris van der Hoeven

Abstract. We present an algorithm that computes the product of two n-bit integers in $O(n \log n)$ bit operations, thus confirming a conjecture of Schönhage and Strassen from 1971. Our complexity analysis takes place in the multitape Turing machine model, with integers encoded in the usual binary representation. Central to the new algorithm is a novel "Gaussian resampling" technique that enables us to reduce the integer multiplication problem to a collection of multidimensional discrete Fourier transforms over the complex numbers, whose dimensions are all powers of two. These transforms may then be evaluated rapidly by means of Nussbaumer's fast polynomial transforms.

Submitted on 28 Nov 2020

David Harvey, Joris van der Hoeven. Integer multiplication in time O(n log n). Annals of Mathematics, Princeton University, Department of Mathematics, In press. hal-02070778v2

Key ideas of Schönhage and Strassen

Revisiting natural numbers and the notion of "Place Value"

$$\begin{aligned} 4035 &= 5 \times 1 + 3 \times 10 + 0 \times 100 + 4 \times 1000 \\ &= 5 \times x^0 + 3 \times x^1 + 0 \times x^2 + 4 \times x^3 \end{aligned}$$

with $x = 10$.

Multiplication of natural numbers can be translated into polynomial multiplication.

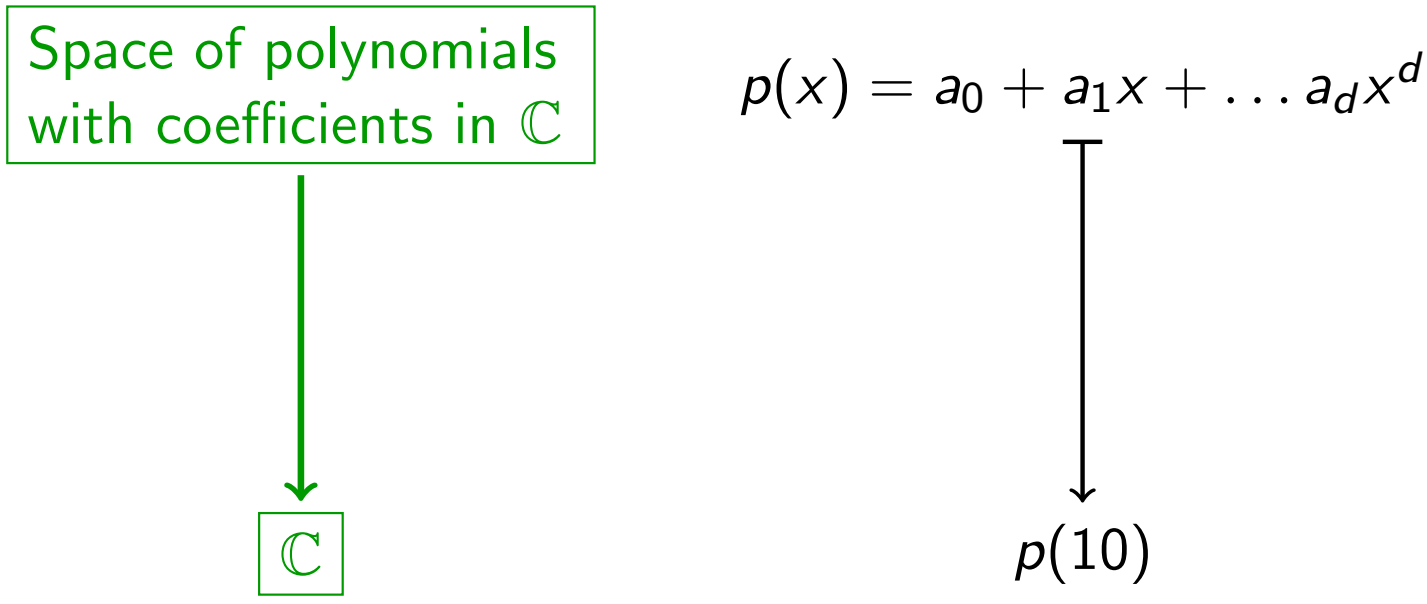
Binary setting

In fact, Schönhage and Strassen work with powers of 2 rather then 10, e.g., 4035 would be

$$\begin{aligned} 111111000011 &= 1 \times 2048 + 1 \times 1024 + 1 \times 512 + 1 \times 256 \\ &\quad +1 \times 128 + 1 \times 64 + 0 \times 32 + 0 \times 16 \\ &\quad +0 \times 8 + 0 \times 4 + 1 \times 2 + 1 \times 1 \end{aligned}$$

