代数同构视角下的离散 Fourier 变换 多项式环、求值插值与相似对角化

sun123zxy

2024-05-13

- ① 1. 从 Fourier 变换到 DFT
- ② 2. DFT 与多项式环
 - 2.1 引例: C[x]、求值插值与复数域 DFT
 - 2.2 整环上的推广
 - 2.3 唯一性的讨论
- 3. DFT 与矩阵代数

- 1. 从 Fourier 变换到 DFT
- 2 2. DFT 与多项式环
 - 2.1 引例: ℂ[x]、求值插值与复数域 DFT
 - 2.2 整环上的推广
 - 2.3 唯一性的讨论
- 3 3. DFT 与矩阵代数

Fourier 变换及其卷积性质

• Fourier 变换: 将给定函数 f 映为函数 $\mathcal{F}[f]$:

$$\mathcal{F}[\mathit{f}](\lambda) := \int_{-\infty}^{\infty} \mathit{f}(t) e^{-\mathrm{i}\lambda t} \, \mathrm{d}t$$

● 定义函数 f 和 g 的卷积

$$(f * g)(\lambda) := \int_{-\infty}^{\infty} f(\lambda - x)g(x) dx$$

则 Fourier 变换将两个函数的卷积化为逐点乘积,即

$$\mathcal{F}[f * g] = \mathcal{F}[f]\mathcal{F}[g]$$

复数域上的 DFT 及其卷积性质

• 离散 Fourier 变换 (Discrete Fourier Transform, DFT): 线性空间 $\mathbb{C}^n \to \mathbb{C}^n$ 上的线性变换 F, 将向量 $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})^{\mathrm{T}} \in \mathbb{C}^n$ 映为 $F\mathbf{a}$, 其第 i 个分量如下所示

$$(F\mathbf{a})_i := \sum_{k=0}^{n-1} \omega_n^{ik} a_i$$

这里分量下标从 0 开始计数, $\omega_n:=e^{2\pi \mathrm{i}/n}$ 是 $\mathbb C$ 上的一个 n 次本原单位根.

• 相仿的卷积性: 两个向量 $a, b \in \mathbb{C}^n$ 的循环卷积定义为

$$(\mathbf{a} * \mathbf{b})_k := \sum_{i+j=k \pmod{n}} a_i b_j$$

则 DFT 将两个向量的循环卷积化为逐项乘积 ×, 即

$$F(\mathbf{a} * \mathbf{b}) = (F\mathbf{a}) \times (F\mathbf{b})$$

矩阵表示

在 \mathbb{C}^n 的自然基下,变换 F 有矩阵表示

$$F = \left(\omega_n^{ij}\right)_{(i,j)\in n\times n} = \begin{pmatrix} 1 & 1 & \dots & 1\\ 1 & \omega_n & \dots & \omega_n^{n-1}\\ \vdots & \vdots & \ddots & \vdots\\ 1 & \omega_n^{n-1} & \dots & \omega_n^{(n-1)(n-1)} \end{pmatrix}$$

● 卷积性: 系数为全体复平面 n 次单位根的可逆 Vandermonde 矩阵

● 正交性: 适当单位化后为酉矩阵

问题¹

- DFT 化卷为乘的本质?
 - 我们给出一大类具备卷积性的线性映射的构造,DFT 将作为特例推出.
- 如何从代数角度理解 DFT?
 - 两个视角: 多项式环、矩阵代数
 - 两种表现: 求值插值、相似对角化
 - 一致观点: 保加法、保数乘、保乘法的代数同构
- DFT 是否是唯一一类化卷为乘的变换?作为底层结构的 ℂ 是否可以放宽?
 - 工程上复数乘法运算较慢且具有浮点误差,更换底层代数结构具有实际意义. 例如,被称为数论变换(number theoretic transforms, NTT)的 DFT 变种就将 $\mathbb C$ 替换为有限域 $\mathbb F_p$ 而同时保留了其卷积性质.
 - 我们将其 DFT 扩展至任意整环并证明特定含义下的唯一性.

