矩阵乘法算法笔记

2012-06-11 12:17:49

（一）双线性复杂度

考虑具有如下一般形式的问题：输入变量为域 $\mathbb{F}$ 中的元素 $X_1, \ldots, X_m$，设计算法输出 $f_1(X_1, \ldots, X_m), \ldots, f_n(X_1, \ldots, X_m)$，其中 $f_1, \ldots f_n$ 为 $\mathbb{F}$ 上的多项式。不加说明的话默认 $\mathbb{F} = \mathbb{C}$。

举例：

1. (矩阵乘法)

$$f_{i,k}(A, B) = \sum_{j=1}^{n} A_{ij} B_{jk}, \qquad 1 \leq i, k \leq n.$$

2. (离散 Fourier 变换)

$$f_i(X) = \sum_{j=1}^{n} \omega^{ij} X_j, \qquad i = 1, \ldots, n$$

其中 ω 为 n 次单位根 (n-th root of unity)。

3. (一元多项式乘法)

$$f_i(X, Y) = \sum_{j,k:j+k=i} X_j Y_k, \qquad i = 0, \ldots, n-1.$$

这里“算法”指算术线路 (arithmetic circuit)，即采用 $\mathbb{F}$ 上的二元运算加减乘除为运算门的线路（当然算法和线路是有区别的，但这里先不作区分）。一般用运算门的数量来衡量线路大小或者说算法的复杂度。有时也会将加减和数乘操作忽略不计，具体视上下文而定。

显然减法可以用加法以及数乘代替，下面的定理说明在某种意义上也可以忽略掉除法：

定理 1.1 ([Str73])：
计算 d 阶多项式的大小为 s 的 $(+,\times,/)$-线路可用大小为 $sd^{O(1)}$ 的 $(+,\times)$-线路代替。

证明：原线路的每一个运算门都计算一个有理函数 f/g。在构造的新线路中将其转化为两个运算门，分别计算 f 和 g。这一步是自底向上地作的。
具体地说，考虑一个运算门，设其操作数为 a/b 和 c/d。在新线路中 a,b,c,d 已经被计算。若该运算门为加法，则输出为 $(ad+bc)/bd$。在新线路中计算 $ad+bc$ 和 bd，需要4个运算；若该运算门为乘法，则输出为 ac/bd。在新线路中计算 ac 和 bd，需要2个运算；若该运算门为除法，则输出为 ad/bc。在新线路中计算 ad 和 bc，需要2个运算。
这样在新线路中只在顶端输出的位置有除法运算 $f=g/h$，而线路大小增加至多常数因子。下面把这些除法也去掉：
取 $\alpha_1,\ldots,\alpha_n\in\mathbb{F}^n$ 使得 $h(\alpha_1,\ldots,\alpha_n)=c\neq 0$。令
$g'(X_1,X_2,\ldots,X_n)=(c^{-1})\cdot g(X_1+\alpha_1,\ldots,X_n+\alpha_n)$ 以及
$h'(X_1,X_2,\ldots,X_n)=(c^{-1})\cdot h(X_1+\alpha_1,\ldots,X_n+\alpha_n)$，则 $h'(0,\ldots,0)=1$（常数项为 1）。并且 $f(X_1,\ldots,X_n)=(g/h)(X_1,\ldots,X_n)=(g'/h')(Y_1,\ldots,Y_n)$，其中 $Y_i=X_i+\alpha_i$。这里 g'/h'关于 $X_1,\ldots X_n$ 仍为 d 阶多项式。于是下面转而考虑 g'/h'。
注意到 $1/X$ 为形式幂级数 (formal power series) $1+X+X^2+\ldots\in\mathbb{F}[[X]]$。于是

$$g'/h'=g'/(1-(1-h'))=g'(1+(1-h')+(1-h')^2+\cdots).$$

注意到 $1-h'$ 常数项为零。于是 $(1-h')^i$ 最低的非零项为 i 阶。而 g'/h' 是 d 阶多项式，所以可以把上式中 $i>d$ 的项扔掉。所得线路大小为 $sd^{O(1)}$，证毕。

更精细的分析得出新线路大小至多为 $\binom{d}{2}s$。对于矩阵乘法（$d=2$）这说明不使用除法没有任何损失。

矩阵乘法中 $d=2$，每个输出都可以通过形如 $\sum(\sum\times\sum)$ 的线路计算，称为二次线路 (quadratic circuit)。下面考察不同的计算方式是否有助于减少线路复杂度。例如是否有可能在计算过程中先算出若干高阶的多项式，最后高阶项互相抵消，并减少运算数量。下面的定理说明考虑仅乘法时，二次线路总是最优的。记 $L(f_1,\ldots,f_n)$ 为计算多项式 $f_1,\ldots,f_n$ 的乘法复杂度，则我们有：

定理 1.2 ([Str73])：
对于二阶多项式 $f_1,\ldots,f_n$，成立

$$L(f_1,\ldots,f_n)=\min\left\{m:\begin{array}{l}\exists\text{ 线性型 (linear form) } g_1,\ldots,g_m,h_1,\ldots,h_m,\\ \text{使得 } f_1,\ldots,f_n\in\operatorname{span}\{g_1h_1,\ldots,g_mh_m\}\end{array}\right\}.$$

证明：$\leq$ 是显然的。为证 $\geq$，考虑计算 $f_1,\dots,f_k$ 且乘法复杂度为 $L(f_1,\dots,f_k)$ 的线路。令 $s_1,\dots,s_m$ 为该线路中拓扑排序下的所有乘法门，即 s_i 只依赖于 $s_1,\dots,s_{i-1}$ 的运算结果。将 s_i 的操作数记作 a_i 和 b_i。

对于一个多项式 f，用 $f^{(k)}$ 表示其 k-阶齐次部分 (homogeneous part of degree k)。首先证明如下结论：

$$s_i^{(2)} \in \operatorname{span}\left\{a_1^{(1)}b_1^{(1)}, a_2^{(1)}b_2^{(1)}, \dots, a_i^{(1)}b_i^{(1)}\right\}.$$

可通过对 i 作归纳证明。有 $s_i^{(2)} = a_i^{(0)}b_i^{(2)} + a_i^{(1)}b_i^{(1)} + a_i^{(2)}b_i^{(0)}$。当 $i=1$ 时 $a_i^{(2)} = b_i^{(2)} = 0$，结论成立。对 $i>1$，注意到 a_i 和 b_i 可写作三项之和：

“常数 + $X_1,\dots,X_n$ 的线性组合 + $s_1,\dots,s_{i-1}$ 的线性组合”。而 $a_i^{(2)}$ 和 $b_i^{(2)}$ 恰为第三项的 2-阶齐次部分，也即 $s_1^{(2)},\dots,s_{i-1}^{(2)}$ 的线性组合。于是

$$\begin{aligned} s_i^{(2)} &= a_i^{(0)}b_i^{(2)} + a_i^{(1)}b_i^{(1)} + a_i^{(2)}b_i^{(0)} = \text{常数} \times s_1^{(2)},\dots,s_{i-1}^{(2)} \text{ 的线性组合} \\ &\quad + s_1^{(2)},\dots,s_{i-1}^{(2)} \text{ 的线性组合} \times \text{常数} + a_i^{(1)}b_i^{(1)} \\ &\in \operatorname{span}\left\{a_1^{(1)}b_1^{(1)}, a_2^{(1)}b_2^{(1)}, \dots, a_i^{(1)}b_i^{(1)}\right\} \end{aligned}$$

最后一步由归纳假设得到。这样就证明了上述结论。这说明线路的每个输出 f_i 都属于 $\operatorname{span}\left\{a_1^{(1)}b_1^{(1)}, a_2^{(1)}b_2^{(1)}, \dots, a_m^{(1)}b_m^{(1)}\right\}$，其中 $a_1^{(1)},\dots,a_m^{(1)},b_1^{(1)},\dots,b_m^{(1)}$ 为线性型。证毕。

上述定理对于更高阶的多项式不成立。但对于矩阵乘法我们只需要二阶的情形。更进一步，注意到矩阵乘法的输出 $f_{i,k}(A,B) = \sum_{j=1}^{n} A_{ij}B_{jk}$ 是关于 $A=(A_{ij})$ 和 $B=(B_{ij})$ 的双线性型 (bilinear form)。这类问题称作双线性问题 (bilinear problem)。故我们考虑一类特殊的二次线路：设输入变量为 $X=(X_i)$ 和 $Y=(Y_i)$，线路的每个输出通过 $\sum(\sum\times\sum)$ 的方式计算，并且乘法的两个操作数分别是关于 X 和 Y 的线性型。这样的线路称为双线性线路 (bilinear circuit)。有如下结论：

定理 1.3：
设一个双线性问题存在乘法数量为 m 的二次线路，则该问题亦存在乘法数量为 $2m$ 的双线性线路。

证明：考虑乘法数量为 m 的二次线路。设问题关于输入变量 $X=(X_i)$ 和 $Y=(Y_i)$ 是双线性的。由定理 1.2，线路的每个输出 $f_i \in \operatorname{span}\{g_1(X,Y)h_1(X,Y),\dots,g_m(X,Y)h_m(X,Y)\}$，其中 $g_1,\dots,g_m,h_1,\dots,h_m$ 是线性型。 故成立

$$\begin{aligned} &g_j(X,Y)h_j(X,Y) = (g_j(X,0)+g_j(0,Y))(h_j(X,0)+h_j(0,Y)) \\ &= g_j(X,0)h_j(X,0) + g_j(X,0)h_j(0,Y) + g_j(0,Y)h_j(X,0) + g_j(0,Y)h_j(0,Y). \end{aligned}$$

又由 f_i 的双线性知其不含 X 或 Y的二次项。所以有

$$f_i \in \operatorname{span}\{\, g_1(X,0)h_1(0,Y), g_1(0,Y)h_1(X,0)\ldots, \\ g_m(X,0)h_m(0,Y), g_m(0,Y)h_m(X,0)\}.$$

再由定理 1.2 可知存在乘法数量为 $2m$ 的双线性线路。证毕。

上述几个定理说明双线性问题（包括矩阵乘法）的算法复杂度可以由该问题所需的双线性线路的乘法数量来衡量，称为双线性复杂度 (bilinear complexity)。

（二）张量秩

设某个关于 $X=(X_1,\ldots,X_n)$ 和 $Y=(Y_1,\ldots,Y_m)$ 的双线性问题具有 p 个输出 $f_1,\ldots,f_p$。可用如下三种形式描述该问题：

1.（分别描述 p 个输出）$f_k(X,Y)=\sum_{ij}t_{ijk}X_iY_j$，$k=1,\ldots,p$，$t_{ijk}\in\mathbb{F}$；

2.（多项式描述）引入形式变量 $Z_1,\ldots,Z_p$，然后用多项式
$g(X,Y,Z)=\sum_k f_k(X,Y)Z_k=\sum_{ijk}t_{ijk}X_iY_jZ_k$ 描述该问题；

3.（张量描述）用张量 $T\in\mathbb{F}^n\otimes\mathbb{F}^m\otimes\mathbb{F}^p$ 描述该问题，其中 $T[i,j,k]$ 为上面 $g(X,Y,Z)$ 中 $X_iY_jZ_k$ 的系数，即 t_{ijk}。

定义一个（三阶）张量 $T\in\mathbb{F}^n\otimes\mathbb{F}^m\otimes\mathbb{F}^p$ 的张量秩 (tensor rank) 为

$$R(T)=\min\left\{ r : \begin{array}{c} \exists\, a_i\in\mathbb{F}^n, b_i\in\mathbb{F}^m, c_i\in\mathbb{F}^p,\ i=1,\ldots,r, \\ \text{使得 } T=\sum_{i=1}^{r} a_i\otimes b_i\otimes c_i \end{array} \right\}$$

其中 $a_i\otimes b_i\otimes c_i$ 称为纯张量 (pure tensor)。

定理 2.1 ([Str73])：
设张量 $T\in\mathbb{F}^n\otimes\mathbb{F}^m\otimes\mathbb{F}^p$ 描述一个双线性问题，并设该问题的双线性复杂度为 s，则 $R(T)=s$。

证明：($R(T)\le s$) 考虑乘法数量为 s 的双线性线路，设 $a_i(X)$ 和 $b_i(Y)$ 为其第 i 个乘法门的操作数（a_i 和 b_i 为线性型）。则每个输出 $f_k(X,Y)=\sum_{ij}t_{ijk}X_iY_j$ 都可写作
$a_1(X)b_1(Y),\ldots,a_s(X)b_s(Y)$ 的线性组合。设 $f_k(X,Y)=\sum_{i=1}^{s}\alpha_{ki}a_i(X)b_i(Y)$，

$k=1,\dots,p$，$\alpha_{ki}\in\mathbb{F}$。引入形式变量 $Z_1,\dots,Z_p$ 并定义线性型 $c_i(Z)=\sum_{k=1}^{p}\alpha_{ki}(Z_k)$，$i=1,\dots,s$。则

$$\begin{aligned}\sum_{i=1}^{s}a_i(X)b_i(Y)c_i(Z)&=\sum_{k=1}^{p}\sum_{i=1}^{s}\alpha_{ki}a_i(X)b_i(Y)Z_k\\&=\sum_{k=1}^{p}f_k(X,Y)Z_k\\&=\sum_{ijk}t_{ijk}X_iY_jZ_k.\end{aligned}$$

若将 a_i,b_i,c_i 分别看作 $\mathbb{F}^n,\mathbb{F}^m,\mathbb{F}^p$ 中的向量（a_i 的第 j 个元素为 $a_i(X)$ 中 X_j 的系数，对 b_i 和 c_i 同理），则有 $\sum_{i=1}^{s}a_i\otimes b_i\otimes c_i=(t_{ijk})=T$。

($R(T)\geq s$) 设 $T=\sum_{i=1}^{s}a_i\otimes b_i\otimes c_i$。引入形式变量 $Z_1,\dots,Z_p$。将 a_i，b_i 和 c_i 看作线性型。所求问题的多项式描述为 $\sum_{ijk}t_{ijk}X_iY_jZ_k=\sum_{i=1}^{s}a_i(X)b_i(Y)c_i(Z)$。设计双线性线路如下：对 $i=1,\dots,s$，令第 i 个乘法计算 $a_i(X)b_i(Y)$。并且对 $k=1,\dots,p$ 令第 k 个输出 $f_k(X,Y)=\sum_{i=1}^{s}\alpha_{ki}a_i(X)b_i(Y)$，其中 α_{ki} 满足 $c_i(Z)=\sum_{k=1}^{s}\alpha_{ki}Z_k$。这样的线路使用了 s 个乘法门，并且其计算的问题具有所要求的多项式表述

$$\sum_{k=1}^{p}f_k(X,Y)Z_k=\sum_{k=1}^{p}\sum_{i=1}^{s}\alpha_{ki}a_i(X)b_i(Y)Z_k=\sum_{i=1}^{s}a_i(X)b_i(Y)c_i(Z).$$

证毕。

定理 2.1 说明双线性问题的复杂度可以用其对应的张量秩刻划。对于 $n\times m$ 的矩阵和 $m\times p$ 的矩阵相乘的矩阵乘法问题，其对应的张量记作 $\langle n,m,p\rangle\in\mathbb{F}^{nm}\otimes\mathbb{F}^{mp}\otimes\mathbb{F}^{np}$。这样的张量的张量秩也称作矩阵乘法秩 (rank of matrix multiplication)。

其对应的多项式表述为：

$$\sum_{i=1}^{n}\sum_{k=1}^{p}\left(\sum_{j=1}^{m}X_{ij}Y_{jk}\right)Z_{ik}=\sum_{\substack{1\leq i\leq n\\1\leq j\leq m\\1\leq k\leq p}}X_{ij}Y_{jk}Z_{ik}.$$