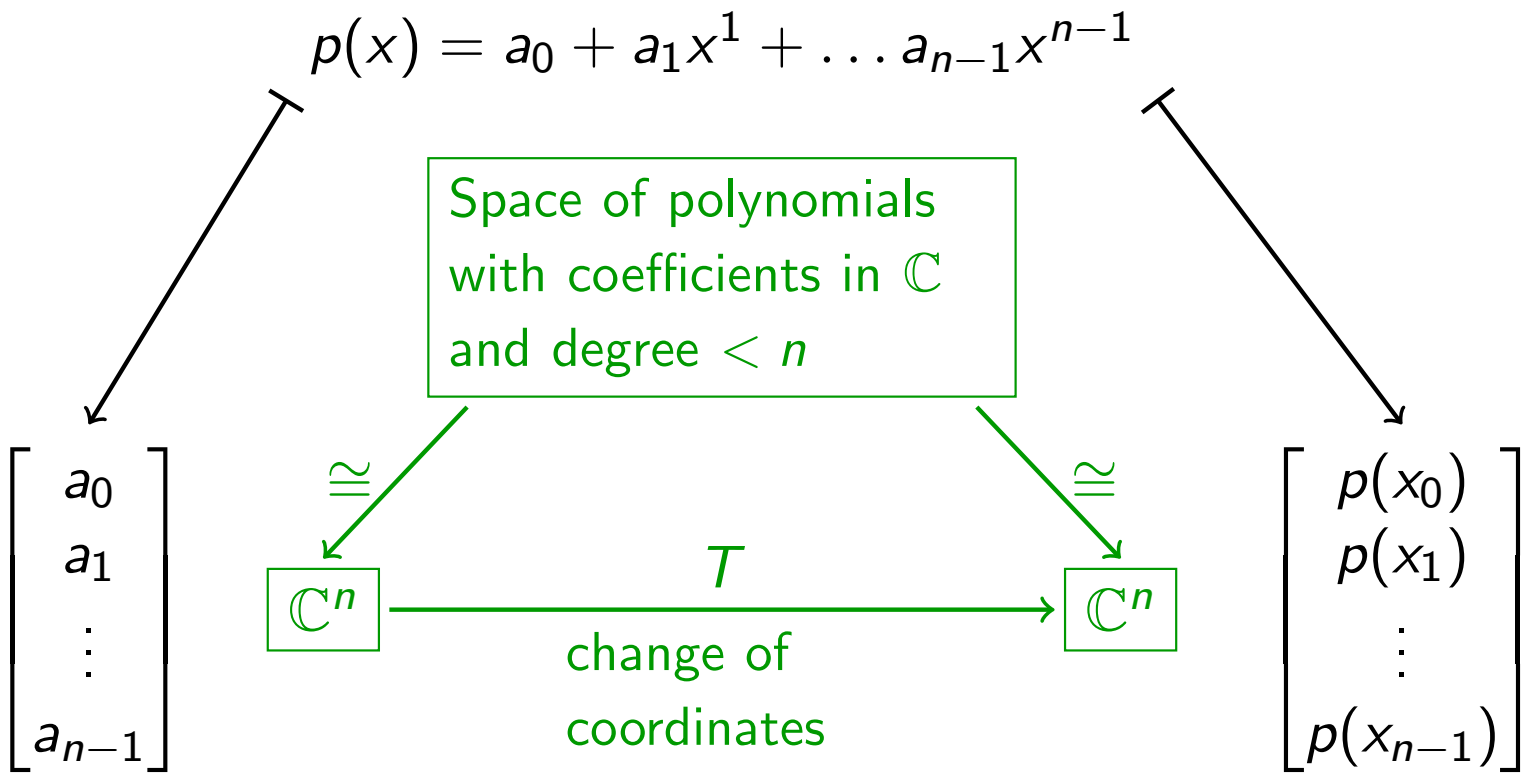
It is easier for the computer to deal only with the two digits 0 and 1 (off/on).