¹Agarwal and Burrus [AB75]; Nicholson [Nic71]; Fürer [Für09]; Amiot [Ami16]; Baraquin and Ratier [BR23]

- 1. 从 Fourier 变换到 DFT
- 2 2. DFT 与多项式环
 - 2.1 引例: C[x]、求值插值与复数域 DFT
 - 2.2 整环上的推广
 - 2.3 唯一性的讨论
- 3 3. DFT 与矩阵代数

- 1. 从 Fourier 变换到 DFT
- ② 2. DFT 与多项式环
 - 2.1 引例: C[x]、求值插值与复数域 DFT
 - 2.2 整环上的推广
 - 2.3 唯一性的讨论
- 3. DFT 与矩阵代数

$\mathbb{C}[x]$ 与循环卷积

设不超过 n-1 次的多项式 $f(x) = \sum_{k=0}^{n-1} a_k x^k$, $g(x) = \sum_{k=0}^{n-1} b_k x^k$. 二者的多项式乘积由 Cauchy 乘积给出

$$f(x)g(x) = \sum_{i=0}^{n-1} a_i x^i \sum_{j=0}^{n-1} b_j x^j = \sum_{k=0}^{2n-2} x^k \sum_{i+j=k} a_i b_j$$

令 $\mathbf{a}:=(a_0,a_1,\dots,a_{n-1})^{\mathrm{T}}$, $\mathbf{b}:=(b_0,b_1,\dots,b_{n-1})^{\mathrm{T}}$, 回顾循环卷积定义

$$(\mathbf{a} * \mathbf{b})_k := \sum_{i+j=k \pmod{n}} a_i b_j$$

可见 Cauchy 乘积与循环卷积尚有区别. 稍加改动,若在模 x^n-1 的意义下——即商环 $\mathbb{C}[x]/(x^n-1)$ 中计算,则二者相合:

$$f(x)g(x) = \sum_{k=0}^{n-1} x^k \sum_{i+j=k \pmod{n}} a_i b_j \pmod{x^n - 1}$$

$\mathbb{C}[x]$ 与复数域 DFT

DFT 亦有在 $\mathbb{C}[x]$ 上的表示. 给定 $\mathbf{a} := (a_0, a_1, \dots, a_{n-1})^{\mathrm{T}} \in \mathbb{C}^n$,其对应多项式 $f(x) = \sum_{k=0}^{n-1} a_k x^k$ 次数不超过 n-1 次,则

$$(F\mathbf{a})_i = \sum_{k=0}^{n-1} \omega_n^{ik} \mathbf{a}_i = \sum_{k=0}^{n-1} \mathbf{a}_i (\omega_n^i)^k = f(\omega_n^i)$$

恰为 f(x) 分别在 $n \cap \mathbb{C}$ 上 n 次单位根处多点求值的结果.

- 可逆性: n 点唯一确定一个不超过 n-1 次的多项式 (Lagrange 插 值)
- 线性性: $(af + bg)(\omega_n^i) = af(\omega_n^i) + bg(\omega_n^i)$
- ullet 卷积性:将取模乘法化为点值逐项相乘,再次与 \mathbb{C}^n 上的表现相合

$$F(\mathbf{a} * \mathbf{b}) = (F\mathbf{a}) \times (F\mathbf{b})$$
$$(fg)(\omega_n^i) = f(\omega_n^i)g(\omega_n^i)$$

小结

- \mathbb{C}^n 与 $\mathbb{C}[x]$ 视角下的 DFT:
 - \mathbb{C}^n : 作为以单位根为参数的 Vandermonde 矩阵,DFT 是 \mathbb{C}^n 上的可 逆线性变换,将向量间的循环卷积 * 化为逐项乘积 \times .
 - $\mathbb{C}[x]$: 作为单位根处的多点求值插值,DFT 在全体不超过 n-1 次的 多项式和 \mathbb{C}^n 间建立起线性同构关系,将多项式乘积化为函数值逐点 乘积.
- 化卷为乘,就是把多项式环上的取模乘法变为 Cⁿ 上的逐项乘积, DFT 保持了两个代数结构间的乘法。
 - ullet $\mathbb{C}[x]$ 作为环结构乘法自然,在多项式环上刻画 DFT 较在 \mathbb{C}^n 上强行 定义循环卷积具有优越性.

