关于矩阵的乘法运算及其变形满足交换律的相关证明

一. 本文的应用价值

在许多二阶、甚至高阶的递推式求值的时候，我们往往会用到矩阵快速幂，然而使用矩阵快速幂的基本条件即为：矩阵乘法满足结合律。所以说矩阵乘法满足结合律可谓是矩阵快速幂的基石。同理，其变形，如倍增 Floyd 使用的先相加再取 min 的“矩阵运算”满足结合律亦是倍增 Floyd 正确性证明的基础。所以本文所涉及证明的价值不言而喻。

二. 矩阵乘法满足交换律的证明[1]

a) 数学命题：$(AB)C = A(BC)$

b) 证明：

$$\because (\mathrm{AB})\mathrm{C} = \begin{pmatrix} \sum_k a_{k1}b_{1k} & \cdots & \sum_k a_{k1}b_{nk} \\ \vdots & \ddots & \vdots \\ \sum_k a_{km}b_{1k} & \cdots & \sum_k a_{km}b_{nk} \end{pmatrix} \mathrm{C} = \begin{pmatrix} \sum_{k'}\sum_k a_{k1}b_{k'k}c_{1k'} & \cdots & \sum_{k'}\sum_k a_{k1}b_{k'k}c_{nk'} \\ \vdots & \ddots & \vdots \\ \sum_{k'}\sum_k a_{km}b_{k'k}c_{1k'} & \cdots & \sum_{k'}\sum_k a_{km}b_{k'k}c_{nk'} \end{pmatrix}$$

$$\therefore \mathrm{A(BC)} = \mathrm{A}\begin{pmatrix} \sum_k b_{k1}c_{1k} & \cdots & \sum_k b_{k1}c_{nk} \\ \vdots & \ddots & \vdots \\ \sum_k b_{km}c_{1k} & \cdots & \sum_k b_{km}c_{nk} \end{pmatrix} = \begin{pmatrix} \sum_{k'}\sum_k a_{k'1}b_{kk'}c_{1k} & \cdots & \sum_{k'}\sum_k a_{k'1}b_{kk'}c_{nk} \\ \vdots & \ddots & \vdots \\ \sum_{k'}\sum_k a_{k'm}b_{kk'}c_{1k} & \cdots & \sum_{k'}\sum_k a_{k'm}b_{kk'}c_{nk} \end{pmatrix}$$

$$\therefore \mathrm{A(BC)} = \begin{pmatrix} \sum_{k'}\sum_k a_{k1}b_{k'k}c_{1k'} & \cdots & \sum_{k'}\sum_k a_{k1}b_{k'k}c_{nk'} \\ \vdots & \ddots & \vdots \\ \sum_{k'}\sum_k a_{km}b_{k'k}c_{1k'} & \cdots & \sum_{k'}\sum_k a_{km}b_{k'k}c_{nk'} \end{pmatrix} = (\mathrm{AB})\mathrm{C}$$

---

[1] 为了叙述方便，本文讨论的矩阵均为 nxn 的矩阵，且 $k, k' \in \{a \mid a \in Z \text{且} a \in [1, n]\}$

三. 倍增 Floyd 所使用的矩阵运算满足交换律的证明

a) 对于矩阵，定义新运算$\otimes$：

$$\mathrm{A}\otimes\mathrm{B}=\begin{pmatrix}\min(a_{k1}+b_{1k}) & \dots & \min(a_{k1}+b_{nk})\\ \vdots & \ddots & \vdots\\ \min(a_{km}+b_{1k}) & \cdots & \min(a_{km}+b_{nk})\end{pmatrix}$$

b) 引理：设 $\mathrm{a}\in\mathrm{A},\mathrm{b}\in\mathrm{B}$，有 $\min(\mathrm{a})+\min(\mathrm{b})=\min\{\mathrm{a}+\mathrm{b}\mid \mathrm{a}\in\mathrm{A},\mathrm{b}\in\mathrm{B}\}$

