

Categorification of Fourier Transforms, Efficient Computation and Computing Intelligence

Nikolaj M. Glazunov

Glushkov Institute of Cybernetics National Academy of Sci. (Kiev)

Email: glanm@yahoo.com

Abstract

We investigate a category theory and homological algebra framework for various types of Fourier transforms (Fourier, Fourier-Deligne, Fourier-Cato, Fourier-Mukai) and efficient algorithms for their implementation.

Overwhelming majority of the fundamental methods for Physics have set theoretic foundations. A category theory framework (by means of a category \mathcal{C} or a functor \mathcal{F}) for a system S , a process Π or a phenomenon Φ can be thought as a collection of objects A, B, \dots , one for each element of S (respectively Π, Φ) which are combined by morphisms $f : A \rightarrow B$, subject to the conditions (i) and (ii) below. Let $\mathcal{C}(A, B)$ be the class of morphisms from A to B . Then

- (i) for any three (not necessary distinct) objects A, B or C of \mathcal{C} , there is defined a map

$$\mathcal{C}(A, B) \times \mathcal{C}(B, C) \rightarrow \mathcal{C}(A, C),$$

called composition which satisfied the *associativity* axiom.

- (ii) For every objects A of \mathcal{C} , the set $\mathcal{C}(A, A)$ contains a morphism id_A , called the identity of A .

A *functor* \mathcal{F} from a category \mathcal{C} to a category \mathcal{K} is a function which maps $Ob(\mathcal{C}) \rightarrow Ob(\mathcal{K})$, and which for each pair A, B of objects of \mathcal{C} maps $\mathcal{C}(A, B) \rightarrow \mathcal{C}(\mathcal{F}(A), \mathcal{F}(B))$, while satisfying the two conditions:

$$\mathcal{F}id_A = id_{\mathcal{F}A} \text{ for every } A \in Ob(\mathcal{C}),$$

$$\mathcal{F}(fg) = \mathcal{F}(f)\mathcal{F}(g).$$

Our talk will illustrate the consequences for the category theory treatment of data representation and analysis, scientific computations, models of interaction and computing intelligence. Also we discuss several optimization and computer algebra problems concerning the approach.

Plan

Abstract

Introduction. motivation

motivations from Computer Sci. & AJ

DFT and the generation of pseudo-random sequences

Fast multiplication of complex polynomials

Fast integer multiplication

Algebraic expressions, processing of the expressions and their categorification

Complexes, homotopy categories, cohomologies and quasiisomorphisms

Bounded derived categories

Fourier-Mukai transform

Its generalizations and applications

Conclusions

Some references

Introduction. Motivation

Categorification of some Physical Theories and Problems:

String Theory

Homological Mirror Symmetry (Kontsevich, Fukaya,...)

Categorification of various kinds of Fourier Transforms:

Deligne – Fourier transform;

Sato – Fourier transform;

Mukai – Fourier transform and its generalizations;

Categorification of Computer Science, Control Theory and some branches of Numerical Analysis (for instance, Interval Computations.)

*Motivation of the Categorification from
Mathematical and Physical points of
view :*

works by Japanese researchers

K. Fukaya

M. Sato

S. Mukai

M. Kashiwara

Motivations from computer science
and A/T

Example 1 Discrete Fourier Transform
(DFT) and the generation of pseudo-
random sequences

Applications: cryptography (stream
ciphers)

E. Berlekamp, J. Massey

Let p be an odd natural number,

$s = \{s_i\}_{i \geq 0}$ the binary p -periodic
sequence,

$c_i \in \mathbb{F}_2$ (\mathbb{F}_2 is the field $\mathbb{Z}/2\mathbb{Z}$)

Problem: What is the minimal $m = m(s)$
of a linear recursion

$$s_{k+m} = \sum_{i \leq m} c_i \cdot s_{k+i} \quad \text{for all } k \geq 0$$

that generates a given periodic sequence s ?

Solution: the minimal $m = m(s)$ of s
equals the Hamming weight of its Fourier
spectrum

The solution is based on elementary number-theoretic lemma and DFT

Lemma. There exists a finite field \mathbb{F}_{2^d} of characteristic 2 containing a primitive p -th root g of unity: $g \in \mathbb{F}_{2^d}$, $x^{p-1} = (x-g^0) \dots (x-g^{p-1}) = 0$, all $g^i \in \mathbb{F}_{2^d}$.

Here the minimal such $d \mid \varphi(p)$, where φ is the Euler function.

Algorithm

Input: The length p , an odd natural number;
a primitive p -root g of unity;
a binary vector $(s_0, s_1, \dots, s_{p-1})$.