- 1. 从 Fourier 变换到 DFT
- 2 2. DFT 与多项式环
 - 2.1 引例: C[x]、求值插值与复数域 DFT
 - 2.2 整环上的推广
 - 2.3 唯一性的讨论
- 3. DFT 与矩阵代数

代数、代数同构与直积

- 整环: 无零因子交换幺环
- 设 R 是一整环,若 $(A, +, \times)$ 为一环且配备了与乘法 \times 相容的 R-数乘 \cdot ,则称 A 是一 R-代数,不至混淆时简称代数.
 - 整环 R 自身也可视为一个代数.
- 我们将 R^n 理解为作为代数的 R 的直积,即 $R^n = R \times R \times \cdots \times R$. 直积的加法、数乘和乘法均在逐项意义下定义.
- 保持代数间加法、数乘和乘法的双射被称为代数同构.

几个观察与整环的优势

- 关于引例的若干观察:
 - DFT 是 $\mathbb{C}[x]/(x^n-1) \to R^n$ 的一个代数同构,具体做法是在单位根处多点求值插值
 - 求值插值在任意 n 个不同位置进行即可,单位根不是本质要求
 - 商环 $\mathbb{C}[x]/(x^n-1)$ 带来了与循环卷积对应的多项式取模乘法,还蕴含着 "不超过 n-1 次" 为求值插值带来的单与满
 - 第一同构定理: 设 $f\colon R\to S$ 是环同态,则 f 诱导出环同构 $R/\operatorname{Ker} f\cong \operatorname{Im} f$
- 选取整环作为底层代数结构的理由:
 - 交换: 确保求值操作是同态
 - 保留环上整除的结构和多项式根与因子的关系(带余除法、余式定理)
 - 在唯一性证明中发挥作用

商环到直积的代数同构

下面固定 R 是一整环. 令 C 是 R 的一有限子集,由若干不同一次 多项式乘积 $\prod_{c\in C}(x-c)$ 生成的 R[x] 上的理想记为 $\left(\prod_{c\in C}(x-c)\right)$.

用记号 \mathbb{R}^C 代表全体 \mathbb{C} 上的 \mathbb{R} 值函数构成的集合. \mathbb{R}^C 与其上定义的函数逐点加法、数乘和乘法构成一个代数,自然也与 \mathbb{R}^n 代数同构.

命题 2.1

多项式商环 $R[x]/\left(\prod_{c\in C}(x-c)\right)$ 与代数直积 R^C 代数同构.

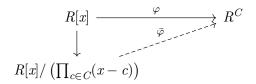


图 1: 命题 2.1 构造示意图

构造

考察 R[x] 到 R^C 上的代数同态 $\varphi: f \mapsto (C \ni x \mapsto f(x))$, 其含义为在每一 $c \in C$ 处对多项式 f 进行求值.

•
φ 的核:

$$\operatorname{Ker} \varphi = \{ f \in R[x] : f(C) = \{0\} \} = \left(\prod_{c \in C} (x - c) \right)$$

• φ 的像: 对每个 $c\in C$ 对应的理想 (x-c) 应用中国剩余定理就有 ${\rm Im}\, \varphi=R^C.$

故由第一同构定理, φ 诱导的

$$\bar{\varphi}: R[x] / \left(\prod_{c \in C} (x - c) \right) \to R^C$$

是一同构映射.

DFT: 代数同构的特例

作为上一定理的特例,DFT 在单位根处求值插值。若 ω_n 为内嵌于 R 的某一 n 阶循环(乘法)群的生成元,则称其为 R 上的 n 次本原单位根.