Evaluation at a fixed data point as linear operator



Evaluation at 10 is a linear operator taking as inputs polynomials and giving as output a number.

Two ways to parametrise spaces of polynomials



vector of coefficients

bad for multiplication

sampling at n distinct data points

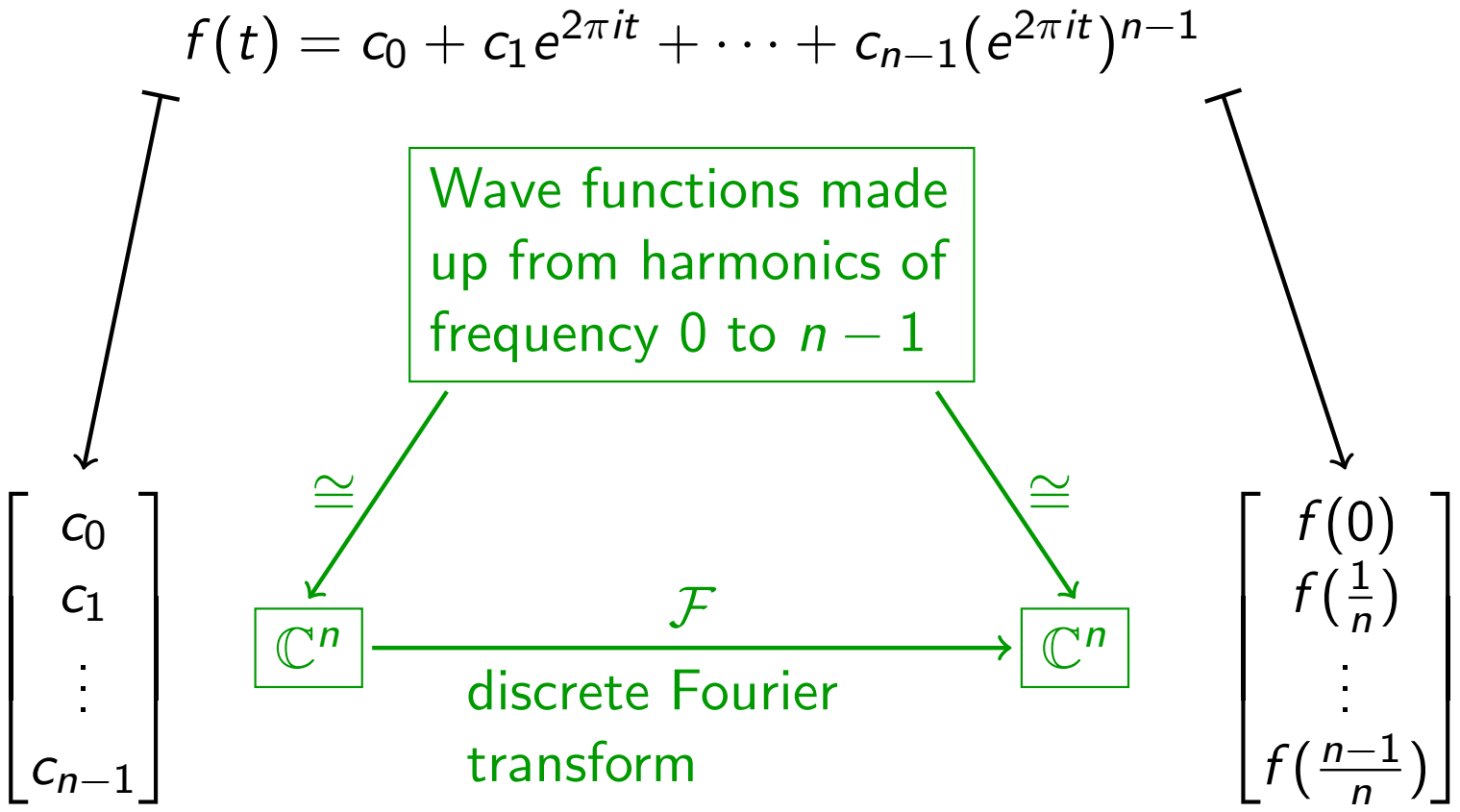
good for multiplication

Change of coordinates matrix

$$T = \begin{bmatrix} 1 & x_0 & \dots & x_0^{n-1} \\ 1 & x_1 & \dots & x_1^{n-1} \\ \vdots & & & \vdots \\ 1 & x_{n-1} & \dots & x_{n-1}^{n-1} \end{bmatrix}$$

Choose data points $x_0, \dots x_{n-1}$ yielding nice T and small $p(x_i)$!