Output: The rank of the diagonal matrix
 $\text{diag}(\hat{s}_0, \hat{s}_1, \dots, \hat{s}_{p-1})$,
where $(\hat{s}_0, \hat{s}_1, \dots, \hat{s}_{p-1})$ is the Fourier spectrum of $(s_0, s_1, \dots, s_{p-1})$.

Step 1. Construct the matrix

$$DFT = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & g & \dots & g^{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & g^{p-1} & \dots & g^{(n-1)(p-1)} \end{pmatrix},$$

Step 2. Compute the Fourier spectrum

$$(\hat{s}_0, \hat{s}_1, \dots, \hat{s}_{p-1}) = (s_0, s_1, \dots, s_{p-1}) \cdot DFT$$

Step 3. Compute the Hamming weight $w(s)$
(the number of non-zero components) of
 $(\hat{s}_0, \dots, \hat{s}_{p-1})$.

All computations in \mathbb{F}_2^d .

By Cooley-Tukey the algorithm is $O(n \log n)$

Example 2: Fast multiplication of complex polynomials
(Cody - Tukey)

Let n be a natural number,
 $f(z), g(z) \in \mathbb{C}[z]$, $\deg f + \deg g < n$,
 g is a primitive root of the equation
 $x^n - 1 = 0$ in \mathbb{C} , cyclic convolution,
DFT , $O(n \log n)$

Example 3: Fast integer multiplication
(Schönhage and Strassen)

Let a, b be big integer numbers with
binary representation of the length N .

Problem: compute $a \cdot b \bmod (2^w + 1)$

Solution: computation of the cyclic convolutions using DFT , $O(N \log N \log \log N)$

Another examples

- digital filtering
- Reed-Muller codes
- data compression
- learning

Algebraic expressions, processing of the expressions and their categorification

Let FinSet be the category of finite sets

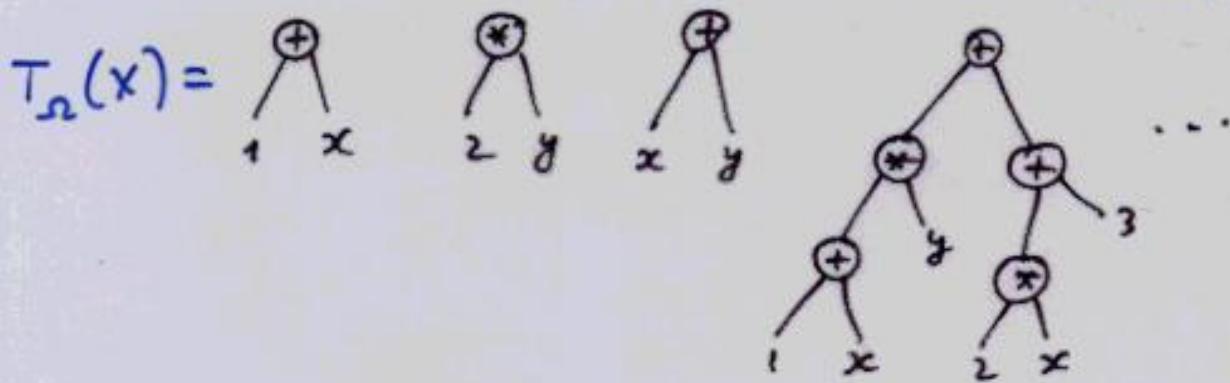
$\Omega \text{FinSet} = \{\text{finite sets } (X, Y, Z, \dots) \}$

$\text{Hom}(X, Y) = \{\text{maps from } X \text{ to } Y\}$

Let $\Omega = \bigcup_{n=0}^k \Omega_n$ be the ranked alphabet.

$T_\Omega(X)$ is the set of finite trees on X generators

Example : $\Omega_0 = \{1, 2, 3\}, \Omega_2 = \{+, *\}, X = \{x, y\}$



$T_\Omega(\cdot)$ is the functor

let ΩAlg be the category of Ω -algebras:

Example : $A = \{+, -\} \times \{0, 1\}^{64}, \mathbb{I}_A = +0..01,$

$\sim_A : A \rightarrow A$ reverse signs,

Complexes, homotopy categories, cohomologies
and quasiisomorphisms (by Gelfand -
 manin)

The cochain complex

$$(K^{\bullet}, d) = \{ K^0 \xrightarrow{d} K^1 \xrightarrow{d} \cdots \xrightarrow{d} K^n \xrightarrow{d} \cdots \}$$

is the sequence of abelian groups and differentials
 $d: K^p \rightarrow K^{p+1}$ with the condition $d \circ d = 0$.