注意到上式具有 $\mathbb{S}_3$-对称性。由此可得对 $\{n,m,p\}$ 的置换 π，有

$$\langle n,m,p\rangle=\langle\pi(n),\pi(m),\pi(p)\rangle.$$

下面考虑张量积 $\langle n,m,p\rangle \otimes \langle n',m',p'\rangle$。其对应的多项式表述为：

$$\sum_{(i,i')(j,j')(k,k')} X_{(i,i')(j,j')} Y_{(j,j')(k,k')} Z_{(i,i')(k,k')}$$

于是 $\langle n,m,p\rangle \otimes \langle n',m',p'\rangle = \langle nn',mm',pp'\rangle$。

定义 $\omega = \inf_n \{\log_n R(\langle n,n,n\rangle)\}$，称为矩阵乘法指数 (matrix multiplication exponent)。如下定理说明 ω 确实刻划了（方块）矩阵乘法的时间复杂度。

定理 2.2：
对任意常数 $\epsilon > 0$，计算两个 $n \times n$ 矩阵相乘的时间复杂度为 $O(n^{\omega+\epsilon})$。

证明：由定义，存在常数 $n_0 = O(1)$ 使得 $R(\langle n_0,n_0,n_0\rangle) \le n_0^{\omega+\epsilon}$。为计算两个 $n \times n$ 矩阵相乘，采用如下递归算法：
将两个 $n \times n$ 矩阵划分成 $n_0 \times n_0$ 块，每个子矩阵的大小为 $(n/n_0) \times (n/n_0)$。由定理 2.1，$n_0 \times n_0$ 方块矩阵相乘可由至多使用 $n_0^{\omega+\epsilon}$ 次乘法的线路计算。利用该线路计算两个 $n \times n$ 矩阵也即 $n_0 \times n_0$ 分块矩阵的乘法。但对于子矩阵相乘，递归地使用 $(n/n_0) \times (n/n_0)$ 矩阵相乘的算法。对于子矩阵相加则使用朴素的 $O(n^2)$-时间算法。该算法运行了至多 $n_0^{\omega+\epsilon}$ 次子矩阵相乘和 $O(1)$ 次子矩阵相加。设该算法的时间复杂度为 $T(n)$，则有：

$$T(n) \le (n_0)^{\omega+\epsilon} T(n/n_0) + O(n^2).$$

解得 $T(n) = O(n^{\omega+\epsilon})$。证毕。

同时有如下结论：

定理 2.3：
若 $R(\langle n,m,p\rangle) \le r$，则 $\omega \le 3\log_{nmp} r$。

证明：注意到张量秩满足 $R(T \otimes T') \le R(T)R(T')$。于是

$$\begin{aligned} R(\langle nmp,nmp,nmp\rangle) &= R(\langle n,m,p\rangle \otimes \langle m,p,n\rangle \otimes \langle p,n,m\rangle) \\ &\le R(\langle n,m,p\rangle) R(\langle m,p,n\rangle) R(\langle p,n,m\rangle) \\ &= R(\langle n,m,p\rangle)^3 \\ &\le r^3. \end{aligned}$$

故 $\omega \le \log_{nmp}(r^3) = 3\log_{nmp} r$。证毕。

经典的 Strassen 算法利用了如下结论：

定理 2.4 ([Str69])：
$R(\langle 2,2,2\rangle) \le 7.$

证明：把 $\langle 2,2,2\rangle$ 根据第三维分量划分为下面四个二阶张量（矩阵）：

$$\begin{array}{c} \\ X_{11} \\ X_{21} \\ X_{12} \\ X_{22} \\ \\ (1,1) \end{array}\!\!\begin{array}{c} \begin{array}{cccc} Y_{11} & Y_{12} & Y_{21} & Y_{22} \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\ X_{11}Y_{11} + X_{12}Y_{21} \end{array}\!\!\begin{array}{c} \begin{array}{cccc} Y_{11} & Y_{12} & Y_{21} & Y_{22} \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\ X_{11}Y_{12} + X_{12}Y_{22} \end{array}\!\!\begin{array}{c} \begin{array}{cccc} Y_{11} & Y_{12} & Y_{21} & Y_{22} \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ X_{21}Y_{11} + X_{22}Y_{21} \end{array}\!\!\begin{array}{c} \begin{array}{cccc} Y_{11} & Y_{12} & Y_{21} & Y_{22} \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ X_{21}Y_{12} + X_{22}Y_{22} \end{array}$$
$$\begin{array}{cc} (1,2) & (2,1) \end{array} \qquad (2,2)$$

注意到有8个非零元素，因此可以用8个三阶纯张量生成。这对应于矩阵乘法的朴素算法。
但事实上7个三阶纯张量就足够了。考虑如下的二阶纯张量：

$$\begin{array}{cccc} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \\ T_1 & T_2 & T_3 & T_4 \end{array}$$
$$\begin{array}{ccc} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} & \begin{pmatrix} -1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\ T_5 & T_6 & T_7 \end{array}$$

则前述四个二阶张量可分别表示为 $T_1 - T_2 + T_4 + T_6$，$T_5 + T_6$，$T_2 + T_3$，以及
$T_1 + T_3 - T_5 + T_7$。所以

$$\begin{aligned} \langle 2,2,2\rangle = {} & T_1 \otimes (1,0,0,1) + T_2 \otimes (-1,0,1,0) + T_3 \otimes (0,0,1,1) + T_4 \otimes (1,0,0,0) \\ & + T_5 \otimes (0,1,0,-1) + T_6 \otimes (1,1,0,0) + T_7 \otimes (0,0,0,1) \end{aligned}$$

其中每一项都是一个三阶纯张量。证毕。

推论 2.1 (Strassen 算法 [Str69])：

$\omega \le \log_2 7 = 2.807\ldots$

$R(\langle n,m,p\rangle)$ 的计算非常困难。一般的三阶张量的张量秩计算已经证明是 $\mathbf{NP}$-难的 [Hås90]。下面是已知的较小的 n,m,p 对应的矩阵乘法秩范围。

$$\begin{aligned} R(\langle 2,2,2\rangle) &= 7; \\ R(\langle 2,2,3\rangle) &= 11; \\ 14 \le R(\langle 2,3,3\rangle) &\le 15; \\ 19 \le R(\langle 3,3,3\rangle) &\le 23. \end{aligned}$$

（三）边界秩

一个张量的边界秩 (border rank) 可以看作其“近似张量”的张量秩 [BLR80]。稍后会给出形式定义。
考察如下的问题，设一列张量 $T(\epsilon)$ 以 T 为极限：$\lim_{\epsilon\to 0} T(\epsilon) = T$。是否可能对任意 $\epsilon > 0$，都有 $R(T(\epsilon)) < R(T)$？对于矩阵秩（等同于二阶张量的张量秩）来说这是不可能的，这是由特征多项式的连续性得到的（若 $f(0) \neq 0$，则 f 在 0 的充分小的邻域上均不为零）。然而对于三阶及三阶以上的张量秩来说这一情形有可能出现。

举例：考虑如下的 $2\times 2\times 2$ 张量：按第三维划分为两个二阶张量如下：

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

对应的多项式为 $p(X,Y,Z) = X_0Y_0Z_0 + X_1Y_0Z_1 + X_0Y_1Z_0$。
显然有 $R(T) \le 3$。另一方面可证明 $R(T) \ge 3$。等价地，X_0Y_0 和 $X_1Y_0 + X_0Y_1$ 至少需要三个线性型之积 $g_1(X)h_1(Y), g_2(X)h_2(Y), g_3(X)h_3(Y)$ 生成。这可通过替换法 (substitution method) 证明 [Pan66]。首先至少有一个线性型 g_i 是关于 X_1 的函数，不妨设 $g_1(X) = \alpha X_1 + \beta X_0$，其中 $\alpha \neq 0$。令 $X_1 = -\beta X_0/\alpha$ 使得 $g_1(X)h_1(Y) = 0$。此时需计算 X_0Y_0 和 $-\beta/\alpha X_0Y_0 + X_0Y_1$。可知除 h_1 以外的某个 h_i 是关于 Y_1 的函数。不妨设 $h_2(Y) = aY_0 + bY_1$，其中 $b \neq 0$。进一步令 $Y_1 = -aY_0/b$ 使得 $g_2(X)h_2(Y) = 0$。此时仍需计算 $X_0Y_0Z_0$。故仍需要第三个线性型之积 $g_3(X)h_3(Y)$。 故 $R(T) \ge 3$。

另一方面，考虑 $2\times 2\times 2$ 张量 $T(\epsilon)$，$\epsilon \neq 0$。其两个二阶张量如下：

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & \epsilon \end{pmatrix}$$

它们均可由下面两个二阶纯张量生成：

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1/\epsilon & 1 \\ 1 & \epsilon \end{pmatrix}$$

由此可得 $T(\epsilon) = (1,0) \otimes (1,0) \otimes (1,-1/\epsilon) + (1/\epsilon,1) \otimes (1,\epsilon) \otimes (0,1)$。故 $R(T(\epsilon)) = 2$。

另一个例子是 $\langle 2,2,3 \rangle$。首先考虑所谓部分矩阵乘法 (partial matrix multiplication)：考虑 2×2 方块矩阵乘法，但只要求 $(1,1),(1,2),(2,1)$ 三个元素的结果。这意味着计算由下面三个二阶张量构成的三阶张量 $T \in \mathbb{F}^{2\times 2} \times \mathbb{F}^{2\times 2} \times \mathbb{F}^3$：

$$\begin{array}{c} \\ X_{11} \\ X_{21} \\ X_{12} \\ X_{22} \\ \\ (1,1) \end{array} \begin{array}{c} Y_{11}Y_{12}Y_{21}Y_{22} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\ X_{11}Y_{11} + X_{12}Y_{21} \end{array} \qquad \begin{array}{c} Y_{11}Y_{12}Y_{21}Y_{22} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\ X_{11}Y_{12} + X_{12}Y_{22} \\ (1,2) \end{array} \qquad \begin{array}{c} Y_{11}Y_{12}Y_{21}Y_{22} \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ X_{21}Y_{11} + X_{22}Y_{21} \\ (2,1) \end{array}$$

平凡地有 $R(T) \leq 6$。利用替换法可得 $R(T) = 6$。然而利用5个三阶纯张量便可生成 T的近似。考虑下面5个二阶纯张量：

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & \epsilon & 0 \end{pmatrix} \quad T_1(\epsilon) \qquad \begin{pmatrix} 1 & \epsilon & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad T_2(\epsilon) \qquad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & \epsilon \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad T_3(\epsilon)$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ \epsilon & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad T_4(\epsilon) \qquad \begin{pmatrix} 0 & 0 & 0 & 0 \\ \epsilon & 0 & 0 & \epsilon^2 \\ 1 & 0 & 0 & \epsilon \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad T_5(\epsilon)$$

利用它们可以得到 T的近似：

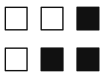
$$\begin{pmatrix} 1 & \epsilon & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & \epsilon & 0 \end{pmatrix} \quad T_1(\epsilon) + T_2(\epsilon) \qquad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \epsilon \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad (1/\epsilon)(T_2(\epsilon) - T_4(\epsilon) + T_5(\epsilon)) \qquad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & \epsilon \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (1/\epsilon)(T_1(\epsilon) - T_3(\epsilon) + T_5(\epsilon))$$

即令

$$\begin{aligned} T(\epsilon) = T_1 \otimes (1,0,1/\epsilon) + T_2 \otimes (1,1/\epsilon,0) + T_3 \otimes (0,0,-1/\epsilon) \\ + T_4 \otimes (0,-1/\epsilon,0) + T_5 \otimes (0,1/\epsilon,1/\epsilon) \end{aligned}$$

则 $R(T(\epsilon)) = 5$ 且 $\lim_{\epsilon \to 0} T(\epsilon) = T$。

注意到对于 2×2 矩阵和 2×3 矩阵的乘法，所得的 2×3 矩阵可划分成两个L型：



每个L型是 2×2 方块矩阵相乘所得的部分矩阵。由此立即得到存在张量列 $T(\epsilon) \to \langle 2,2,3 \rangle$ 且 $R(T(\epsilon)) \leq 2 \times 5 = 10 < 11 = R(\langle 2,2,3 \rangle)$。

若成立 $R(T(\langle 2,2,3 \rangle)) \leq 10$， 则由定理 2.3 可得 $\omega \leq 3 \log_{12} 10 = 2.779\ldots$，优于 Strassen 算法 [Str69]。可惜这并不成立。然而后面将会看到 $R(T(\epsilon)) = 10$ 这一结果已经足以推出 $\omega \leq 2.779\ldots$。

下面先给出边界秩的形式定义：

对于张量 T和任意非负整数 h，定义

$$R_h(T) = \min \Big\{ R(\epsilon^h T + \epsilon^{h+1} T') : T' \text{ 是环 } \mathbb{F}[\epsilon] \text{ 上的张量} \Big\}.$$

并定义 T的边界秩 $\underline{R}(T)$ 为

$$\underline{R}(T) = \min_h R_h(T).$$

上面的例子意味着：

定理 3.1 ([BCRL79])：
$\underline{R}(\langle 2,2,3 \rangle) \leq 10.$

类似于张量秩，容易验证边界秩满足性质 $\underline{R}(T \otimes T') \leq \underline{R}(T)\underline{R}(T')$。这是因为 $R_{h+h'}(T \otimes T') \leq R_h(T) R_{h'}(T')$。此外由 $\langle n,m,p \rangle$ 的 $\mathbb{S}_3$-对称性得到对于 $\{n,m,p\}$ 的置换 π，成立 $R_h\langle n,m,p \rangle = R_h\langle \pi(n), \pi(m), \pi(p) \rangle$ 以及 $\underline{R}\langle n,m,p \rangle = \underline{R}\langle \pi(n), \pi(m), \pi(p) \rangle$。

有如下引理：

引理 3.1：
对于任意非负整数 h，成立 $R(T) \leq \binom{h+2}{2} R_h(T)$.