Inspiration from signal processing: wave functions

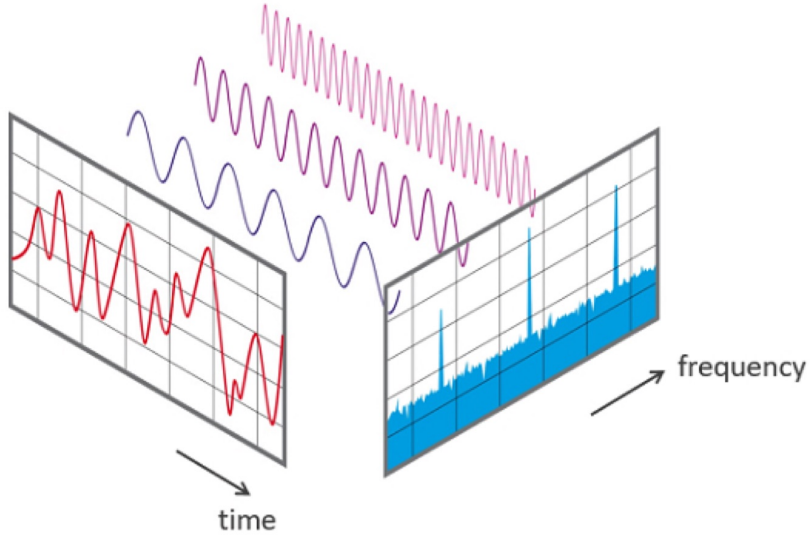


frequency components

sampling at evenly spaced data points

$$e^{2\pi it} = \cos(2\pi t) + i \sin(2\pi t).$$

When studying waves, use complex numbers!



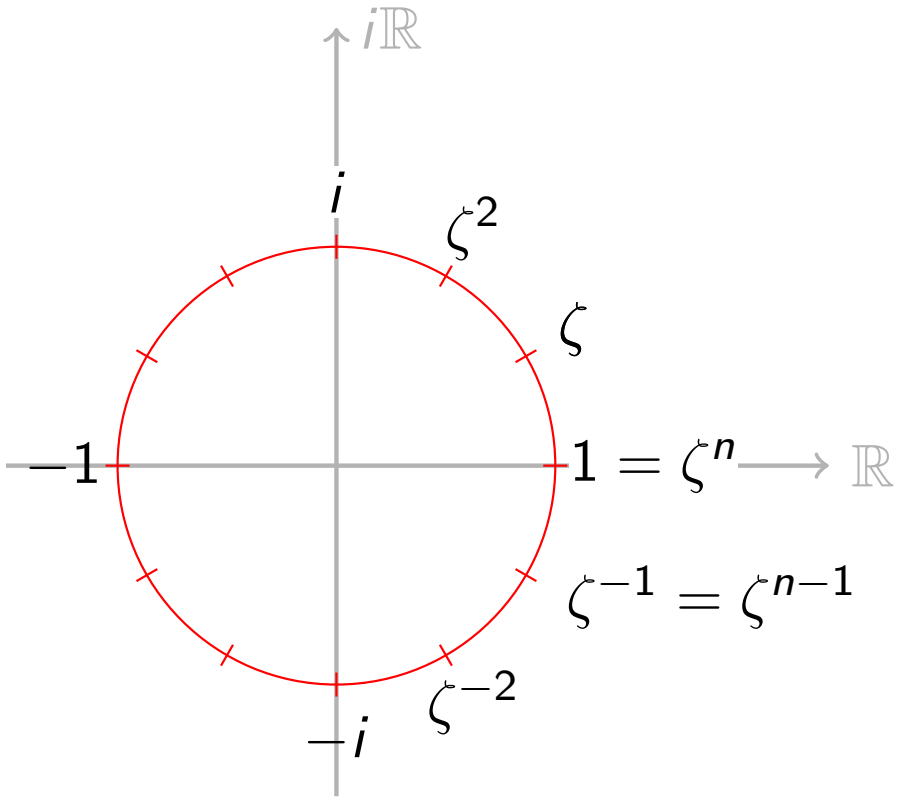
Electrical engineers are the first to know the difference—they take your Fourier transform as they meet you (if you are a function). Fourier's idea is to represent f as a sum of harmonics $c_k e^{ikx}$. The function is seen in *frequency space* through the coefficients c_k, instead of *physical space* through its values $f(x)$.