Let A be an abelian category, $\text{Kom}(A)$ the category of complexes over A . There are many full subcategories of $\text{Kom}(A)$ whose respective objects are the complexes which are bounded below, bounded above, bounded in both sides.

Lemma-definition (i) Let K^{\bullet}, L^{\bullet} be two complexes over abelian category A , $k = k^i: K^i \rightarrow L^{i-1}$ a sequence of morphisms between elements of the complexes.

Then the maps

$$h = kd + dk: K^{\bullet} \rightarrow L^{\bullet}$$

i.e.

$$h^i = k^{i+1} d_{K^i} + d_{L^i} k^i: K^i \rightarrow L^i$$

$$\begin{array}{ccccccc} \cdots & K^{i-1} & \xrightarrow{k^i} & K^i & \xrightarrow{dk} & K^{i+1} & \longrightarrow K^{i+2} \longrightarrow \cdots \\ & \downarrow h^i & \nearrow k^i & \downarrow h^{i+1} & \nearrow k^{i+1} & \ddots & \ddots \\ \cdots & L^{i-1} & \xrightarrow{d_L^{i-1}} & L^i & \xrightarrow{d_L^i} & L^{i+1} & \longrightarrow L^{i+2} \longrightarrow \cdots \end{array}$$

The morphism h is called homotopic to zero ($h \sim 0$);
 (ii) morphisms that are homotopic to zero form the ideal:
 $h_1 \sim 0, h_2 \sim 0, \Rightarrow h_1 + h_2 \sim 0; f \cdot h_1 \sim 0, \Theta h_2 \sim 0$, if they exist.

(iii) morphisms $f, g: K^\bullet \rightarrow L^\bullet$ is called homotopic, if $f-g = kd + dk \sim 0$ ($f \sim g$), k is called homotopy;

(iv) if $f \sim g$ then $H^*(f) = H^*(g)$, where the map H^* is induced on cohomologies of complexes.

The homotopy category $K(A)$ is defined by the following way:

$\text{mor } K(A) = \text{mor Kom}(A)$ by the module of homotopy equivalence.

Let X be a topological space and K^\bullet, L^\bullet be complexes of sheaves over X . The quasimorphism is the map $f: K^\bullet \rightarrow L^\bullet$

which induces the isomorphism of cohomological sheaves

$$f_*: \mathcal{H}^q(K^\bullet) \rightarrow \mathcal{H}^q(L^\bullet), q \geq 0.$$

Bounded derived categories

Definition - theorem. Let A be an abelian category, $\text{Kom}(A)$ the category of complexes \bullet in A . There exists the category $D(A)$ and the functor $Q: \text{Kom}(A) \rightarrow D(A)$ with following properties:

a) for any quasimorphism f the morphism $Q(f)$ is the isomorphism.

b) If $F: \text{Kom}(A) \rightarrow D'$ some other functor, which transforms quasimorphisms to morphisms, then $\exists!$ (only one) functor

$G: D(A) \rightarrow D'$ such that $F = G \circ Q$.

The category $D(A)$ is called the derived category of an abelian category A .

Fourier-mukai transform

Some important problems and methods of Math. Physics have natural Algebraic Geometry, Category Theory and Homological Algebra representation.

Examples: String Theory

Homological mirror Symmetry

D-branes

A Fourier transform

$$\hat{f}(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(t) e^{-itx} dt$$

and its n -dimensional generalization, could be loosely described as "pullback" a function to $\mathbb{R}^n \times \mathbb{R}^n$ multiply by ~~exp~~ $\exp(-i\langle t, x \rangle)$ and take the direct image (integrate) with respect to the second variable.

FMT was defined by Mukai for abelian varieties, Generalizations: by Bartocci, Bruzzo, Hernández-Ruipérez, Maciocia, Bridgeland, Yoshioka, Mukai, ...

Let A be an abelian variety of dimension n ,
 (if $n=1$ this is an elliptic curve)

\hat{A} be the dual abelian variety (a moduli space of line bundles of degree 0 on A),

$$\pi_1: A \times \hat{A} \rightarrow A,$$

$$\pi_2: A \times \hat{A} \rightarrow \hat{A}.$$

A Poincaré bundle P is a line bundle of degree zero on the product $A \times \hat{A}$, defined in such a way that for all $a \in \hat{A}$, the restriction of P on $A \times \{a\}$ is isomorphic to the line bundle corresponding to the $a \in \hat{A}$, (universal bundle).