证明：设 $R_h(T) = r$。则存在 $\mathbb{F}[\epsilon]$ 上的张量 T' 使得

$$\epsilon^h T + \epsilon^{h+1} T' = \sum_{i=1}^{r} a_i \otimes b_i \otimes c_i$$

其中 a_i, b_i, c_i 是 $\mathbb{F}[\epsilon]$ 上的向量。设

$$a_i = \sum_{j=0}^{\infty} a_{i,j} \epsilon^j, \qquad b_i = \sum_{j=0}^{\infty} b_{i,j} \epsilon^j, \qquad c_i = \sum_{j=0}^{\infty} c_{i,j} \epsilon^j$$

其中 $a_{i,j}, b_{i,j}, c_{i,j}$ 是 $\mathbb{F}$ 上的向量。T由 $\sum_{i=1}^{r} a_i \otimes b_i \otimes c_i$ 中 ϵ 的 h 次项系数给出，即

$$T = \sum_{j_1+j_2+j_3=h} \sum_{i=1}^{r} a_{i,j_1} \otimes b_{i,j_2} \otimes c_{i,j_3}$$

故 T是 $\binom{h+2}{2} r = \binom{h+2}{2} R_h(T)$ 个纯张量之和。证毕。

对边界秩有类似于定理 2.3的结论：

定理 3.2：
若 $\underline{R}(\langle n, m, p \rangle) \leq r$，则 $\omega \leq 3 \log_{nmp} r$。

证明：若 $\underline{R}(\langle n, m, p \rangle) \leq r$，则存在常数 h 使得 $R_h(\langle n, m, p \rangle) \leq r$。于是

$$\begin{aligned} R_{3h}(\langle nmp, nmp, nmp \rangle) &= R_{3h}(\langle n, m, p \rangle \otimes \langle m, p, n \rangle \otimes \langle p, n, m \rangle) \\ &\leq R_h(\langle n, m, p \rangle) R_h(\langle m, p, n \rangle) R_h(\langle p, n, m \rangle) \\ &= R_h(\langle n, m, p \rangle)^3 \\ &\leq r^3. \end{aligned}$$

进而对于任意正整数 i，有 $R_{3hi}\left(\left\langle (nmp)^i, (nmp)^i, (nmp)^i \right\rangle\right) \leq r^{3i}$。由引理 3.1，成立 $R\left(\left\langle (nmp)^i, (nmp)^i, (nmp)^i \right\rangle\right) \leq \binom{3hi+2}{2} r^{3i}$。于是有

$\omega \leq \lim_{i\to\infty} \log_{(nmp)^i} \left(\binom{3hi+2}{2} r^{3i} \right) = 3\log_{nmp} r$。证毕。

结合定理 3.1 和 定理 3.2 可得：

推论 3.1 ([BCRL79])：
$\omega \leq 3\log_{12} 10 = 2.779\ldots$

（四）张量的直和

对于张量 $T \in \mathbb{F}^n \otimes \mathbb{F}^m \otimes \mathbb{F}^p$ 和 $T \in \mathbb{F}^{n'} \otimes \mathbb{F}^{m'} \otimes \mathbb{F}^{p'}$，定义其直和 (direct sum) $T \oplus T' \in \mathbb{F}^{n+n'} \otimes \mathbb{F}^{m+m'} \otimes \mathbb{F}^{p+p'}$ 如下：

$$(T \oplus T')[i,j,k] = \begin{cases} T[i,j,k] & i \leq n, j \leq m, k \leq p \\ T[i-n, j-m, k-p] & i > n, j > m, k > p \\ 0 & \text{否则.} \end{cases}$$

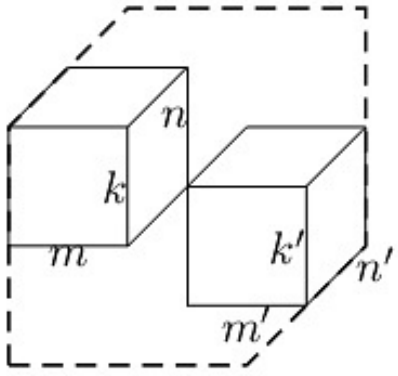


Figure 4.3: Sum of two tensors

张量的直和。图示来自 [Blä09]

易证这样定义的直和满足分配律：

$$(T\oplus T')\otimes T'' = (T\otimes T'')\oplus(T'\otimes T'')$$
$$T''\otimes(T\oplus T') = (T''\otimes T)\oplus(T''\otimes T').$$

设 T和 T' 分别描述两个矩阵乘法，则直观上 $T\oplus T'$ 并行地描述了这两个矩阵乘法。易证 $R(T\oplus T')\le R(T)+R(T')$ 和 $\underline{R}(T\oplus T')\le \underline{R}(T)+\underline{R}(T')$。下面的猜想若成立，则意味着要同时求解两个矩阵乘法，最优（即双线性复杂度最小）的方法乃是独立地求解它们。

猜想 4.1 (加性猜想 (additivity conjecture) [Str73])：
$R(T\oplus T') = R(T)+R(T')$.

后面将看到类似的命题对边界秩不成立，换言之存在比独立地求解每个矩阵乘法更优的方法来同时求解两个或两个以上的矩阵乘法。这一事实可以配合下面的定理以改进 ω 的上界：

定理 4.1 (渐进和不等式 (asymptotic sum inequality) [Sch81])：
对于正整数 $r,s\in\mathbb{N}$，$(n_1,m_1,p_1),\dots,(n_s,m_s,p_s)\in\mathbb{N}^3$，若 $\underline{R}\big(\bigoplus_{i=1}^s\langle n_i,m_i,p_i\rangle\big)\le r$，则有 $\sum_{i=1}^s(n_im_ip_i)^{\omega/3}\le r$。

证明：由假设，存在非负整数 h 使得 $R_h\big(\bigoplus_{i=1}^s\langle n_i,m_i,p_i\rangle\big)\le r$。对任意 $\epsilon>0$，存在 $c_\epsilon>0$ 使得对所有正整数 N，成立 $R(\langle N,N,N\rangle)\le c_\epsilon N^{\omega+\epsilon}$。考虑某个这样的 N，则根据引理 3.1，有

$$\begin{aligned}
R\left(\left(\bigoplus_{i=1}^s\langle n_i,m_i,p_i\rangle\right)^{\otimes N}\right) &\le \binom{hN+2}{2} R_{hN}\left(\left(\bigoplus_{i=1}^s\langle n_i,m_i,p_i\rangle\right)^{\otimes N}\right)\\
&\le \binom{hN+2}{2} R_h\left(\bigoplus_{i=1}^s\langle n_i,m_i,p_i\rangle\right)^N\\
&\le \binom{hN+2}{2} r^N.
\end{aligned}$$

设正整数 $\mu_1,\dots,\mu_s$ 满足 $\mu_1+\ldots+\mu_s=N$。令 $n=\prod_{i=1}^s n_i^{\mu_i}$，$m=\prod_{i=1}^s m_i^{\mu_i}$，$p=\prod_{i=1}^s p_i^{\mu_i}$。注意到

$$\begin{aligned}\left(\bigoplus_{i=1}^{s}\langle n_i,m_i,p_i\rangle\right)^{\otimes N} &= \bigoplus_{d_1+\ldots+d_s=N}\bigotimes_{i=1}^{s}\langle n_i,m_i,p_i\rangle^{\otimes d_i}\\ &= \bigoplus_{d_1+\ldots+d_s=N}\left\langle\prod_{i=1}^{s}n_i^{d_i},\prod_{i=1}^{s}m_i^{d_i},\prod_{i=1}^{s}p_i^{d_i}\right\rangle\\ &= \langle n,m,p\rangle^{\oplus\binom{N}{\mu_1,\ldots,\mu_s}}\oplus\ldots\end{aligned}$$

于是

$$R\left(\langle n,m,p\rangle^{\oplus\binom{N}{\mu_1,\ldots,\mu_s}}\right)\le R\left(\left(\bigoplus_{i=1}^{s}\langle n_i,m_i,p_i\rangle\right)^{\otimes N}\right)\le\binom{hN+2}{2}r^N.$$

令 $M=c_\epsilon^{-1}\binom{N}{\mu_1,\ldots,\mu_s}^{1/(\omega+\epsilon)}$（出于方便假设 M 是整数），则 $M\times M$ 方块矩阵乘法可用不超过 $\binom{N}{\mu_1,\ldots,\mu_s}$ 个乘法计算。现在可以如下计算 $Mn\times Mm$ 矩阵与 $Mm\times Mp$ 矩阵的乘法：将这两个矩阵划分为 $M\times M$ 分块矩阵，子矩阵大小分别为 $n\times m$ 和 $m\times p$。之后用至多 $c_\epsilon M^{\omega+\epsilon}\le\binom{N}{\mu_1,\ldots,\mu_s}$ 个子矩阵乘法和若干子矩阵加法完成计算。注意到并行地计算 $\binom{N}{\mu_1,\ldots,\mu_s}$ 个子矩阵乘法可用 $\langle n,m,p\rangle^{\oplus\binom{N}{\mu_1,\ldots,\mu_s}}$ 描述。于是有

$$R(\langle Mn,Mm,Mp\rangle)\le R\left(\langle n,m,p\rangle^{\oplus\binom{N}{\mu_1,\ldots,\mu_s}}\right)\le\binom{hN+2}{2}r^N.$$

由定理 2.3，$(M^3nmp)^{\omega/3}\le R(\langle Mn,Mm,Mp\rangle)\le\binom{hN+2}{2}r^N$。故有

$$\binom{N}{\mu_1,\ldots,\mu_s}\prod_{i=1}^{s}\left((n_im_ip_i)^{\omega/3}\right)^{\mu_i}\le c_\epsilon^{\omega}(s^N)^{\epsilon/(\omega+\epsilon)}\binom{hN+2}{2}r^N$$

其中用到不等式 $\binom{N}{\mu_1,\ldots,\mu_s}\le s^N$（前者是将 N 个元素涂成 s 种颜色，且其中第 i 中颜色的元素数量为 μ_i 的方案数，而后者是将 N 个元素涂成 s 种颜色的方案数）。上式对任意 $\mu_1+\ldots+\mu_s=N$ 成立，于是有

$$\begin{aligned}\left(\sum_{i=1}^{s}(n_im_ip_i)^{\omega/3}\right)^N &= \sum_{\mu_1+\ldots+\mu_s=N}\binom{N}{\mu_1,\ldots,\mu_s}\prod_{i=1}^{s}\left((n_im_ip_i)^{\omega/3}\right)^{\mu_i}\\ &\le \binom{N+s-1}{s-1}c_\epsilon^{\omega}(s^N)^{\epsilon/(\omega+\epsilon)}\binom{hN+2}{2}r^N.\end{aligned}$$

上式对任意正整数 N 成立。对不等式两边开 N 次方并令 $N\to\infty$，则得到

$$\sum_{i=1}^{s}(n_im_ip_i)^{\omega/3}\le s^{\epsilon/(\omega+\epsilon)}r.$$

上式对任意 $\epsilon>0$ 成立。于是 $\sum_{i=1}^{s}(n_im_ip_i)^{\omega/3}\le\lim_{\epsilon\to0}s^{\epsilon/(\omega+\epsilon)}r=r$。证毕。

推论 4.1：
若存在正整数 n 使得 $\underline{R}\left(\bigoplus_{i=1}^{n}\langle n,n,n\rangle\right)\le n^3$，则 $\omega=2$。

接下来将给出具体的构造，使张量直和的边界秩 $\underline{R}\left(\bigoplus_{i=1}^{s}\langle n_i,m_i,p_i\rangle\right)$ 较小，以满足定理 4.1 的条件。考虑张量 $\langle k,1,n\rangle$ 与 $\langle 1,m,1\rangle$。它们分别对应 k 维向量与 n 维向量的外积，以及两个 m 维向量的内积。成立如下事实：

$$\begin{aligned}R(\langle k,1,n\rangle\oplus\langle 1,m,1\rangle)&=kn+m\\ \underline{R}(\langle k,1,n\rangle)&=kn\\ \underline{R}(\langle 1,m,1\rangle)&=m.\end{aligned}$$

然而有如下引理：

引理 4.1：
对任意正整数 k，n 以及 $m\le(k-1)(n-1)$，成立

$$\underline{R}(\langle k,1,n\rangle\oplus\langle 1,m,1\rangle)\le kn+1.$$

证明：将三阶张量 $T=\langle k,1,n\rangle\oplus\langle 1,m,1\rangle\in\mathbb{F}^{k+m}\times\mathbb{F}^{n+m}\times\mathbb{F}^{kn+1}$ 按第三维划分为 $kn+1$ 个二阶张量。可以验证其中前 kn 个张量为 $T_{ij}=(e_{ij})\otimes\mathbf{0}_{m\times m}$，剩下一个张量为 $T'=0_{k\times n}\otimes\mathbf{I}_m$。这里 (e_{ij}) 代表只有第 (i,j) 个元素为 1 其余为 0 的 $k\times n$ 矩阵，$\mathbf{0}_{r\times s}$ 代表 $r\times s$ 的零矩阵，I_m 则代表 $m\times m$ 的单位矩阵。令 $e_i\in\mathbb{F}^k$，$e'_j\in\mathbb{F}^n$ 分别代表第 i，j 个元素为 1 其余为 0 的向量，则 $(e_{ij})=e_i\otimes e'_j$。接下来需要用 $kn+1$ 个二阶纯张量生成上面的 $kn+1$ 个张量。

考虑交换群 $G=\mathbb{Z}_k\times\mathbb{Z}_n$。对于 $g=(i,j)\in G$，定义同态

$$\begin{aligned}\chi_g:\quad G &\to \mathbb{C}\\ (a,b) &\mapsto \omega_k^{ai}\omega_n^{bj}\end{aligned}$$

其中 ω_t 代表 t 阶单位根。将所有 χ_g 称作 G 的不可约特征标 (irreducible characters)。对于函数 $f,f':G\to\mathbb{C}$，定义内积 $\langle f,f'\rangle=\mathbb{E}_{g\in G}f(g)f'(g)$。易证对于 $g\neq g'$，有 $\langle\chi_g,\chi_{g'}\rangle=0$，即所有 $|G|$ 个不可约特征标彼此正交。因此若将 G 到 $\mathbb{C}$ 的函数集合看作 $|G|$ 维向量空间，则 $|G|$ 个不可约特征标构成了其一组正交基。因此对任意函数 $f:G\to\mathbb{C}$ 可作 G 上的 Fourier 变换：

$$f=\sum_{g\in G}\widehat{f}(g)\chi_g$$

其中 $\widehat{f}(g)=\langle f,\chi_g\rangle$。
任选 m 个不同元素 $g_1=(i_1,j_1),\dots,g_m=(i_m,j_m)\in G$，使得其中 i_ℓ 和 j_ℓ 不为零，$\ell=1,\dots,m$。对任意 $g\in G$，定义向量 $u_g\in\mathbb{F}[\epsilon]^{k+m}$ 和 $v_g\in\mathbb{F}[\epsilon]^{n+m}$ 如下：

$$\begin{aligned}u_g&=\Big(\chi_g((0,0)),\dots,\chi_g((k-1,0)),\chi_g(g_1)\epsilon,\dots,\chi_g(g_m)\epsilon\Big)\\ v_g&=\Big(\chi_g((0,0)),\dots,\chi_g((0,n-1)),\chi_g(g_1^{-1})\epsilon,\dots,\chi_g(g_m^{-1})\epsilon\Big).\end{aligned}$$

有

$$u_g\otimes v_g=\left(\begin{array}{ccc|ccc}\chi_g((0,0)) & \cdots & \chi_g((0,n-1)) & \chi_g((0,0)g_1)\epsilon & \cdots & \chi_g((0,0)g_m)\epsilon\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ \chi_g((k-1,0)) & \cdots & \chi_g((k-1,n-1)) & \chi_g((k-1,0)g_1)\epsilon & \cdots & \chi_g((k-1,0)g_m)\epsilon\\ \hline \chi_g(g_1^{-1}(0,0))\epsilon & \cdots & \chi_g(g_1^{-1}(0,n-1))\epsilon & \chi_g(g_1^{-1}g_1)\epsilon^2 & \cdots & \chi_g(g_1^{-1}g_m)\epsilon^2\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ \chi_g(g_m^{-1}(0,0))\epsilon & \cdots & \chi_g(g_m^{-1}(0,n-1))\epsilon & \chi_g(g_m^{-1}g_1)\epsilon^2 & \cdots & \chi_g(g_m^{-1}g_m)\epsilon^2\end{array}\right).$$

对 $h\in G$，定义函数 $\delta_h:G\to\mathbb{C}$：

$$\delta_h(g)=\begin{cases}1 & g=h\\ 0 & g\neq h.\end{cases}$$

注意到 $\delta_h=\sum_{g\in G}\widehat{\delta}_h(g)\chi_g$。于是对于 $h=(i-1,j-1)$，$i=1,\dots,k$，$j=1,\dots,n$，有

$$
\begin{aligned}
&\sum_{g\in G}\widehat{\delta}_h(g)(u_g\otimes v_g)\\
&=\left(\begin{array}{ccc|ccc}
\delta_h((0,0)) & \cdots & \delta_h((0,n-1)) & \delta_h((0,0)g_1)\epsilon & \cdots & \delta_h((0,0)g_m)\epsilon\\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\
\delta_h((k-1,0)) & \cdots & \delta_h((k-1,n-1)) & \delta_h((k-1,0)g_1)\epsilon & \cdots & \delta_h((k-1,0)g_m)\epsilon\\
\hline
\delta_h(g_1^{-1}(0,0))\epsilon & \cdots & \delta_h(g_1^{-1}(0,n-1))\epsilon & \delta_h(g_1^{-1}g_1)\epsilon^2 & \cdots & \delta_h(g_1^{-1}g_m)\epsilon^2\\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\
\delta_h(g_m^{-1}(0,0))\epsilon & \cdots & \delta_h(g_m^{-1}(0,n-1))\epsilon & \delta_h(g_m^{-1}g_1)\epsilon^2 & \cdots & \delta_h(g_m^{-1}g_m)\epsilon^2
\end{array}\right)\\
&=\left(\begin{array}{c|c}
e_{ij} & \epsilon T_1\\
\hline
\epsilon T_2 & \epsilon^2 T_3
\end{array}\right).
\end{aligned}
$$