Gilbert Strang
Introduction to
Linear Algebra

Matrix of the discrete Fourier transform

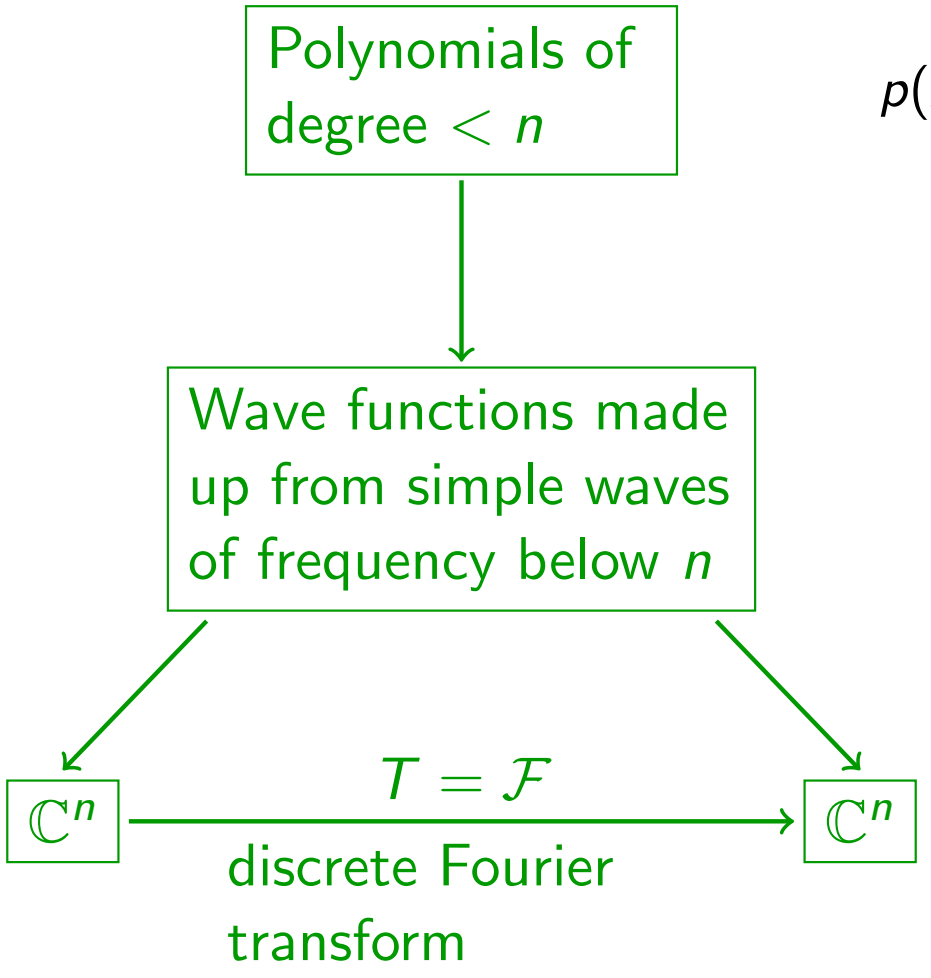
$$\zeta := e^{\frac{2\pi i}{n}}$$

$$\mathcal{F} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta & \zeta^2 & \dots & \zeta^{-1} \\ 1 & \zeta^2 & \zeta^4 & \dots & \zeta^{-2} \\ \vdots & & \vdots & & \vdots \\ 1 & \zeta^{-1} & \zeta^{-2} & \dots & \zeta \end{bmatrix}$$



In the example on the left, $n = 12$

Substitute $x = e^{2\pi it}$ in $p(x)$



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

$$\downarrow$$

$$a_0 + a_1 e^{2\pi it} \ldots a_n e^{2(n-1)\pi it}$$

$$\downarrow$$

$$\begin{bmatrix} p(1) \\ p(\zeta) \\ \vdots \\ p(\zeta^{n-1}) \end{bmatrix}$$

a_i count frequency components

powers of ζ as data samples for p