c) 数学命题：$(\mathrm{A}\otimes\mathrm{B})\otimes C=\mathrm{A}\otimes(\mathrm{B}\otimes C)$

d) 证明：

$$(A\otimes B)\otimes C=\begin{pmatrix}\min(a_{k1}+b_{1k}) & \dots & \min(a_{k1}+b_{nk})\\ \vdots & \ddots & \vdots\\ \min(a_{km}+b_{1k}) & \cdots & \min(a_{km}+b_{nk})\end{pmatrix}\otimes C=\begin{pmatrix}\min(\min(a_{k1}+b_{k'k})+c_{1k'}) & \dots & \min(\min(a_{k1}+b_{k'k})+c_{nk'})\\ \vdots & \ddots & \vdots\\ \min(\min(a_{km}+b_{k'k})+c_{1k'}) & \cdots & \min(\min(a_{km}+b_{k'k})+c_{nk'})\end{pmatrix}$$

由引理可得：$(A\otimes B)\otimes C=\begin{pmatrix}\min(a_{k1}+b_{k'k}+c_{1k'}) & \dots & \min(a_{k1}+b_{k'k}+c_{nk'})\\ \vdots & \ddots & \vdots\\ \min(a_{km}+b_{k'k}+c_{1k'}) & \cdots & \min(a_{km}+b_{k'k}+c_{nk'})\end{pmatrix}$

同理可得：$A\otimes(B\otimes C)=\begin{pmatrix}\min(a_{k'1}+b_{kk'}+c_{1k}) & \dots & \min(a_{k'1}+b_{kk'}+c_{nk})\\ \vdots & \ddots & \vdots\\ \min(a_{k'm}+b_{kk'}+c_{1k}) & \cdots & \min(a_{k'm}+b_{kk'}+c_{nk})\end{pmatrix}$

$\therefore (A\otimes B)\otimes C=A\otimes(B\otimes C)$

四. 相关推广

a) 一种猜想：

i. 定义一种对于矩阵的新运算$\odot$：

$$\mathrm{A}\odot\mathrm{B}=\begin{pmatrix}\min(a_{k1}\wedge b_{1k}) & \dots & \min(a_{k1}\wedge b_{nk})\\ \vdots & \ddots & \vdots\\ \min(a_{km}\wedge b_{1k}) & \cdots & \min(a_{km}\wedge b_{nk})\end{pmatrix}$$

ii. 猜想：该种新运算满足结合律

iii. 证明：

不难发现，这个命题和上述 Floyd 相关命题很相似。但因为亦或不满足 三.b) 中提到的引理，故无法将 $\begin{pmatrix} \min(\min(a_{k1}+b_{k'k})+c_{1k'}) & \cdots & \min(\min(a_{k1}+b_{k'k})+c_{nk'}) \\ \vdots & \ddots & \vdots \\ \min(\min(a_{km}+b_{k'k})+c_{1k'}) & \cdots & \min(\min(a_{km}+b_{k'k})+c_{nk'}) \end{pmatrix}$ 展开。进而无法证明该猜想[2]。

b) 推广：

i. 对于包含取 min()或取 max()的新运算⊕，不难发现能否将形如 min(min(a⊕b) ⊕c)展开为形如 min(a⊕b⊕c)的式子为关键。

ii. 对于更玄妙的定义，一般来说都可以使用这种暴力运算进而写出表达式的方式进行简单证明。

五. References

a) 杨永祎学长提供的相关证明

b) Wikipedia–Matrix_Multiplication

六. 致谢

感谢杨永祎学长提供了本文的所有证明[3]

感谢张若琦学长给予的大力帮助

[2] 事实上，该猜想可以被证明是错误的。但因为篇幅的限制，所以不给出严格的证明

[3] 其手稿可以再这里找到：https://zyqn.tech/wp-content/uploads/2016/10/simple_provement_to_matrix_pow.jpg