于是 $\lim_{\epsilon\to 0}\sum_{g\in G}\widehat{\delta}_h(g)(u_g\otimes v_g)=(e_{ij})\otimes \mathbf{0}_{m\times m}=T_{ij}$。这样就生成了 T_{ij} 的近似。同时由 $g_1,\dots,g_m$ 的选取可得：

$$
\sum_{g\in G}\widehat{\delta}_{(0,0)}(g)(u_g\otimes v_g)=\left(\begin{array}{c|c}
e_{11} & 0\\
\hline
0 & \epsilon^2\mathbf{I}_m
\end{array}\right).
$$

于是 $\left(\sum_{g\in G}\widehat{\delta}_{(0,0)}(g)(u_g\otimes v_g)-e_1\otimes e_1'\right)/\epsilon^2=0_{k\times n}\otimes\mathbf{I}_m=T'$。这样就生成了 T'。对 $g\in G$，定义向量 $w_g=\left(\widehat{\delta}_{(0,0)}(g),\dots,\widehat{\delta}_{(k-1,n-1)}(g),\widehat{\delta}_{(0,0)}(g)/\epsilon^2\right)\in\mathbb{F}[\epsilon]^{kn+1}$。并定义 $w'=(0,\dots,0,-1/\epsilon^2)\in\mathbb{F}[\epsilon]^{kn+1}$。对 $\epsilon>0$，令

$$
T(\epsilon)=e_1\otimes e_1'\otimes w'+\sum_{g\in G}u_g\otimes v_g\otimes w_g
$$

则 $\lim_{\epsilon\to 0}T(\epsilon)=T$ 且 $R(T(\epsilon))\le kn+1$。故 $\underline{R}(T)\le kn+1$。证毕。

推论 4.2 ([Sch 81])：
$\omega<2.548.$

证明：令 $k=4$，$n=4$，$m=9$。由引理 4.1 得 $\underline{R}(\langle 4,1,4\rangle\oplus\langle 1,9,1\rangle)\le 17$。由定理 4.1 得 $16^{\omega/3}+9^{\omega/3}\le 17$。解得 $\omega<2.548$。证毕。

（五）群表示论方法

本节仅考虑有限群。设 V是 $\mathbb{C}$ 上的向量空间，且 $\rho:G\to\mathbf{GL}(V)$ 是群 G 到 $\mathbf{GL}(V)$ 的同态，则称 ρ 为群 G 的表示 (representation)，其维数即为 V的维数。若 V中在 $\rho(G)$ 的作用下的不变子空间都

是平凡的（即 V 或 $\{0\}$），则称 ρ 为不可约表示 (irreducible representation)。群 G 的表示总可以分解为不可约表示的直和。

成立如下事实 [Lan84]：
1. 有限群 G 只有有限个（非同构）的不可约表示。设其维数分别为 $d_1, \ldots, d_k$，则有 $|G| = \sum_{i=1}^{k} d_i^2$。
2. G 为交换群当且仅当所有的 $d_i = 1$。
3. 设 H 为 G 的子群，且 H 是交换的，则 $d_i \leq [G : H] = |G|/|H|$，$i = 1, \ldots, k$。
4. 设 G 的所有不可约表示为 $\rho_1, \ldots, \rho_n$，其维数分别为 $d_1, \ldots, d_n$。并设 H 的所有不可约表示为 $\sigma_1, \ldots, \sigma_m$，其维数分别为 $d'_1, \ldots, d'_m$。则 $G \times H$ 共有 nm 个不可约表示 $\tau_{11}, \ldots, \tau_{nm}$，其中对 $g \in G, h \in H$，$\tau_{ij}(g, h) = \rho_i(g) \otimes \sigma_j(h)$。$\tau_{ij}$ 的维数为 $d_i d'_j$。

定义 $\mathbb{C}[G]$ 为 $\mathbb{C}$ 上以 G 为基底的自由向量空间 (free vector space)。即 G 中的元素具有如下形式：

$$x = \sum_{g \in G} a_g g$$

其中 $a_g \in \mathbb{C}$。在此基础上定义乘法：

$$\left(\sum_{g \in G} a_g g \right) \cdot \left(\sum_{h \in G} b_h h \right) = \sum_{f \in G} \left(\sum_{gh = f} a_g b_h \right) f.$$

可以验证 $\mathbb{C}[G]$ 是 $\mathbb{C}$ 上的代数，称为 G 的群代数 (group algebra)。

记 $\mathbb{C}^{n \times n}$ 为 $\mathbb{C}$ 上的 $n \times n$ 矩阵代数 (matrix algebra)。有如下定理：

定理 5.1 (Wedderburn 结构定理 [Lan84])

$$\begin{array}{rcl} \mathbb{C}[G] & \cong & \mathbb{C}^{d_1 \times d_1} \times \ldots \times \mathbb{C}^{d_k \times d_k} \\ g & \mapsto & \big(\rho_1(g), \ldots, \rho_k(g)\big) \end{array}$$

其中 $\rho_1, \ldots, \rho_k$ 是 G 的所有不可约表示，其维数分别为 $d_1, \ldots, d_k$。

令 D 为 $\mathbb{C}[G]$ 到 $\mathbb{C}^{d_1 \times d_1} \times \ldots \times \mathbb{C}^{d_k \times d_k}$ 的同构映射，则有

$$a \cdot b = D^{-1}(D(a) \cdot D(b)).$$

若 G 为交换群，则 $d_1 = \ldots = d_k = 1$。于是 $D(a), D(b) \in \mathbb{C}^{|G|}$，其乘法定义为逐点相乘，而 $a \cdot b$ 可看作向量的卷积。此时上式即为卷积定理 (convolution theorem)。而对于一般的有限群 G，$D(a) \cdot D(b)$ 可通过计算 $\mathbb{C}^{d_i \times d_i}$ 中的矩阵乘法得到（$i = 1, \ldots, k$）。这说明要计算 $\mathbb{C}[G]$ 中的乘法，只需求解 $\oplus_{i=1}^{k} \langle d_i, d_i, d_i \rangle$（事实上还需计算 D 和 D^{-1}，但 D 是 $\mathbb{C}$-线性的，因此 D 和 D^{-1} 的计算只需要加法和数乘操作，不计入双线性复杂度）。

接下来将矩阵乘法“嵌入”到 $\mathbb{C}[G]$ 的乘法中，再通过上面的讨论将其归约为更小规模的矩阵乘法。为此引入如下定义：对于群 G 的子集 S，定义 S 的商集 (quotient set) 为 $Q(S) = \left\{ ss'^{-1} : s, s' \in S \right\}$。对于群 G 的子集 X, Y, Z，如果下列条件成立，则称 (X, Y, Z) 在 G 中满足三元组乘积性质 (triple product property)：

$$xyz = 1 \iff x = y = z = 1 \qquad \forall x \in Q(X),\ y \in Q(Y),\ z \in Q(Z).$$

举例：令 $G = \mathbb{Z}_n \times \mathbb{Z}_m \times \mathbb{Z}_p$，$X = \mathbb{Z}_n \times \{0\} \times \{0\}$，$Y = \{0\} \times \mathbb{Z}_m \times \{0\}$，$Z = \{0\} \times \{0\} \times \mathbb{Z}_p$。则 (X, Y, Z) 在 G 中满足三元组乘积性质。

考虑矩阵乘法 $A \cdot B$，其中 A，B 分别为 $\mathbb{F} = \mathbb{C}$ 上的 $n \times m$ 和 $m \times p$ 矩阵。设 (X, Y, Z) 在 G 中满足三元组乘积性质，并且 $|X| = n$，$|Y| = m$，$|Z| = p$。设 $A = (A_{xy})_{x \in X, y \in Y}$，其行和列分别以 X 和 Y 中的元素为索引。类似地设 $B = (B_{yz})_{y \in Y, z \in Z}$。定义 $\bar{A}, \bar{B} \in \mathbb{C}[G]$：

$$\bar{A} = \sum_{x \in X, y \in Y} A_{xy} x^{-1} y, \qquad \bar{B} = \sum_{y \in Y, z \in Z} B_{yz} y^{-1} z.$$

引理 5.1：
设 (X, Y, Z) 在 G 中满足三元组乘积性质。并设 $A = (A_{xy})_{x \in X, y \in Y}$，$B = (B_{yz})_{y \in Y, z \in Z}$，而 $C = A \cdot B = (C_{xz})_{x \in X, z \in Z}$ 为矩阵 A 与 B 的乘积，则对任意 $x \in X$，$z \in Z$，C_{xz} 即为 $\bar{A} \cdot \bar{B}$ 中 $x^{-1} z$ 的系数。

证明：由 $\mathbb{C}[G]$ 中乘法的定义，对任意 $x \in X$，$z \in Z$，$\bar{A} \cdot \bar{B}$ 中 $x^{-1} z$ 的系数为

$$\sum_{\substack{x' \in X, y \in Y \\ y' \in Y, z' \in Z \\ x'^{-1} y y'^{-1} z' = x^{-1} z}} A_{x'y} B_{y'z'}.$$

注意到 $x'^{-1} y y'^{-1} z' = x^{-1} z$ 当且仅当 $x x'^{-1} y y'^{-1} z' z^{-1} = 1$（由三元组乘积性质）当且仅当 $x = x'$，$y = y'$，$z = z'$。故 $x^{-1} z$ 的系数即为 $\sum_{y \in Y} A_{xy} B_{yz} = C_{xz}$。证毕。

引理 5.2：
设 (X, Y, Z) 在 G 中满足三元组乘积性质，而 π 是 $\{X, Y, Z\}$ 的一个置换， 则 $(\pi(X), \pi(Y), \pi(Z))$ 在 G 中亦满足三元组乘积性质。

证明：只需证明

$$\begin{aligned} & xx'^{-1}yy'^{-1}zz'^{-1} = 1 && \forall x, x' \in X,\ y, y' \in Y,\ z, z' \in Z \\ \iff\ & \tau(xx'^{-1})\tau(yy'^{-1})\tau(zz'^{-1}) = 1 && \forall x, x' \in X,\ y, y' \in Y,\ z, z' \in Z \end{aligned}$$

其中 τ 是 $\left\{xx'^{-1}, yy'^{-1}, zz'^{-1}\right\}$ 的任意置换。对等式 $xx'^{-1}yy'^{-1}zz'^{-1} = 1$ 的两边作关于 zz'^{-1} 的共轭得到 $zz'^{-1}xx'^{-1}yy'^{-1} = 1$。因此所需性质对 $\tau_1 : xx'^{-1} \mapsto zz'^{-1}, yy'^{-1} \mapsto xx'^{-1}, zz'^{-1} \mapsto yy'^{-1}$ 成立。类似地，对等式 $xx'^{-1}yy'^{-1}zz'^{-1} = 1$ 的两边求逆得到 $z'z^{-1}y'y^{-1}x'x^{-1} = 1$，再将 x, x'（以及 y, y' 和 z, z'）交换名称，可知所需性质对 $\tau_2 : xx'^{-1} \mapsto zz'^{-1}, yy'^{-1} \mapsto yy'^{-1}, zz'^{-1} \mapsto xx'^{-1}$ 成立。由 τ_1 和 τ_2 可生成所有置换。证毕。

引理 5.3：
设 (X, Y, Z) 在 G 中满足三元组乘积性质，且 (S, T, U) 在 H 中满足三元组乘积性质，则 $(X \times S, Y \times T, Z \times U)$ 在 $G \times H$ 中满足三元组乘积性质。

证明：由定义立即得到。

采用如下术语：若 G 包含子集 X, Y, Z 使得 (X, Y, Z) 在 G 中满足三元组乘积性质，且 $|X| = n$，$|Y| = m$，$|Z| = p$，则称 G “实现” (realize) 了 $\langle n, m, p\rangle$。由引理 5.1，这意味着求解 $\langle n, m, p\rangle$ 可转化为计算 $\mathbb{C}[G]$ 中的乘法。

定理 5.2 ([CU03])：
设 G 的所有不可约表示的维数分别为 $d_1, \ldots, d_k$，并设 G 实现了 $\langle n, m, p\rangle$，则成立：

$$(nmp)^{\omega/3} \leq \sum_{i=1}^{k} d_i^{\omega}.$$

证明：对任意 $\epsilon > 0$，存在常数 $c_\epsilon > 0$ 使得 $R(\langle N, N, N\rangle) \leq c_\epsilon N^{\omega+\epsilon}$ 对所有正整数 N 成立。固定 ϵ。由假设，G 包含子集 X, Y, Z 使得 (X, Y, Z) 在 G 中满足三元组乘积性质，且 $|X| = n$，$|Y| = m$，$|Z| = p$。由引理 5.2，(Y, Z, X) 和 (Z, X, Y) 在 G 中亦满足三元组乘积性质。由引理 5.3，(XYZ, XYZ, XYZ) 在 G^3 中满足三元组乘积性质。再由引理 5.3，对任意正整数 i，

$\left((XYZ)^i,(XYZ)^i,(XYZ)^i\right)$ 在 G^{3i} 中满足三元组乘积性质，故 G^{3i} 实现了 $\left\langle (nmp)^i,(nmp)^i,(nmp)^i \right\rangle$。由引理 5.1，求解 $\left\langle (nmp)^i,(nmp)^i,(nmp)^i \right\rangle$ 可转化为计算 $\mathbb{C}\left[G^{3i}\right]$ 中的乘法。注意到 G^{3i} 共有 k^{3i} 个不可约表示。对 $J=(j_1,\dots,j_{3i})\in\{1,\dots,k\}^{3i}$，其第 J 个表示的维度为 $d_J=\prod_{\ell=1}^{3i} d_{j_\ell}$。前面的讨论说明要计算 $\mathbb{C}\left[G^{3i}\right]$ 中的乘法，只需求解 $\oplus_J\langle d_J,d_J,d_J\rangle$。由此得到：

$$
\begin{aligned}
(nmp)^{i\omega} &\le R\Big(\left\langle (nmp)^i,(nmp)^i,(nmp)^i \right\rangle\Big)\\
&\le R(\oplus_J\langle d_J,d_J,d_J\rangle)\\
&\le \sum_J R(\langle d_J,d_J,d_J\rangle)\\
&\le \sum_J c_\epsilon d_J^{\omega+\epsilon}\\
&= c_\epsilon\left(\sum_{j=1}^k d_j^{\omega+\epsilon}\right)^{3i}.
\end{aligned}
$$

上式对任意正整数 i 成立。对不等式两边开 $3i$ 次方并令 $i\to\infty$，则得到

$$
(nmp)^{\omega/3}\le \sum_{j=1}^k d_j^{\omega+\epsilon}.
$$

上式对任意 $\epsilon>0$ 成立。于是 $(nmp)^{\omega/3}\le \lim_{\epsilon\to 0}\sum_{j=1}^k d_j^{\omega+\epsilon}=\sum_{j=1}^k d_j^{\omega}$。证毕。

推论 5.1 ([CU03])：
设 G 的所有不可约表示的维数分别为 $d_1,\dots,d_k$，并设 G 实现了 $\langle n,m,p\rangle$。令 $d_{\max}=\max\{d_1,\dots,d_k\}$，则成立：

$$
(nmp)^{\omega/3}\le d_{\max}^{\omega-2}\cdot\sum_{i=1}^k d_i^2 = d_{\max}^{\omega-2}|G|.
$$

