Матрицы Вандермонда и быстрые преобразования Фурье

> Цель статьи выделить класс матриц которые позволяют использовать методы FFT и в частности NTT (Число-Теоретическое преобразование) при вычислении умножения матриц. Вид матриц Вандермонда допускает диагонализацию и переход к симметричной матрице Вандермонда.

#матрица Вандермонда, дискретное преобразование Фурье, Cyclotomic fast Fourier transform

Данное изложение построено на основе статьи [1]. Частным случаем квадратной матрицы Вандермонда является матрица дискретного преобразования Фурье (DFT) составленная из корней ω степени N из единицы. В методе теоретико-числового преобразования (NTT), который является частным случаем DFT поверх колец полиномов, мы используем вектор неповторяющихся элементов x_j с требованием $x_j^N = \alpha$. Матрицу $N \times N$ Вандермонда общего вида можно представить в виде произведения симметричной матрицы Вандермонда и диагональной матрицы, что позволяет использовать методы DFT для решения задачи умножения матриц MDS и в задаче генерации кода Рида-Соломона.

Заветной целью является возможность использования быстрых преобразований Фурье для решения задачи умножения матриц в искусственных нейронных сетях, где возникает структура матрицы Вандермонда, в частности в SSM (state space models) при использовании свертки и матричной экспоненты.

Мы называем A матрицей Вандермонда общего вида с комплексными элементами x_j:

$$A = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{N-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_N & x_N^2 & \cdots & x_N^{N-1} \end{pmatrix},$$

где $x_j \in \mathbb{C}$.

Мы называем матрицу Вандермонда симметричной, если $A^T = A$. В этом случае $x_1 = 1$, а остальные элементы x_j представляют собой степени одного и того же комплексного числа λ. Этот частный случай матриц Вандермонда имеет следующую структуру:

$$\Lambda = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \lambda & \lambda^2 & \cdots & \lambda^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda^{N-1} & \lambda^{2(N-1)} & \cdots & \lambda^{(N-1)(N-1)} \end{pmatrix},$$

где $\lambda \in \mathbb{C}$.

Замечание. Для унитарной матрицы U, её эрмитово сопряжение U^* является также и обратным преобразованием ($U^{-1} = U^*$). Унитарные матрицы сохраняют норму вектора при преобразовании. Для приведения симметричной матрицы Вандермонда к унитарной матрице надо выполнить нормировку $1/\sqrt{N}$.

Известное свойство унитарности матриц дискретного преобразования Фурье,
приводит нас к следующему уравнению для матриц Вандермонда (1):

$$AA^* = A^*A = N \cdot E,$$

где $*$ обозначает эрмитово сопряжение $A^* = \overline{A}^{\mathsf{T}}$, а $E = \mathrm{diag}(1, \ldots, 1)$ — единичная матрица.

Теорема 1. Матрица Вандермонда (1) удовлетворяет сравнению (3) в том и только в том случае, если x_j для $j = 1, 2, \ldots, N$ являются N различными корнями уравнения $x^N = e^{iN\gamma}$, $\gamma \in \mathbb{R}$. При этом матрица (1) записывается в виде произведения симметричной матрицы Вандермонда (2) с $\lambda^N = 1$ и диагональной $A = \Delta \cdot \mathrm{diag}(1, e^{i\gamma}, e^{i2\gamma}, \ldots)$.

Лемма 1. В условиях теоремы 1 выполняется $|x_j| = 1$ для любого j.

Таким образом, независимо от размера матрицы Вандермонда доказательство теоремы 1 сводится в силу формул Виета к проверке импликации

$$\begin{cases} x_1 + \cdots + x_N = 0, \\ x_1^2 + \cdots + x_N^2 = 0, \\ \ldots \\ x_1^{N-1} + \cdots + x_N^{N-1} = 0 \end{cases} \quad \Longrightarrow \; x_j^N = a \; (\forall j \in [N]).$$

Остается заметить, что $|a| = 1$ в силу леммы 1 и что уравнение $x^N = a$ сводится к уравнению $\lambda^N = 1$ заменимой $z = e^{i\gamma}$, при $a = e^{iN\gamma}$. Доказательство обратного утверждения, т. е. $\lambda = e^{\frac{2\pi i}{N}} \Rightarrow (3)$, можно извлечь из монографии [1].

Следующая теорема показывает, что для симметричных матриц Вандермонда Λ вида (2) условие $AA^* = N \cdot E$ из теоремы 1 можно заменить условием $\Lambda^2 = N \cdot Q$, где Q — матрица перестановок, состоящая из нулей и единиц, например:

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

Теорема 2. Симметричная $N \times N$ матрица Вандермонда (2) является матрицей дискретного преобразования Фурье и удовлетворяет условию $\Lambda^N = 1$ тогда и только тогда, когда $\Lambda^2 = N \cdot Q$, где Q — симметричная матрица перестановок (5).

Алгоритм 1.4.1[2] Если $x \in \mathbb{C}^n$ и $n = 2^t$, то этот алгоритм вычисляет дискретное преобразование Фурье $y = F_n x$, где F_n - матрица фурье (симметричная матрица Вандермонда, составленная из корней степени n из единицы).

```
function y = fft(x, n)
    if n = 1
        y = x
    else
        m = n / 2
        y_r = fft(x(1:2:n), m)
        y_b = fft(x(2:2:n), m)
        w = exp(-2πi / n)
        d = [1, w, ..., w^(m-1)]^T
        z = d .* y_b
        y = [y_r + z
             y_r - z]
    end
end
```

- [2510.00563] Memory Determines Learning Direction: A Theory of Gradient-Based Optimization in State Space Models

1. Артисевич А. Е., Шабат А. Б. Три теоремы о матрицах Вандермонда // Владикавк. мат. журн.—2020.—Т. 22, вып. 1.—С. 5–12. DOI: 10.23671/VNC.2020.1.57532. ↩
2. Golub, Gene H. and Van Loan, Charles F., "Matrix Computations - 4th Edition" (2013), ISBN:978-1-4214-0794-4. DOI: 10.56021/9781421407944 ↩