推论 2.1

若 R 上存在 n 次本原单位根 ω_n ,则多项式

$$x^{n} - 1 = \prod_{k=0}^{n-1} (x - \omega_{n}^{k})$$

故 $R[x]/(x^n-1)$ 与 R^n 代数同构. 我们便称二者间的代数同构为 R 上的 n 点 DFT.

- 1. 从 Fourier 变换到 DFT
- 2 2. DFT 与多项式环
 - 2.1 引例: C[x]、求值插值与复数域 DFT
 - 2.2 整环上的推广
 - 2.3 唯一性的讨论
- 3. DFT 与矩阵代数

全体代数同构的结构

已经建立 $R[x]/(m(x)) \to R^n$ 的同构关系,这里 m(x) 是若干不同一次因式的乘积。但这种同构或不止一种。为研究其是否在某种意义下具有唯一性,需研究全体同构 $\mathrm{Iso}(R[x]/(m(x)),R^n)$ 的结构。该问题化归为研究 R^n 上全体自同构 $\mathrm{Aut}(R^n)$ 的结构。

命题 2.2

设 \mathcal{A} 是一与 R^n 同构的任一代数. 固定代数同构 $\varphi:\mathcal{A}\to R^n$, 则任一 $\mathcal{A}\to R^n$ 的代数同构 f 都具有形式 $f=p\varphi$, 这里 $p\in \operatorname{Aut}(R^n)$.

<ロト < /p>

R^n 上的自同构

设 e_1,\ldots,e_n 是 R^n 上的自然基,设 $\sigma\in S_n$ 是有限集 $\{0,1,\ldots,n-1\}$ 上的一个置换。定义 R^n 上由置换 σ 诱导的模自同构

$$P_{\sigma}: \mathbf{e}_k \mapsto \mathbf{e}_{\sigma(k)}$$

容易验证 P_{σ} 保持逐项乘法,因此它也是 R^n 上的代数自同构。 下面的引理刻画了 R^n 上代数自同构的形式。

引理 2.1

全体 P_{σ} 构成 R^n 上全体代数自同构,即

$$\operatorname{Aut}(R^n) = \{ P_{\sigma} : \sigma \in S_n \}$$

只需证对任意 R^n 上任意代数自同构 P,其都可被某一置换 $\sigma \in S_n$ 诱导得到. 不妨考察 P 在 R^n 自然基下的矩阵表示 $(p_{i,j})_{(i,j)\in n\times n}$. 则

$$P(\mathbf{e}_i) \times P(\mathbf{e}_i) = P(\mathbf{e}_i \times \mathbf{e}_i) = P(\mathbf{e}_i)$$

可分行写为对 $k=0,1,\ldots,n-1$, 都有 $p_{k,i}^2=p_{k,i}$, 因为 R 是整环, 故 $p_{k,i}$ 为 0 或 1,即矩阵各元素只能取 0 或 1. 又对 $i\neq j$ 将

$$P(\mathbf{e}_i) \times P(\mathbf{e}_j) = P(\mathbf{e}_i \times \mathbf{e}_j) = P(\mathbf{0}) = \mathbf{0}$$

分行写开,得对 $k=0,1,\ldots,n-1$,都有 $p_{k,i}p_{k,j}=0$. 于是(由 R 是整环)矩阵任一行至多只能由一个 1. 假如存在第 k 行全为 0,则 $e_k\notin\operatorname{Im} P$,与 P 作为自同构的满性矛盾,故 P 的矩阵表示每行有且只有一个 1,其余为 0. P 的某两行亦不能完全相同,否则(由鸽巢原理)矩阵某列一定全为 0,与 P 作为自同构的单性矛盾。因此 P 的矩阵表示是一个置换矩阵,即 P 由一置换诱导。

DFT 的唯一性

推论 2.2

设 f 是任一 R 上的 n 点 DFT,则任何 R 上的 n 点 DFT g 都具有形式 $g = P_{\sigma}f$,这里 f 是一事先固定的 n 点 DFT.