注意到要利用推论 5.1 得到非平凡的矩阵乘法快速算法，必须成立 $|G|<nmp$，否则最多得到 $\omega\le 3$。然而有如下结论：

引理 5.4：
对于实现了 $\langle n,m,p\rangle$ 的交换群 G，成立 $|G|\ge nmp$。

证明：由假设，G 包含子集 X, Y, Z 使得 (X, Y, Z) 在 G 中满足三元组乘积性质，且 $|X| = n$，$|Y| = m$，$|Z| = p$。定义

$$\begin{aligned} f\colon \quad X \times Y \times Z &\to G \\ (x, y, z) &\mapsto xyz. \end{aligned}$$

只需证明 f 是单射。假设对于 $(x, y, z) \neq (x', y', z')$，成立 $f(x, y, z) = f(x', y', z')$，即 $xyz = x'y'z'$。由于 G 是交换群，有 $xx'^{-1}yy'^{-1}zz'^{-1} = 1$。由三元组乘积性质得 $x = x'$，$y = y'$，$z = z'$，即 $(x, y, z) = (x', y', z')$，矛盾。故 $|G| \geq nmp$。证毕。

然而对于非交换群 G 有可能成立 $|G| < nmp$，比如下面的例子：

举例：
令 $G = \mathbb{S}_3$。定义 G 的子群 $X = \langle (12) \rangle = \{\mathbf{id}, (12)\}$，$Y = \langle (23) \rangle = \{\mathbf{id}, (23)\}$，$Z = \langle (13) \rangle = \{\mathbf{id}, (13)\}$。则 (X, Y, Z) 在 G 中满足三元组乘积性质。并且 $|G| = 6 < 8 = |X||Y||Z|$。

这一结论可以推广到高阶的对称群：

定理 5.3：
对正整数 n，令 $N = n(n+1)/2$，则 $\mathbb{S}_N$ 实现了 $\langle m, m, m \rangle$，其中 $m = \prod_{i=1}^{n} i! = |\mathbb{S}_N|^{1/2 - o(1)}$。

证明：考虑下面的三角阵

$$\begin{array}{ccccc} & & (n,1) & & \\ & (n-1,1) & & (n-1,2) & \\ \vdots & & \vdots & & \ddots \\ (1,1) & & (1,2) & \cdots & (1,n) \end{array}$$

令 $\mathbb{S}_N$ 作用于这 $N = n(n+1)/2$ 个元素上。令 $X, Y, Z \subseteq \mathbb{S}_N$ 分别为保持任意元素所在的行/列/对角线不变的置换构成的子群，则 $|X| = |Y| = |Z| = \prod_{i=1}^{n} i! = m$。接下来只需证明 (X, Y, Z) 在 $\mathbb{S}_N$ 中满足三元组乘积性质。由于 X, Y, Z 是子群，只需证明：

$$\pi_3 \pi_2 \pi_1 = 1 \iff \pi_1 = \pi_2 = \pi_3 = 1 \qquad \forall \pi_1 \in X,\ \pi_2 \in Y,\ \pi_3 \in Z.$$

考虑满足 $\pi_1 \pi_2 \pi_3 = 1$ 的 π_1，π_2，π_3。定义字典序：$(x, y) < (x', y')$ 若 $y < y'$，或者 $y = y'$

且 $x < x'$。对 (x, y) 做归纳。假设对所有 $(x', y') < (x, y)$，都有
$\pi_1((x', y')) = \pi_2((x', y')) = \pi_3((x', y')) = (x', y')$（当 $(x, y) = (1, 1)$ 时显然成立），下面证明 $\pi_1((x, y)) = \pi_2((x, y)) = \pi_3((x, y)) = (x, y)$。由归纳假设，$\pi_1$ 固定 (x, y) 同一行以左的元素。于是 π_1 固定 (x, y) 或将其向右移动。设 π_1 将 (x, y) 向右移动。接下来由归纳假设，π_2 固定 $\pi_1((x, y))$ 或将其向上移动。无论哪种情况，π_3 都无法将其移回原位。这与 $\pi_3\pi_2\pi_1 = 1$ 矛盾。故 π_1 固定 (x, y)。接下来由归纳假设，π_2 固定 $\pi_1((x, y))$ 或将其向上移动。若 π_2 将 (x, y) 向上移动，则 π_3 无法将其移回原位。故 π_2 固定 (x, y)。随之可得 π_3 固定 (x, y)。
由归纳法，上述结论对所有 (x, y) 成立。故 $\pi_1 = \pi_2 = \pi_3 = 1$。证毕。

然而，定理 5.3 不能直接给出 ω 的非平凡上界，这是因为对称群的不可约表示的（平均）维度太高了：考虑 $\mathbb{S}_N$ 的不可约表示数量 k，即其共轭类数量，亦即 N 的正整数拆分方案数。有 $k = 2^{O(\sqrt{N})} \ll |\mathbb{S}_N|$。由 Hölder 不等式，

$$|\mathbb{S}_N| = \sum_{i=1}^{k} d_i^2 \le \left(\sum_{i=1}^{k} d_i^3\right)^{2/3} \left(\sum_{i=1}^{k} 1^3\right)^{1/3} = \left(\sum_{i=1}^{k} d_i^3\right)^{2/3} k^{1/3}.$$

故 $\sum_{i=1}^{k} d_i^3 \ge |\mathbb{S}_N|^{3/2} / k^{1/2} \ge \left(\prod_{i=1}^{n} i!\right)^3 = |X||Y||Z|$。这说明即便令 $\omega = 3$，定理 5.2 中的不等式依然成立，从而无法得到 ω 的非平凡上界。

（六）群表示论方法续

首先给出如下的构造，配合推论 5.1 可以给出 ω 的非平凡上界：

对正整数 m，令 $G = (\mathbb{Z}_m)^6 \rtimes \mathbb{S}_2$ 为 $(\mathbb{Z}_m)^6$ 和 $\mathbb{S}_2$ 的半直积 (semidirect product)。用 2×3 矩阵表示 $(\mathbb{Z}_m)^6$ 中的元素，并设 $\mathbb{S}_2 = \{1, \pi\}$。$G$ 中的元素可唯一地表示为

$$\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \pi^i, \qquad i \in \{0, 1\}.$$

$\mathbb{S}_2$ 作用在 $(\mathbb{Z}_m)^6$ 上，其中 π 交换 $(\mathbb{Z}_m)^6$ 中元素的两行，即

$$\pi \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} = \begin{pmatrix} d & e & f \\ a & b & c \end{pmatrix} \pi.$$

定义 X, Y, Z 如下：

$$X = \left\{ \begin{pmatrix} x_1 & 0 & 0 \\ 0 & x_2 & 0 \end{pmatrix} \pi^i : \ x_1 \neq 0,\ i \in \{0,1\} \right\}$$
$$Y = \left\{ \begin{pmatrix} 0 & y_1 & 0 \\ 0 & 0 & y_2 \end{pmatrix} \pi^i : \ y_1 \neq 0,\ i \in \{0,1\} \right\}$$
$$Z = \left\{ \begin{pmatrix} 0 & 0 & z_1 \\ z_2 & 0 & 0 \end{pmatrix} \pi^i : \ z_1 \neq 0,\ i \in \{0,1\} \right\}.$$

定理 6.1：
上述构造中 (X, Y, Z) 在 G 中满足三元组乘积性质。

证明：设 $x \in Q(X)$，$y \in Q(Y)$，$z \in Q(Z)$ 且 $xyz = 1$。有

$$xyz = \begin{matrix} ■ & □ & □ \\ □ & ? & □ \end{matrix} z^i \begin{matrix} ■ & □ & □ \\ □ & ? & □ \end{matrix} \cdot \begin{matrix} □ & ■ & □ \\ □ & □ & ? \end{matrix} z^j \begin{matrix} □ & ■ & □ \\ □ & □ & ? \end{matrix} \cdot \begin{matrix} □ & □ & ■ \\ ? & □ & □ \end{matrix} z^k \begin{matrix} □ & □ & ■ \\ ? & □ & □ \end{matrix} = \begin{matrix} □ & □ & □ \\ □ & □ & □ \end{matrix}$$

其中 ■ 代表非零元素，□ 代表零，而 ? 代表两种情况皆有可能。由 $xyz = 1$ 可得 $i + j + k$ 为偶数。有如下四种情况：
(1) $i = j = k = 0$。此时有

$$xyz = \begin{matrix} ? & □ & □ \\ □ & ? & □ \end{matrix} \cdot \begin{matrix} □ & ? & □ \\ □ & □ & ? \end{matrix} \cdot \begin{matrix} □ & □ & ? \\ ? & □ & □ \end{matrix} = \begin{matrix} □ & □ & □ \\ □ & □ & □ \end{matrix}.$$

可知 $x = y = z = 1$。
(2) $i = 1$，$j = 1$，$k = 0$。将 z^i 移到 z^j 处，得到：

$$xyz = \begin{matrix} ■ & □ & □ \\ □ & ? & □ \end{matrix} \cdot \begin{matrix} □ & ? & □ \\ ■ & □ & □ \end{matrix} \cdot \begin{matrix} □ & □ & ? \\ □ & ■ & □ \end{matrix} \cdot \begin{matrix} □ & ■ & □ \\ □ & □ & ? \end{matrix} \cdot \begin{matrix} □ & □ & ■ \\ ? & □ & □ \end{matrix} \cdot \begin{matrix} □ & □ & ■ \\ ? & □ & □ \end{matrix} = \begin{matrix} □ & □ & □ \\ □ & □ & □ \end{matrix}$$

但这是不可能的，因为只有一个乘数左上角的位置不为零。
(3) $i = 0$，$j = 1$，$k = 1$。和第二种情况对称。类似地可证明这种情况不会出现。
(4) $i = 1$，$j = 0$，$k = 1$。和第二种情况对称。类似地可证明这种情况不会出现。
故 $x = y = z = 1$。(X, Y, Z) 在 G 中满足三元组乘积性质。证毕。

推论 6.1 ([CKSU05])：
$\omega \leq 2.908\ldots$

证明：上面的构造中 $|G| = 2m^6$，$|X| = |Y| = |Z| = 2m(m-1)$。$G$ 的不可约表示的最大可能维度为 2，因为 $(\mathbb{Z}_m)^6$ 是交换群且 $\left[G : (\mathbb{Z}_m)^6\right] = 2$。由推论 5.1，成立：

$$(2m(m-1))^{\omega} \le 2^{\omega-2} 2m^6.$$

令 $m = 17$，解得 $\omega \le 2.908\ldots$。证毕。

下面给出一种更好的构造：

设 H 为交换群。其子集 $A_0, \ldots, A_{n-1}, B_0, \ldots, B_{n-1}$ 满足如下性质：
1. $|A_i + B_i| = |A_i||B_i|$, $\forall 0 \le i < n$
2. $(A_i + B_i) \cap (A_j + B_k) = \emptyset$, $\forall 0 \le i < n$, $0 \le j \ne k < n$
称作同时双乘积性质 (simultaneous double product property)。

考虑三角阵

$$\begin{array}{cccc} (n,1,1) & & & \\ (n-1,1,2) & (n-1,2,1) & & \\ \vdots & \vdots & \ddots & \\ (1,1,n) & (1,2,n-1) & \cdots & (1,n,1) \end{array}$$

即定理 5.3 证明中的三角阵，但每个元素扩充为三元组 (s,t,u)，其中 $s+t+u = n+2$。记所有三元组构成的集合为 Δ_m，其中 $m = n(n+1)/2$ 为集合大小。令 $G = (H^3)^m \rtimes \mathbb{S}_m$。用 $3 \times m$ 矩阵表示 $(H^3)^m$ 中的元素。G 中的元素可唯一地表示为

$$\begin{pmatrix} x_1 & y_1 & z_1 \\ \vdots & \vdots & \vdots \\ x_m & y_m & z_m \end{pmatrix} \pi, \qquad x_i, y_i, z_i \in H,\ \pi \in \mathbb{S}_m.$$

$\mathbb{S}_m$ 作用在 $(H^3)^m$ 上，将 $(H^3)^m$ 中元素的行重新排列：

$$\pi \begin{pmatrix} x_1 & y_1 & z_1 \\ \vdots & \vdots & \vdots \\ x_m & y_m & z_m \end{pmatrix} = \begin{pmatrix} x_{\pi(1)} & y_{\pi(1)} & z_{\pi(1)} \\ \vdots & \vdots & \vdots \\ x_{\pi(m)} & y_{\pi(m)} & z_{\pi(m)} \end{pmatrix} \pi.$$

定义 $X, Y, Z \subseteq G$ 如下：

$$
\begin{aligned}
X &= \left\{ \begin{pmatrix} a_{11n} & -b_{11n} & 0 \\ \vdots & \vdots & \vdots \\ a_{n11} & -b_{n11} & 0 \end{pmatrix} \pi : a_{stu} \in A_s,\ b_{stu} \in B_t,\ \pi \in \mathbb{S}_m \right\} \\
Y &= \left\{ \begin{pmatrix} 0 & a_{11n} & -b_{11n} \\ \vdots & \vdots & \vdots \\ 0 & a_{n11} & -b_{n11} \end{pmatrix} \pi : a_{stu} \in A_t,\ b_{stu} \in B_u,\ \pi \in \mathbb{S}_m \right\} \\
Z &= \left\{ \begin{pmatrix} -b_{11n} & 0 & a_{11n} \\ \vdots & \vdots & \vdots \\ -b_{n11} & 0 & a_{n11} \end{pmatrix} \pi : a_{stu} \in A_u,\ b_{stu} \in B_s,\ \pi \in \mathbb{S}_m \right\}.
\end{aligned}
$$

定理 6.2：
上述构造中 (X, Y, Z) 在 G 中满足三元组乘积性质。

证明：设 $x \in Q(X)$，$y \in Q(Y)$，$z \in Q(Z)$ 且 $xyz = 1$。有

$$
\begin{aligned}
xyz = & \begin{pmatrix} a^x_{11n} & -b^x_{11n} & 0 \\ \vdots & \vdots & \vdots \\ a^x_{n11} & -b^x_{n11} & 0 \end{pmatrix} \pi_1 \begin{pmatrix} -{a'}^x_{11n} & {b'}^x_{11n} & 0 \\ \vdots & \vdots & \vdots \\ -{a'}^x_{n11} & {b'}^x_{n11} & 0 \end{pmatrix} \\
& \cdot \begin{pmatrix} 0 & a^y_{11n} & -b^y_{11n} \\ \vdots & \vdots & \vdots \\ 0 & a^y_{n11} & -b^y_{n11} \end{pmatrix} \pi_2 \begin{pmatrix} 0 & -{a'}^y_{11n} & {b'}^y_{11n} \\ \vdots & \vdots & \vdots \\ 0 & -{a'}^y_{n11} & {b'}^y_{n11} \end{pmatrix} \\
& \cdot \begin{pmatrix} b^z_{11n} & 0 & -a^z_{11n} \\ \vdots & \vdots & \vdots \\ b^z_{n11} & 0 & -a^z_{n11} \end{pmatrix} \pi_3 \begin{pmatrix} -{b'}^z_{11n} & 0 & {a'}^z_{11n} \\ \vdots & \vdots & \vdots \\ -{b'}^z_{n11} & 0 & {a'}^z_{n11} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \end{pmatrix}
\end{aligned}
$$

其中 $\pi_1, \pi_2, \pi_3 \in \mathbb{S}_m$。由 $xyz = 1$ 得 $\pi_1 \pi_2 \pi_3 = 1$。考虑等式两边的第一列第 (s, t, u) 行并将 π_1，π_2 右移到 π_3 处得到：

$$
a^x_{stu} - {a'}^x_{\pi_1(stu)} - b^z_{\pi_1\pi_2(stu)} + {b'}^z_{stu} = 0.
$$