Let \mathcal{C}_A the category of \mathcal{O}_A -modules on A ,

$$\mathcal{C}_{\hat{A}} = \dots \dashv \hat{A},$$

$M \in \mathcal{C}_A$, $\mathcal{D}(A)$, $\mathcal{D}(\hat{A})$ - bounded derived categories of coherent sheaves on A and \hat{A} .

$$\hat{S}(M) = \pi_{\hat{A}, *}^*(P \otimes \pi_A^* M).$$

FMT:

the derived functor $R\hat{S}$

Importance of derived categories of coherent sheaves on complex manifolds M .

Let $D(M)$ be the bounded derived category of coherent sheaves on M .

Theorem (Bondal, Orlov, Politelski).

If M is projective and the canonical or anti-canonical bundle of M is ample, then the manifold M can be reconstructed from $D(M)$.

Theorem (Mukai)

The derived functor $R\hat{S}$ (Fourier-Mukai transform) induces an equivalence of categories between two derived categories $D(A)$ and $D(\hat{A})$.

—

$$S(M) = \pi_{A,*} (\mathcal{P} \otimes \pi_A^* M)$$

Theorem (Mukai) There are isomorphisms of functors

$$RS \circ R\hat{S} \cong (-\iota_A)^*[-g],$$

$$R\hat{S} \circ RS \cong (-\iota_{\hat{A}})^*[-g],$$

where $[-g]$ denotes "shift" the complex g places to the right.

The case of elliptic curves (by Mukai and Bridgeland)

Let E be an elliptic curve over \mathbb{C} .

$$y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \neq 0,$$

F a sheaf on E with its first Chern class $(c(F), d(F))$. Let a and b be coprime integers with $a > 0$ and let Y be the moduli space of stable bundles on E of Chern class (a, b) .

Let \mathcal{P} be a tautological bundle on $E \times Y$, and $D(E)$ the bounded derived category of coherent sheaves on E .

FMT RS

$$\text{let } A = \begin{pmatrix} c & a \\ d & b \end{pmatrix} \in SL_2(\mathbb{Z}), \quad a > 0$$

By some conditions on \mathcal{P} on $E \times \hat{E}$

$$\begin{pmatrix} c(RS\bar{F}) \\ d(RS\bar{F}) \end{pmatrix} = \begin{pmatrix} c & a \\ d & b \end{pmatrix} \begin{pmatrix} c(F) \\ d(F) \end{pmatrix}$$

For the usual FMT \bar{F} on E

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Conclusions (Summary)

- Categorification of mathematical and physical problems and structures in the frame of Homological Algebra is the method of linearization of the problems and structures (reducing to linearity)
- Relevant framework:
 - differential graded (dg) algebras and categories
 - derived categories, derived functors
 - A_∞ -algebras, categories and functors
- Needs 2-categories
- Categorification of physical and Comp. Sci. & AI problems has a similar Homological Algebra framework but
 - also has differences:
 - for physical problems there are representations mainly over complex numbers (Riemann surfaces)
 - for computer science & AI there are representations over field of characteristic $p > 0$.
- Thanks to reducing to linearity we can construct efficient algorithms
- Possibility of verified computations and results

References

- [1] Glazunov N. On computational aspects of the Fourier-Mukai transform. Int. Conf. SYMMETRY IN NONLINEAR MATHEMATICAL PHYSICS (2003) (Submitted)
<http://arXiv.org/abs/hep-th/0311009>
- [2] N.M. Glazunov, Category Theory Aspects of Complex Manifolds and Problems of Mirror Symmetry (in Russian,) *Problemy Program-mirovaniya*. No. 3-4, Kiev, (2002) pp.104-110.
- [3] Glazunov N. Interval Computations and their Categorification. SCAN2002. Int. Symposium on Scientific Computing, Computer Arithmetic, and Validated Numerics. Proceedings (Submitted)
<http://arXiv.org/abs/math.CT/0311021>
- [4] Glazunov N., Kapitonova Ju. On a common context of number theory and harmonic analysis. *Cybernetics and System Analysis*. N 1 (2003), pp.134-147.
- [5] Glazunov N. On Validated Numerics, Category Theory and Computer Algebra Framework for Simulation and Computation in Theoretical Physics, *Nuclear Inst. and Methods in Physics, A*, 2003. P.654-656.
- [6] Glazunov N. On algebraic geometric and computer algebra aspects of mirror symmetry. E-print. 11p. <http://arXiv.org/abs/hep-th/0112250>
- [7] Glazunov N. On Some Interval-Algebraic Methods for Verifications of Dynamical Systems. *Cybernetics and Computer Technologies. Complex Control Systems*. 109 (1997) p.15-23.
- [8] Glazunov N. Knowledge Base Systems and Dynamic Control Systems. *Cybernetics and Computer Technologies. Complex Control Systems*. 85 (1990) P.18-22.