作为推论,n 点 DFT 共有 n! 种. 这一结果的显著性在于,只要不计求值得到的 n 个点值在 R^n 上的排列顺序,DFT 是唯一满足卷积性质的可逆线性映射.

- 1. 从 Fourier 变换到 DFT
- 2 2. DFT 与多项式环
 - 2.1 引例: ℂ[x]、求值插值与复数域 DFT
 - 2.2 整环上的推广
 - 2.3 唯一性的讨论
- 3. DFT 与矩阵代数

第二个视角: 矩阵代数

我们建立了

$$R[x]/(m(x)) \xrightarrow{\bar{\varphi}} R^n \xrightarrow{\bar{\varphi}}^{P_{\sigma}}$$

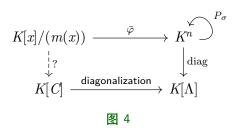
$$\boxtimes 3$$

这一交换图可以继续扩展,将视角从多项式环转向矩阵代数,我们将看到,DFT 不仅是多项式环上的求值插值,更体现为矩阵代数上的相似对角化。

简单起见,下面只考察代数闭域的情况,并用域的常用记号 K 替代 R.

相似对角化

设 C 是域 K 上的 n 阶可对角化矩阵,特征值两两不同。设其特征多项式(或最小多项式)为 m(x), Λ 为其对角化得到的矩阵。K[C] 和 $K[\Lambda]$ 分别是矩阵 C 和 Λ 在 $K^{n\times n}$ 上生成的代数。



对角化 C 的矩阵也同时对角化了 K[C] 中的任意矩阵。若设这一对角化矩阵为 F,则 $A\mapsto F^{-1}AF$ 便规定了一个 $K[C]\to K[\Lambda]$ 的代数同构。 K^n 与 $K[\Lambda]$ 的代数同构是平凡的。下面来建立 K[x]/m(x) 与 K[C] 间的联系。

命题 3.1

设 C 是域 K 上的 n 阶矩阵,m(x) 是其最小多项式,则 K[x]/m(x) 与 K[C] 代数同构.

仍然考察 $K[x] \to K[C]$ 自然的 "代入" $\psi: f \mapsto f(C)$. C 的全体零化 多项式恰为 m(x) 生成的 K[x] 上的理想,因此 $\mathrm{Ker}\, \psi = (m(x))$. ψ 的满射性平凡.用第一同构定理就得到结论.

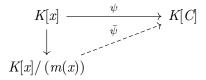


图 5: 命题 3.1 证明示意图

友矩阵

为显式刻画上述对角化过程,我们选取一类特殊的矩阵 2 作为 C 进 行研究:

$$C = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ -c_0 & -c_1 & -c_2 & \dots & -c_{n-1} \end{pmatrix}$$

C 被称为首一多项式 $m(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_0$ 的友矩阵 (companion matrix).

- 直接计算, C 的特征多项式恰为 m(x).
- 直接验证, $(1, \lambda, \dots, \lambda^{n-1})^T$ 是其特征值 λ 的一个特征向量.

²这类矩阵在高阶常系数线性 ODE 和常系数齐次线性递推中也有重要应用。 📱

友矩阵的最小多项式

命题 3.2

C 的最小多项式也恰为 m(x). 等价地,友矩阵的特征多项式与最小多项式相同.

等价地,我们研究 C^{Γ} 的最小多项式. 注意到如下事实:

$$C^{\mathrm{T}} \mathbf{e}_{i} = \begin{cases} \mathbf{e}_{i+1} & i = 0, 1, \dots, n-2 \\ -\sum_{k=0}^{n-1} c_{k} \mathbf{e}_{k} & i = n-1 \end{cases}$$

考察任意不超过 n-1 次的 C^{Γ} 的零化多项式 $f(x):=\sum_{k=0}^{n-1}a_kx^k$,有

$$\mathbf{0} = f(C^{\mathrm{T}})\mathbf{e}_0 = \sum_{k=0}^{n-1} a_k (C^{\mathrm{T}})^k \mathbf{e}_0 = \sum_{k=0}^{n-1} a_k \mathbf{e}_k$$

因此 $a_k = 0$ 对所有 k 成立,即 f = 0. 这说明 C^{Γ} 的(非零)零化多项式次数至少为 n. 再用零化多项式和最小多项式的整除关系就得到结论。

上述命题的逆命题在相似意义下成立。

命题 3.3

若矩阵的特征多项式与最小多项式相同,则它与其特征多项式对应 的友矩阵相似.