设 $\pi_1(stu) = s't'u'$，$\pi_1\pi_2(stu) = s''t''u''$。注意到 $a^x_{stu}, {b'}^z_{stu} \in A_s$，${a'}^x_{\pi_1(stu)} \in A_{s'}$，$b^z_{\pi_1\pi_2(stu)} \in A_{s''}$。由子集 $A_0, \ldots, A_{n-1}, B_0, \ldots, B_{n-1}$ 的同时双乘积性质的第二条得 $s' = s''$。故 $\pi_1\pi_2\pi_1^{-1}(s't'u') = s't''u''$。当 (s, t, u) 取遍 Δ_m 中元素时 (s', t', u') 也取遍 Δ_m 中元素。故 $\pi_1\pi_2\pi_1^{-1}$ 固定 Δ_m 中元素的第一个坐标，即保持元素在三角阵中的行索引不变。类似地考虑第二和第三列，可证明 $(\pi_1\pi_2)^{-1}$ 保持元素在三角阵中的列索引不变，以及 π_1 保持元素在三角阵中的对

角线索引不变。注意到 $(\pi_1\pi_2)^{-1}\cdot\pi_1\pi_2\pi_1^{-1}\cdot\pi_1=1$。由定理 5.3 的证明，保持三角阵行/列/对角线不变的置换构成的子群在 $\mathbb{S}_m$ 中满足三元组乘积性质。故 $(\pi_1\pi_2)^{-1}=\pi_1\pi_2\pi_1^{-1}=\pi_1=1$。由此得到 $\pi_1=\pi_2=\pi_3=1$。再由子集 $A_0,\dots,A_{n-1},B_0,\dots,B_{n-1}$ 的同时双乘积性质的第一条得对任意 $(s,t,u)\in\Delta_m$，成立 $a^x_{stu}=a'^x_{stu},\dots,b^z_{stu}=b'^z_{stu}$。故 $x=y=z=1$。证毕。

设 $|A_i||B_i|=n^\alpha$，$i=1,\dots,n$，且 $|H|=n^\beta$。有 $|G|=n^{3m\beta}m!$，$|X|=|Y|=|Z|=n^{m\beta}m!$，$d_{\max}\le m!$。由推论 5.1，成立

$$(n^{m\beta}m!)^\omega\le(m!)^{\omega-1}n^{3m\beta}.$$

若上述结论对任意充分大的 n 成立，则令 $n\to\infty$ 可得

$$\omega\le(3\beta-2)/\alpha.$$

注意到 $n^\alpha=|A_i||B_i|=|A_i+B_i|\le|H|=n^\beta$，因此有 (1) $\alpha\le\beta$。此外所有 A_i（以及 B_i）是不交的，否则无法满足同时双乘积性质。因此有 $\sum_{i=1}^n|A_i|,\sum_{i=1}^n|B_i|\le|H|$。于是 $n^{2+2\alpha}\le|H|^2=n^{2\beta}$，解得 (2) $\alpha+2\le\beta$。由 (1) 和 (2) 得到 $(3\beta-2)/\alpha\ge2$，并且有 $\lim_{n\to\infty}(3\beta-2)/\alpha=2$ 当且仅当 $\lim_{n\to\infty}\alpha=\lim_{n\to\infty}\beta=2$。由此给出如下猜想：

猜想 6.1 ([CKSU05])
对任意充分大的 n，存在交换群 H 以及子集 $A_0,\dots,A_{n-1},B_0,\dots,B_{n-1}\subseteq H$，使得 $A_0,\dots,A_{n-1},B_0,\dots,B_{n-1}$ 满足同时双乘积性质，且 $|H|=n^{2+o(1)}$，$|A_i||B_i|\le n^{2-o(1)}$，$i=1,\dots,n$。

该猜想若成立，则有 $\omega=2$。

目前能做到的是对任意正整数 k，$\lim_{n\to\infty}\alpha=\log_2(k-1)$，$\lim_{n\to\infty}\beta=\log_2k$：

定理 6.3 ([Str87, CKSU05])：
$\omega\le2.478\dots$

证明：
构造交换群 H 以及子集 $A_0,\dots,A_{n-1},B_0,\dots,B_{n-1}\subseteq H$ 如下：对于正整数 ℓ 和 k，令 $H=\mathbb{Z}_k^{2\ell}$。对大小为 ℓ 的集合 $S\subseteq\{1,\dots,2\ell\}$，令 $A_S=\prod_{i=1}^{2\ell}X_i^S$，其中若 $i\in S$，则 $X_i^S=\mathbb{Z}_k\setminus\{0\}$，否则 $X_i^S=\{0\}$。令 $B_S=\prod_{i=1}^{2\ell}X_i^{\bar S}$。易证这样选取的子集 $A_0,\dots,A_{n-1},B_0,\dots,B_{n-1}$ 满足同时双乘积性质。每个子集的大小为 $(k-1)^\ell$。这里 $n=\binom{2\ell}{\ell}=2^{2\ell-o(\ell)}$，$m=n(n+1)/2=2^{4\ell-o(\ell)}$。可得 $n^\beta=|H|=k^{2\ell}$，$n^\alpha=|A_i||B_i|=(k-1)^{2\ell}$。解得 $\lim_{\ell\to\infty}\alpha=\log_2(k-1)$，$\lim_{\ell\to\infty}\beta=\log_2k$。令 $k=6$，

得 $\omega \le (3\log_2 6 - 2)/\log_2 5 = 2.478\ldots$。证毕。

（七）唯一可解谜题

考虑一个 $N \times n$ 矩阵 P，其第 i 行 j 列的上的数字 $P_{ij} \in \{1,2,3\}$，$i = 1,\ldots,N$，$j = 1,\ldots,n$。令 $S_{ik} = \{1 \le j \le n : P_{ij} = k\}$，$k = 1,2,3$，$i = 1,\ldots,N$。

设矩阵 P 满足如下性质：对任意不完全相同的 $1 \le i_1, i_2, i_3 \le N$，存在 $1 \le j \le n$，使得三个条件 $P_{i_1 j} = 1$，$P_{i_2 j} = 2$，$P_{i_3 j} = 3$ 中至少成立两个（等价地，j 属于 $S_{i_1 1}, S_{i_2 2}, S_{i_3 3}$ 中至少两个集合）。则称 P 为一个唯一可解谜题 (uniquely solvable puzzle)。进一步，若对任意不完全相同的 $1 \le i_1, i_2, i_3 \le N$，存在 $1 \le j \le n$，使得三个条件 $P_{i_1 j} = 1$，$P_{i_2 j} = 2$，$P_{i_3 j} = 3$ 中恰好成立两个（等价地，j 恰属于 $S_{i_1 1}, S_{i_2 2}, S_{i_3 3}$ 中的两个集合），则称 P 为一个强唯一可解谜题 (strong uniquely solvable puzzle)。定义（强）唯一可解谜题的容量 (capacity) 为最大的实数 C，使得对任意正整数 n，存在 $N \times n$ 的（强）唯一可解谜题，其中 $N = (C - o(1))^n$。

易证 P 为唯一可解谜题当且仅当如下性质成立：设 π_1, π_2, π_3 是 $\{1,\ldots,N\}$ 上的置换，并设对于任意 $1 \le i \le N$，集合 $S_{\pi_1(i)1}, S_{\pi_2(i)2}, S_{\pi_3(i)3}$ 都构成了 $\{1,\ldots,n\}$ 的一个划分，则有 $\pi_1 = \pi_2 = \pi_3$。可将 P 看作一个拼图游戏 (jigsaw puzzle)，其每一行有三块拼图 S_{i1}, S_{i2}, S_{i3}，$i = 1,\ldots,N$，分别写着数字 $1,2,3$。对于写着同一个数字的 N 块拼图，允许对于将其所在的行进行置换。目标是对于每一行，其中置换后的三块拼图仍然能够完美地拼成完整的一行。则 P 为唯一可解谜题意味着完成上述目标的唯一方式是将每块拼图保持原有的位置不变。这是其名字的由来。

对正整数 m，令 $G = (\mathbb{Z}_m)^{Nn} \rtimes \mathbb{S}_N$。用 $N \times n$ 矩阵表示 $(\mathbb{Z}_m)^{Nn}$ 中的元素。G 中的元素可唯一地表示为

$$\begin{pmatrix} x_{11} & \ldots & x_{1n} \\ \vdots & \vdots & \vdots \\ x_{N1} & \ldots & x_{Nn} \end{pmatrix} \pi, \qquad x_{ij} \in \mathbb{Z}_m,\ \pi \in \mathbb{S}_N.$$

$\mathbb{S}_N$ 作用在 $(\mathbb{Z}_m)^{Nn}$ 上，将 $(\mathbb{Z}_m)^{Nn}$ 中元素的行重新排列：

$$\pi \begin{pmatrix} x_{11} & \ldots & x_{1n} \\ \vdots & \vdots & \vdots \\ x_{N1} & \ldots & x_{Nn} \end{pmatrix} = \begin{pmatrix} x_{\pi(1)1} & \ldots & x_{\pi(1)n} \\ \vdots & \vdots & \vdots \\ x_{\pi(N)1} & \ldots & x_{\pi(N)n} \end{pmatrix} \pi.$$

对于 $N \times n$ 矩阵 P，定义 $X, Y, Z \subseteq G$ 如下：

$$
\begin{aligned}
X &= \left\{ \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & \vdots & \vdots \\ x_{N1} & \dots & x_{Nn} \end{pmatrix} \pi : x_{ij} \neq 0 \iff P_{ij} = 1,\ \pi \in \mathbb{S}_m \right\} \\
Y &= \left\{ \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & \vdots & \vdots \\ x_{N1} & \dots & x_{Nn} \end{pmatrix} \pi : x_{ij} \neq 0 \iff P_{ij} = 2,\ \pi \in \mathbb{S}_m \right\} \\
Z &= \left\{ \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & \vdots & \vdots \\ x_{N1} & \dots & x_{Nn} \end{pmatrix} \pi : x_{ij} \neq 0 \iff P_{ij} = 3,\ \pi \in \mathbb{S}_m \right\}.
\end{aligned}
$$

定理 7.1：
若 P为强唯一可解谜题，则如上定义的 (X, Y, Z) 在 G 中满足三元组乘积性质。

证明：设 $x \in Q(X)$，$y \in Q(Y)$，$z \in Q(Z)$ 且 $xyz = 1$。有

$$
\begin{aligned}
xyz = &\begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & \vdots & \vdots \\ x_{N1} & \dots & x_{Nn} \end{pmatrix} \pi_1 \begin{pmatrix} -x'_{11} & \dots & -x'_{1n} \\ \vdots & \vdots & \vdots \\ -x'_{N1} & \dots & -x'_{Nn} \end{pmatrix} \\
&\cdot \begin{pmatrix} y_{11} & \dots & y_{1n} \\ \vdots & \vdots & \vdots \\ y_{N1} & \dots & y_{Nn} \end{pmatrix} \pi_2 \begin{pmatrix} -y'_{11} & \dots & -y'_{1n} \\ \vdots & \vdots & \vdots \\ -y'_{N1} & \dots & -y'_{Nn} \end{pmatrix} \\
&\cdot \begin{pmatrix} z_{11} & \dots & z_{1n} \\ \vdots & \vdots & \vdots \\ z_{N1} & \dots & z_{Nn} \end{pmatrix} \pi_3 \begin{pmatrix} -z'_{11} & \dots & -z'_{1n} \\ \vdots & \vdots & \vdots \\ -z'_{N1} & \dots & -z'_{Nn} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \end{pmatrix}
\end{aligned}
$$

其中 $x_{ij}, x'_{ij} \neq 0$ 当且仅当 $P_{ij} = 1$；$y_{ij}, y'_{ij} \neq 0$ 当且仅当 $P_{ij} = 2$；$z_{ij}, z'_{ij} \neq 0$ 当且仅当 $P_{ij} = 3$。 将 π_1 和 π_2 右移到 π_3 处可得 $\pi_1 \pi_2 \pi_3 = 1$，以及

$$\begin{pmatrix} x_{11}-z'_{11} & \cdots & x_{1n}-z'_{1n} \\ \vdots & \vdots & \vdots \\ x_{N1}-z'_{N1} & \cdots & x_{Nn}-z'_{Nn} \end{pmatrix} \cdot \begin{pmatrix} y_{\pi_1(1)1}-x'_{\pi_1(1)1} & \cdots & y_{\pi_1(1)n}-x'_{\pi_1(1)n} \\ \vdots & \vdots & \vdots \\ y_{\pi_1(N)1}-x'_{\pi_1(N)1} & \cdots & y_{\pi_1(N)n}-x'_{\pi_1(N)n} \end{pmatrix} \cdot \begin{pmatrix} z_{\pi_1\pi_2(1)1}-y'_{\pi_1\pi_2(1)1} & \cdots & z_{\pi_1\pi_2(1)n}-y'_{\pi_1\pi_2(1)n} \\ \vdots & \vdots & \vdots \\ z_{\pi_1\pi_2(N)1}-y'_{\pi_1\pi_2(N)1} & \cdots & z_{\pi_1\pi_2(N)n}-y'_{\pi_1\pi_2(N)n} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \end{pmatrix}.$$

接下来证明 $\pi_1=\pi_2=\pi_3=1$。假设这不成立，则存在 $1\le i\le N$ 使得 $i,\pi_1(i),\pi_1\pi_2(i)$ 不完全相同。由于 P 是强唯一可解谜题，存在 $1\le j\le n$ 使得条件 $P_{ij}=2$，$P_{\pi_1(i)j}=3$，$P_{\pi_1\pi_2(i)j}=1$ 中恰好成立两个。注意到 $x_{ij}-z'_{ij}=0$ 当且仅当 $P_{ij}=2$，$y_{\pi_1(i)j}-x'_{\pi_1(i)j}=0$ 当且仅当 $P_{\pi_1(i)j}=3$，以及 $z_{\pi_1\pi_2(i)j}-y'_{\pi_1\pi_2(i)j}=0$ 当且仅当 $P_{\pi_1\pi_2(i)j}=1$。于是 $x_{ij}-z'_{ij}+y_{\pi_1(i)j}-x'_{\pi_1(i)j}+z_{\pi_1\pi_2(i)j}-y'_{\pi_1\pi_2(i)j}\neq 0$，矛盾。故 $\pi_1=\pi_2=\pi_3=1$。于是 $x=x_{ij}-x'_{ij}$，$y=y_{ij}-y'_{ij}$，$z=z_{ij}-z'_{ij}$，并且 $xyz=\mathbf{id}$。注意到 $x_{ij}-x'_{ij}$，$y_{ij}-y'_{ij}$，$z_{ij}-z'_{ij}$ 不为零仅当 P_{ij} 分别等于 $1,2,3$，而这是互斥的。故只可能有 $x_{ij}-x'_{ij}=y_{ij}-y'_{ij}=z_{ij}-z'_{ij}=0$，$i=1,\dots,N$，$j=1,\dots,n$。即 $x=y=z=\mathbf{id}$。证毕。

推论 7.1 ([CKSU05])：
设强唯一可解谜题的容量为 C。对任意正整数 $m\ge 3$，成立 $\omega\le 3(\log_2 m-\log_2 C)/\log_2(m-1)$。

证明：由定理 7.1，上面构造的有限群 G 实现了 $\langle |X|,|Y|,|Z|\rangle$。由推论 5.1，成立 $(|X||Y||Z|)^{\omega/3}\le d_{\max}^{\omega-2}|G|$。这里 $d_{\max}\le \left[G:(\mathbb{Z}_m)^{Nn}\right]=|\mathbb{S}_N|=N!$，$|G|=m^{Nn}N!$，$|X||Y||Z|=(m-1)^{Nn}(N!)^3$，并且 N 可取到 $(C-o(1))^n$。解得 $\omega\le 3(\log_2 m-\log_2(C-o(1)))/\log_2(m-1)$。令 $n\to\infty$ 得 $\omega\le 3(\log_2 m-\log_2 C)/\log_2(m-1)$。证毕。

一种构造强唯一可解谜题的方式如下：对正整数 n（出于方便假设 n 是 4 的倍数），$\{1,2\}^{n/2}$ 中含有相同数量 1 和 2 的 $(n/2)$-元组共有 $\binom{n/2}{n/4}$ 个，记其集合为 S_1。同理 $\{2,3\}^{n/2}$ 中含有相同数量 2 和 3 的 $(n/2)$-元组共有 $\binom{n/2}{n/4}$ 个，记其集合为 S_2。以任意顺序排列 S_1 及 S_2 中的元素。构造的强唯一可解谜题 P共有 $N=\binom{n/2}{n/4}=(\sqrt{2}-o(1))^n$ 行，其中第 i 行 为 $(P_{i1},\dots,P_{in})$。这里

$(P_{i1},\dots,P_{i(n/2)})$ 和 $(P_{i(n/2+1)},\dots,P_{in})$ 分别为 S_1 和 S_2 中的第 i 个元素。为证明 P是强唯一可解谜题，考虑任意不完全相同的 $1\le i_1,i_2,i_3\le N$，并且由对称性可假设 $i_1\ne i_2$，于是 $(P_{i_11},\dots,P_{i_1(n/2)})\ne(P_{i_21},\dots,P_{i_2(n/2)})$。由于二者含有相同数量的 1 和 2，存在 $1\le j\le n/2$ 使得 $P_{i_1j}=1$，$P_{i_2j}=2$，并且 $P_{i_3j}\in\{1,2\}\not\ni 3$。
于是 P是强唯一可解谜题。这给出了强唯一可解谜题的容量下界 $C\ge\sqrt{2}$。

上面构造的 P的每一列仅出现 $\{1,2,3\}$ 中的至多两个元素。对于满足这样性质的构造，我们有如下引理：

引理 7.1：
若 P是唯一可解谜题，且每一列仅出现 $\{1,2,3\}$ 中的至多两个元素，则 P是强唯一可解谜题。

证明：对任意不完全相同的 $1\le i_1,i_2,i_3\le N$，存在 $1\le j\le n$，使得三个条件 $P_{i_1j}=1$，$P_{i_2j}=2$，$P_{i_3j}=3$ 中至少成立两个。但是第 j 列仅出现 $\{1,2,3\}$ 中的至多两个元素。故前述三个条件恰好成立两个。故 P是强唯一可解谜题。证毕。

一种更好的构造方式如下：对正整数 n（出于方便假设 n 是 6 的倍数），令 $m=\binom{n/3}{n/6}$。$\{1,2\}^{n/3}$ 中含有相同数量 1 和 2 的 $(n/2)$-元组共有 m 个，记其集合为 S_1。同理 $\{2,3\}^{n/2}$ 中含有相同数量 2 和 3 的 $(n/2)$-元组共有 m 个，记其集合为 S_2，且 $\{1,3\}^{n/2}$ 中含有相同数量 1 和 3 的 $(n/2)$-元组共有 m 个，记其集合为 S_3。以任意顺序排列 S_1，S_2 以及 S_3 中的元素。考虑定理 6.2 证明中构造的三角阵 Δ_m。构造的强唯一可解谜题 P共有 $N=|\Delta_m|=\left(2^{2/3}-o(1)\right)^n$ 行，并以 Δ_m 中元素为行索引，其中第 (s,t,u) 行 为 $(P_{(stu)1},\dots,P_{(stu)n})$。这里 $(P_{(stu)1},\dots,P_{(stu)(n/3)})$，$(P_{(stu)(n/3+1)},\dots,P_{(stu)(2n/3)})$ 和 $(P_{(stu)(2n/3+1)},\dots,P_{(stu)n})$ 分别为 S_1，S_2 和 S_3 中的第 s，t，u 个元素。

定理 7.2：
上面构造的 P是强唯一可解谜题。

证明：注意到 P的每一列仅出现 $\{1,2,3\}$ 中的至多两个元素，故由引理 7.1，只需证明 P是唯一可解谜题。等价地，考虑作用于 Δ_m 上的置换 $\pi_1,\pi_2,\pi_3\in\mathbb{S}_m$，使得对任意 $(s,t,u)\in\Delta_m$，集合 $S_{\pi_1((s,t,u))1},S_{\pi_2((s,t,u))2},S_{\pi_3((s,t,u))3}$ 都构成了 $\{1,\dots,n\}$ 的一个划分，其中 $S_{(s,t,u)k}=\{1\le j\le n:P_{(s,t,u)j}=k\}$，$k=1,2,3$。只需证明 $\pi_1=\pi_2=\pi_3$。接下来首先证明对任意 $u\in\Delta_m$，都有 u 和 $\pi_1\pi_2^{-1}(u)$ 的第一个坐标分量相同。否则令 $v=\pi_2^{-1}(u)$，有 $(P_{\pi_1(v)1},\dots,P_{\pi_1(v)(n/3)})\ne(P_{\pi_2(v)1},\dots,P_{\pi_2(v)(n/3)})$。由于二者含有相同数量的 1 和 2，存在 $1\le j\le n/3$ 使得 $P_{\pi_1(v)j}=1$，$P_{\pi_2(v)j}=2$。这使得 $j\in S_{\pi_1(v)1}\cap S_{\pi_2(v)2}$。矛盾。故 $\pi_1\pi_2^{-1}$ 保持 Δ_m 中元素的第一个分量不变。类似地可证明 $\pi_2\pi_3^{-1}$ 保持 Δ_m 中元素的第二个分量不变，以及 $\pi_3\pi_1^{-1}$ 保持 Δ_m 中元素的第三个分量不变。注意到 $(\pi_1\pi_2^{-1})(\pi_2\pi_3^{-1})(\pi_3\pi_1^{-1})=1$。由定理 5.3 的证明，分别保持三个分量不变的置换构成的子群在 $\mathbb{S}_m$ 中满足三元组乘积性质。故

$\pi_1\pi_2^{-1}=\pi_2\pi_3^{-1}=\pi_3\pi_1^{-1}=1$。故 $\pi_1=\pi_2=\pi_3$。证毕。

由定理 7.2 可知强唯一可解谜题的容量 $C\geq 2^{2/3}$。应用推论 7.1 并令 $m=6$，可得 $\omega\leq 3(\log_2 6-2/3)/\log_2 5=2.478\ldots$。这样就重新证明了定理 6.3。

另一方面可以给出唯一可解谜题的容量上界：

定理 7.3：
唯一可解谜题的容量 $C\leq (27/4)^{1/3}$。

证明：考虑一个 $N\times n$ 的唯一可解谜题 P。首先证明对 $n_1,n_2,n_3\in\mathbb{N}$ 并且 $n_1+n_2+n_3=n$，P中 $1,2,3$ 分别出现 n_1,n_2,n_3 次的行至多有 $\min_{1\leq i\leq 3}\binom{n}{n_i}$ 个。考虑所有这样的行。易证对任意两行 $1\leq i,j\leq N$，都有 $S_{i1}\neq S_{j1}$。否则定义 π_1 为 i 和 j 的对换，$\pi_2=\pi_3=1$，则对于任意 $1\leq k\leq N$，集合 $S_{\pi_1(k)1},S_{\pi_2(k)2},S_{\pi_3(k)3}$ 都构成了 $\{1,\ldots,n\}$ 的一个划分，且有 $\pi_1\neq\pi_2=\pi_3$，与 P是唯一可解谜题矛盾。但共有 $\binom{n}{n_1}$ 种可能的集合 S_{i1}，故至多有 $\binom{n}{n_1}$ 个这样的行。类似地考虑数字 2 和 3 可知至多有 $\min_{1\leq i\leq 3}\binom{n}{n_i}$ 个这样的行。故

$$N\leq\sum_{n_1+n_2+n_3=n}\min_{1\leq i\leq 3}\binom{n}{n_i}\leq\binom{n+2}{2}\binom{n}{n/3}=((27/4)^{1/3}-o(1))^n.$$

故唯一可解谜题的容量 $C\leq (27/4)^{1/3}$。证毕。

这自然也是强唯一可解谜题的容量上界。下面猜想这一上界是可以达到的：

猜想 7.1 ([CKSU05])：
强唯一可解谜题的容量 $C=(27/4)^{1/3}$。

若猜想 7.1 成立，则结合推论 7.1 并令 $m=3$，可得 $\omega\leq 3\log_2 3-\log_2(27/4)=2$。

另一方面对于唯一可解谜题来说，这一上界是可以达到的：

定理 7.4 ([CW90, CKSU05])：
唯一可解谜题的容量 $C=(27/4)^{1/3}$。

为证明定理 7.4，首先给出如下引理：

引理 7.2 ([SS42])：

对正整数 N，存在集合 $S \subseteq \{1,\dots,N\}$ 使得 $|S| = N^{1-o_N(1)}$，且 S 中不存在不完全相同的三个数 x,y,z 满足 $x+y=2z$，即不包含长度为 3 的非平凡等差数列。

证明：对正整数 n，定义

$$T = \{t=(t_1,\dots,t_n) \in (\mathbb{Z}_{10n})^n : t_1,\dots,t_n \text{ 是 } 1,\dots,n \text{ 的排列}\}$$

则 $|T| = n!$。设 $x,y,z \in T$满足 $x+y=2z$。对 $1 \le j \le n$，存在 $1 \le i_j \le n$ 使得 $z_{i_j} = j$。成立 $x_{i_n} + y_{i_n} = 2z_{i_n} = 2n$。这样只可能有 $x_{i_n} = y_{i_n} = n = z_{i_n}$。依此类推可证明 $x_{i_j} = y_{i_j} = z_{i_j} = j$ 对任意 $1 \le j \le n$ 成立。故 $x=y=z$。接下来选取 $N = (10n)^n$ 并选取 $\{1,\dots,N\}$ 的子集使之具备同样的性质：定义映射 $\phi : T \to \{1,\dots,N\}$ 使得 $\phi(t) = \sum_{i=1}^n t_{i-1}(10n)^{i-1}$，即若 t_i 代表一个正整数以 $10n$ 为基底的第 i 位（自低到高），则 $\phi(t)$ 代表这个数的值。令 $S = \phi(T)$。显然 ϕ 是双射，故 $|S| = |T| = n!$。设 $x,y,z \in S$ 满足 $x+y=2z$，则由于基底 $10n$ 足够大而 x,y 以 $10n$ 为基底的每一位数字最多为 n，可知 $x+y$ 不出现进位。这说明 $\phi^{-1}(x) + \phi^{-1}(y) = \phi^{-1}(z)$。由 T的性质知 $\phi^{-1}(x) = \phi^{-1}(y) = \phi^{-1}(z)$。故 $x=y=z$。这说明 S 中所有等差数列都是平凡的（公差为零）。这里 $|S| = n! = N^{1-o(1)}$。证毕。

证明（定理 7.4）：下面构造一个 $N \times n$ 的唯一可解谜题。取素数 m 并以均匀分布独立随机地取 $w_1,\dots,w_{n+2} \in \mathbb{F}_m$（这里 $\mathbb{F}_m$ 即为素域 $\mathbf{GF}(m)$）。
定义哈希函数 (hash function) $h_1,h_2,h_3 : \{0,1\}^n \to \mathbb{F}_m$ 如下：

$$\begin{aligned} h_1(a) &= \sum_{i=1}^n w_i a_i + w_{n+1} \\ h_2(b) &= \sum_{i=1}^n w_i b_i + w_{n+2} \\ h_3(c) &= \frac{1}{2}\left(\sum_{i=1}^n w_i(1-c_i) + w_{n+1} + w_{n+2}\right). \end{aligned}$$

易证如下事实：
1. 设 $h,h' \in \{h_1,h_2,h_3\}$，$a,a',b \in \{0,1\}^n$，其中 $a \neq a'$，则 $h(a), h(a'), h'(b)$ 相互独立，且为 $\mathbb{F}_m$ 上的均匀分布。
2. 对于 $a,b,c \in \{0,1\}^n$，若 $a+b+c = (1,\dots,1)$，则 $h_1(a) + h_2(b) = 2h_3(c)$。
定义

$$S = \left\{(a,b,c) \in \left(\{0,1\}^n\right)^3 : \begin{array}{c} a+b+c=(1,\dots,1), \\ |\mathrm{supp}(a)| = |\mathrm{supp}(b)| = |\mathrm{supp}(c)| = n/3 \end{array}\right\}$$

其中 $\mathrm{supp}(u)=\{1\le i\le n:u_i=1\}$。由引理 7.2，存在集合 $Q\subseteq\{1,\dots,m/2-1\}$ 使得 $|Q|=(m/2)^{1-o_m(1)}=m^{1-o_m(1)}$，且 Q 不包含长度为 3 的非平凡等差数列。注意到 Q 中任意元素 x,y 满足 $x+y=(x+y)\bmod m$。将 Q 看作 $\mathbb{F}_m$ 的子集。则 Q 中不包含不完全相同的三个数 x,y,z 使得 $x+y=2z$ 在 $\mathbb{F}_m$ 上成立。定义 $S'=\{(a,b,c)\in S:h_1(a),h_2(b),h_3(c)\in Q\}$。定义 S' 的子集 T_1,T_2,T_3 如下：

$$
\begin{aligned}
T_1&=\{(a,b,c)\in S':\exists\,(a,b',c')\in S',b\neq b'\}\\
T_2&=\{(a,b,c)\in S':\exists\,(a',b,c')\in S',a\neq a'\}\\
T_3&=\{(a,b,c)\in S':\exists\,(a',b',c)\in S',a\neq a'\}.
\end{aligned}
$$

令 $U=S'\setminus(T_1\cup T_2\cup T_3)$。令 $N=|U|$ 并构造矩阵 $N\times n$ 矩阵 P：P以 U 中元素为行索引。对 $(a,b,c)\in U$，P中第 (a,b,c) 行 $(P_{(a,b,c)1},\dots,P_{(a,b,c)n})$ 满足

$$
P_{(a,b,c)i}=\begin{cases}1, & i\in\mathrm{supp}(a),\\ 2, & i\in\mathrm{supp}(b),\\ 3, & i\in\mathrm{supp}(c).\end{cases}
$$

注意到对于 $(a,b,c)\in U$，有 $a+b+c=(1,\dots,1)$，因此 $\mathrm{supp}(a),\mathrm{supp}(b),\mathrm{supp}(c)$ 构成了 $\{1,\dots,n\}$ 的划分。故 P是良好定义的。 下面证明 P是唯一可解谜题。考虑任意 $(a,b,c),(a',b',c'),(a'',b'',c'')\in U$使得 $a+b'+c''=(1,\dots,1)$，只需证明 $(a,b,c)=(a',b',c')=(a'',b'',c'')$。注意到因为 U 的定义中删去了 T_1 中的元素，有 $(a,b',c'')=(a,b,c)$。类似地有 $(a,b',c'')=(a',b',c')$ 和 $(a,b',c'')=(a'',b'',c'')$。故 $(a,b,c)=(a',b',c')=(a'',b'',c'')$。这说明 P是是唯一可解谜题。下面分析 N的大小。注意到对任意 $(a,b,c)\in S$，有 $h_1(a)+h_2(b)=2h_3(c)$。于是 $h_1(a)\in Q$，$h_2(b)\in Q$，$h_3(c)\in Q$ 同时成立当且仅当 $h_1(a)=h_2(b)=h_3(c)\in Q$ 当且仅当 $h_1(a)=h_2(b)\in Q$。于是有

$$
\begin{aligned}
\mathbb{E}\big[|S'|\big]&=\sum_{(a,b,c)\in S}\Pr[h_1(a)\in Q\ \wedge\ h_2(b)\in Q\ \wedge\ h_3(c)\in Q]\\
&=\sum_{(a,b,c)\in S}\sum_{q\in Q}\Pr[h_1(a)=h_2(b)=q]\\
&=|S||Q|/m^2.
\end{aligned}
$$