可在 Jordan 标准型下理解. 此时每个特征值对应的 Jordan 块有且只有一个.

当友矩阵 C 可对角化时,其最小多项式可分解为不同一次因式的乘积。又其最小多项式与特征多项式相同,故其必有 n 个两两不同的特征值 $\lambda_0,\lambda_1,\ldots,\lambda_{n-1}$ 结合上述命题可以看到,我们特殊地取 C 为友矩阵做研究是不失一般性的.

友矩阵对角化的显式表达

前面已经得到友矩阵特征向量的形式,因此 Vandermonde 矩阵

$$F = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \lambda_0 & \lambda_1 & \dots & \lambda_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_0^{n-1} & \lambda_1^{n-1} & \dots & \lambda_{n-1}^{n-1} \end{pmatrix}$$

正是将 C 对角化的矩阵.

$$F^{-1}CF = \Lambda = \operatorname{diag}(\lambda_0, \lambda_1, \dots, \lambda_{n-1})$$

注意到 K[C] 也被对角化 C 的矩阵同时对角化,故 $A\mapsto F^{-1}AF$ 确为 $K[C]\to K[\Lambda]$ 的代数同构,与先前的关于对角化的讨论结果一致.

循环矩阵的对角化

特别地,若取

$$C = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

它是基本循环矩阵,对应最小多项式 $m(x)=x^n-1$. C 生成的代数 K[C] 即 $K^{n\times n}$ 上的全体循环矩阵. 此时 DFT 体现为利用 DFT 矩阵

$$F = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega_n & \dots & \omega_n^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n^{n-1} & \dots & \omega_n^{(n-1)(n-1)} \end{pmatrix}$$

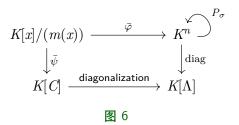
对循环矩阵进行对角化的过程.

结语

以刻画 DFT 的卷积性质为目标,以代数同构为构造手段,我们为理解 DFT 的代数含义提供了两个视角:

- DFT 是多项式商环上的多点求值插值
- DFT 是矩阵代数上的相似对角化

可见 DFT 背后的代数理论非常丰富,不失为联系起本科阶段代数课程的有趣实例,亦体现出代数工具与视角在工程实践中的强大效用。



参考文献

- [AB75] R.C. Agarwal and C.S. Burrus. "Number theoretic transforms to implement fast digital convolution". In: Proceedings of the IEEE 63.4 (Apr. 1975), pp. 550–560. ISSN: 1558-2256. DOI: 10.1109/PROC.1975.9791.
- [Ami16] Emmanuel Amiot. Music Through Fourier Space. Computational Music Science. Cham: Springer International Publishing, 2016. ISBN: 978-3-319-45580-8 978-3-319-45581-5. DOI: 10.1007/978-3-319-45581-5.
- [BR23] Isabelle Baraquin and Nicolas Ratier. "Uniqueness of the discrete Fourier transform". In: Signal Processing 209 (Aug. 2023), p. 109041. ISSN: 0165-1684. DOI: 10.1016/j.sigpro.2023.109041.

参考文献 ||

- [Für09] Martin Fürer. "Faster Integer Multiplication". In: SIAM Journal on Computing 39.3 (Jan. 2009), pp. 979–1005. ISSN: 0097-5397. DOI: 10.1137/070711761.
- [Nic71] Peter J. Nicholson. "Algebraic theory of finite fourier transforms". In: Journal of Computer and System Sciences 5.5 (Oct. 1971), pp. 524–547. ISSN: 0022-0000. DOI: 10.1016/S0022-0000(71)80014-4.