接下来有

—

$$
\begin{aligned}
\mathbb{E}[|T_1|] &= \sum_{(a,b,c)\in S} \Pr\left[(a,b,c)\in S' \ \wedge\ \exists\,(a,b',c')\in S', b\neq b'\right] \\
&\le \sum_{(a,b,c),(a,b',c')\in S, b\neq b'} \Pr\left[(a,b,c)\in S' \ \wedge\ (a,b',c')\in S'\right] \\
&= \sum_{(a,b,c),(a,b',c')\in S, b\neq b'} \Pr[h_1(a),h_2(b),h_3(c),h_2(b'),h_3(c')\in Q] \\
&= \sum_{(a,b,c),(a,b',c')\in S, b\neq b'} \sum_{q\in Q} \Pr[h_1(a)=h_2(b)=h_2(b')=q] \\
&\le \binom{2n/3}{n/3} |S||Q|/m^3.
\end{aligned}
$$

类似地可证明 $|T_2|, |T_3| \le \binom{2n/3}{n/3}|S||Q|/m^3$。于是

$$
\begin{aligned}
\mathbb{E}[|U|] &\ge \frac{|S||Q|}{m^2} - 3\binom{2n/3}{n/3}\frac{|S||Q|}{m^3} \\
&= \frac{|S||Q|}{m^2}\left(1 - \frac{3\binom{2n/3}{n/3}}{m}\right).
\end{aligned}
$$

选择 $m = O\left(\binom{2n/3}{n/3}\right)$ 使得 $1 - \frac{3\binom{2n/3}{n/3}}{m} \ge 1/2$。则

$$
\mathbb{E}[|U|] \ge \frac{|S||Q|}{2m^2} \ge \frac{\binom{n}{n/3,n/3,n/3} m^{1-o(1)}}{m^2} = \left((27/4)^{1/3} - o(1)\right)^n.
$$

故存在 $w_1,\ldots,w_{n+2}$ 使得 $N = |U| \ge \mathbb{E}[|U|] = (27/4 - o(1))^n$。
由此可得唯一可解谜题的容量 $C = (27/4)^{1/3}$。证毕。

唯一可解谜题可以用来得到矩阵乘法的快速算法：对正整数 m，仍令 $G = (\mathbb{Z}_m)^{Nn} \rtimes \mathbb{S}_N$，并用 $N\times n$ 矩阵表示 $(\mathbb{Z}_m)^{Nn}$ 中的元素。$\mathbb{S}_N$ 在 $(\mathbb{Z}_m)^{Nn}$ 上的作用与之前相同。令 $H = \mathbb{Z}_m \setminus \{0,1\}$。
对于 $N\times n$ 矩阵 P，定义 $X, Y, Z \subseteq G$ 如下：

$$
\begin{aligned}
X &= \left\{ \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & \vdots & \vdots \\ x_{N1} & \dots & x_{Nn} \end{pmatrix} \pi : \pi \in \mathbb{S}_m, x_{ij} = \begin{cases} 0 & P_{ij} = 1 \\ 1 & P_{ij} = 2 \\ \in H & P_{ij} = 3 \end{cases} \right\} \\
Y &= \left\{ \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & \vdots & \vdots \\ x_{N1} & \dots & x_{Nn} \end{pmatrix} \pi : \pi \in \mathbb{S}_m, x_{ij} = \begin{cases} \in -H & P_{ij} = 1 \\ 0 & P_{ij} = 2 \\ 0 & P_{ij} = 3 \end{cases} \right\} \\
Z &= \left\{ \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & \vdots & \vdots \\ x_{N1} & \dots & x_{Nn} \end{pmatrix} \pi : \pi \in \mathbb{S}_m, x_{ij} = \begin{cases} 0 & P_{ij} = 1 \\ \in H & P_{ij} = 2 \\ 0 & P_{ij} = 3 \end{cases} \right\}.
\end{aligned}
$$

定理 7.5：
若 P为唯一可解谜题，则如上定义的 (X, Y, Z) 在 G 中满足三元组乘积性质。

证明：设 $x \in Q(X)$，$y \in Q(Y)$，$z \in Q(Z)$ 且 $xyz = 1$。有

$$
\begin{aligned}
xyz = &\begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & \vdots & \vdots \\ x_{N1} & \dots & x_{Nn} \end{pmatrix} \pi_1 \begin{pmatrix} -x'_{11} & \dots & -x'_{1n} \\ \vdots & \vdots & \vdots \\ -x'_{N1} & \dots & -x'_{Nn} \end{pmatrix} \\
&\cdot \begin{pmatrix} y_{11} & \dots & y_{1n} \\ \vdots & \vdots & \vdots \\ y_{N1} & \dots & y_{Nn} \end{pmatrix} \pi_2 \begin{pmatrix} -y'_{11} & \dots & -y'_{1n} \\ \vdots & \vdots & \vdots \\ -y'_{N1} & \dots & -y'_{Nn} \end{pmatrix} \\
&\cdot \begin{pmatrix} z_{11} & \dots & z_{1n} \\ \vdots & \vdots & \vdots \\ z_{N1} & \dots & z_{Nn} \end{pmatrix} \pi_3 \begin{pmatrix} -z'_{11} & \dots & -z'_{1n} \\ \vdots & \vdots & \vdots \\ -z'_{N1} & \dots & -z'_{Nn} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \end{pmatrix}.
\end{aligned}
$$

将 π_1 和 π_2 右移到 π_3 处可得 $\pi_1 \pi_2 \pi_3 = 1$，以及

$$\begin{pmatrix} x_{11}-z'_{11} & \cdots & x_{1n}-z'_{1n} \\ \vdots & \vdots & \vdots \\ x_{N1}-z'_{N1} & \cdots & x_{Nn}-z'_{Nn} \end{pmatrix}$$
$$\cdot \begin{pmatrix} y_{\pi_1(1)1}-x'_{\pi_1(1)1} & \cdots & y_{\pi_1(1)n}-x'_{\pi_1(1)n} \\ \vdots & \vdots & \vdots \\ y_{\pi_1(N)1}-x'_{\pi_1(N)1} & \cdots & y_{\pi_1(N)n}-x'_{\pi_1(N)n} \end{pmatrix}$$
$$\cdot \begin{pmatrix} z_{\pi_1\pi_2(1)1}-y'_{\pi_1\pi_2(1)1} & \cdots & z_{\pi_1\pi_2(1)n}-y'_{\pi_1\pi_2(1)n} \\ \vdots & \vdots & \vdots \\ z_{\pi_1\pi_2(N)1}-y'_{\pi_1\pi_2(N)1} & \cdots & z_{\pi_1\pi_2(N)n}-y'_{\pi_1\pi_2(N)n} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \end{pmatrix}.$$

接下来证明 $\pi_1=\pi_2=\pi_3=1$。假设这不成立，则存在 $1\le i\le N$ 使得 $i,\pi_1(i),\pi_1\pi_2(i)$ 不完全相同。由于 P 是唯一可解谜题，存在 $1\le j\le n$ 使得条件 $P_{ij}=1$，$P_{\pi_1(i)j}=2$，$P_{\pi_1\pi_2(i)j}=3$ 中成立至少两个。有如下几种情况：

1. $P_{ij}=1$，$P_{\pi_1(i)j}=2$，$P_{\pi_1\pi_2(i)j}=3$。此时有

$$x_{ij}-z'_{ij}=0,\ y_{\pi_1(i)j}-x'_{\pi_1(i)j}=-1,\ z_{\pi_1\pi_2(i)j}-y'_{\pi_1\pi_2(i)j}=0.$$

于是 $x_{ij}-z'_{ij}+y_{\pi_1(i)j}-x'_{\pi_1(i)j}+z_{\pi_1\pi_2(i)j}-y'_{\pi_1\pi_2(i)j}=-1\neq 0$，矛盾。

2. $P_{ij}=1$，$P_{\pi_1(i)j}=2$，$P_{\pi_1\pi_2(i)j}\neq 3$。此时有

$$x_{ij}-z'_{ij}=0,\ y_{\pi_1(i)j}-x'_{\pi_1(i)j}=-1,\ z_{\pi_1\pi_2(i)j}-y'_{\pi_1\pi_2(i)j}\in H.$$

于是 $x_{ij}-z'_{ij}+y_{\pi_1(i)j}-x'_{\pi_1(i)j}+z_{\pi_1\pi_2(i)j}-y'_{\pi_1\pi_2(i)j}\in H-1\not\ni 0$，矛盾。

3. $P_{ij}=1$，$P_{\pi_1(i)j}\neq 2$，$P_{\pi_1\pi_2(i)j}=3$。此时有

$$x_{ij}-z'_{ij}=0,\ y_{\pi_1(i)j}-x'_{\pi_1(i)j}\in -H,\ z_{\pi_1\pi_2(i)j}-y'_{\pi_1\pi_2(i)j}=0.$$

于是 $x_{ij}-z'_{ij}+y_{\pi_1(i)j}-x'_{\pi_1(i)j}+z_{\pi_1\pi_2(i)j}-y'_{\pi_1\pi_2(i)j}\in -H\not\ni 0$，矛盾。

4. $P_{ij}\neq 1$，$P_{\pi_1(i)j}=2$，$P_{\pi_1\pi_2(i)j}=3$。此时有

$$x_{ij}-z'_{ij}\in H\text{ 或 }1-H,\ y_{\pi_1(i)j}-x'_{\pi_1(i)j}=-1,\ z_{\pi_1\pi_2(i)j}-y'_{\pi_1\pi_2(i)j}=0.$$

于是 $x_{ij}-z'_{ij}+y_{\pi_1(i)j}-x'_{\pi_1(i)j}+z_{\pi_1\pi_2(i)j}-y'_{\pi_1\pi_2(i)j}\in (H-1)\cup(-H)\not\ni 0$，矛盾。

上述几种情况都推出矛盾。故 $\pi_1=\pi_2=\pi_3=1$。于是 $x=x_{ij}-x'_{ij}$，$y=y_{ij}-y'_{ij}$，

$z = z_{ij} - z'_{ij}$，并且 $xyz = \mathbf{id}$。注意到 $x_{ij} - x'_{ij}$，$y_{ij} - y'_{ij}$，$z_{ij} - z'_{ij}$ 不为零仅当 P_{ij} 分别等于 $3, 1, 2$，而这是互斥的。故只可能有 $x_{ij} - x'_{ij} = y_{ij} - y'_{ij} = z_{ij} - z'_{ij} = 0$，$i = 1, \ldots, N$，$j = 1, \ldots, n$。即 $x = y = z = \mathbf{id}$。证毕。

类似于推论 7.1，有如下结论：

推论 7.2 ([CKSU05])：
设唯一可解谜题的容量为 C。对任意正整数 $m \geq 3$，成立
$\omega \leq 3(\log_2 m - \log_2 C)/\log_2(m-2)$。

证明：由定理 7.1，上面构造的有限群 G 实现了 $\langle |X|, |Y|, |Z| \rangle$。由推论 5.1，成立
$(|X||Y||Z|)^{\omega/3} \leq d_{\max}^{\omega-2}|G|$。这里 $d_{\max} \leq \left[G : (\mathbb{Z}_m)^{Nn}\right] = |\mathbb{S}_N| = N!$，$|G| = m^{Nn}N!$，
$|X||Y||Z| = (m-2)^{Nn}(N!)^3$，并且 N 可取到 $(C - o(1))^n$。解得
$\omega \leq 3(\log_2 m - \log_2(C - o(1)))/\log_2(m-2)$。令 $n \to \infty$ 得
$\omega \leq 3(\log_2 m - \log_2 C)/\log_2(m-2)$。证毕。

注意分母为 $\log_2(m-2)$，而非推论 7.1 中的 $\log_2(m-1)$。在这一点上推论 7.2 比推论 7.1 稍弱，但它的应用只需要唯一可解谜题而非强唯一可解谜题。由定理 7.4，唯一可解谜题的容量为 $(27/4)^{1/3}$。应用推论 7.2 并令 $m = 10$ 可得：

定理 7.6 ([CW90, CKSU05])：
$\omega \leq (3\log_2 10 - \log_2(27/4))/\log_2 8 = 2.403\ldots$

（八）Coppersmith-Winograd 算法

对正整数 q，定义张量 T，其对应的多项式为
$p(X, Y, Z) = \sum_{i=1}^{q}(X_0 Y_i Z_i + X_i Y_0 Z_i + X_i Y_i Z_0)$。对于 $\epsilon > 0$，定义张量 $T(\epsilon)$，其对应的多项式为

$$\begin{aligned}
&\left(\sum_{i=1}^{q} \epsilon^{-2}(X_0 + \epsilon X_i)(Y_0 + \epsilon Y_i)(Z_0 + \epsilon Z_i)\right) \\
&-\epsilon^{-3}\left(X_0 + \epsilon^2 \sum_{i=1}^{q} X_i\right)\left(Y_0 + \epsilon^2 \sum_{i=1}^{q} Y_i\right)\left(Z_0 + \epsilon^2 \sum_{i=1}^{q} Z_i\right) \\
&+\left(\epsilon^{-3} - q\epsilon^{-2}\right) X_0 Y_0 Z_0
\end{aligned}$$

则 $\lim_{\epsilon \to 0} T(\epsilon) = T$ 且 $R(T(\epsilon)) \leq q + 2$。故 $\underline{R}(T) \leq q + 2$。

出于方便采用如下的记号：将变量 $X_0,\dots,X_q$ 分成两块，其中块 $[0]$ 包含 X_0，块 $[1]$ 包含 $X_1,\dots,X_q$。对 Y和 Z 作同样的处理。令 $X^{[I_1]}Y^{[I_2]}Z^{[I_3]}$ 包含 $p(X,Y,Z)$ 中所有单项式 $X_{j_1}Y_{j_2}Z_{j_3}$ 之和，其中 j_1,j_2,j_3 分别属于块 $[I_1],[I_2],[I_3]$。即

$$\begin{aligned}X^{[0]}Y^{[1]}Z^{[1]}&=\sum_{i=1}^{q}X_0Y_iZ_i,\\X^{[1]}Y^{[0]}Z^{[1]}&=\sum_{i=1}^{q}X_iY_0Z_i,\\X^{[1]}Y^{[1]}Z^{[0]}&=\sum_{i=1}^{q}X_iY_iZ_0,\end{aligned}$$

其对应的张量分别为 $\langle 1,1,q\rangle$，$\langle 1,q,1\rangle$，$\langle q,1,1\rangle$。并且有 $p(X,Y,Z)=X^{[0]}Y^{[1]}Z^{[1]}+X^{[1]}Y^{[0]}Z^{[1]}+X^{[1]}Y^{[1]}Z^{[0]}$。下面考虑张量 $T^{\otimes N}$（N为 3 的倍数），并设其对应的多项式为 $p'(X,Y,Z)$，其中 $X=\{X_{i_1,\dots,i_N}:0\le i_t\le q\}$，对 Y,Z 同理。称 $X_{j_1,\dots,j_N}$ 属于块 $[I_1,\dots,I_N]$，若 X_{j_t} 属于块 $[I_t]$。对 Y和 Z 作同样的处理。令 $X^{[I_1,\dots,I_N]}Y^{[I'_N,\dots,I'_N]}Z^{[I''_N,\dots,I''_N]}$ 包含 $p'(X,Y,Z)$ 中所有单项式 $X_{j_1,\dots,j_N}Y_{j'_1,\dots,j'_N}Z_{j''_1,\dots,j''_N}$ 之和，其中 $X_{j_1,\dots,j_N},Y_{j'_1,\dots,j'_N},Z_{j''_1,\dots,j''_N}$ 分别属于块 $[I_1,\dots,I_N],[I'_1,\dots,I'_N],[I''_1,\dots,I''_N]$。并且有

$$p'(X,Y,Z)=\sum X^{[I_1,\dots,I_N]}Y^{[I'_N,\dots,I'_N]}Z^{[I''_N,\dots,I''_N]}.$$

对任意变量 $X_{j_1,\dots,j_N}$，设其属于块 $[I_1,\dots,I_N]$ 且 $I_1,\dots,I_N$ 中 0 的数量不为 $N/3$（即 1 的数量不为 $2N/3$），则删除 $p'(X,Y,Z)$ 中所有含变量 $X^{j_1,\dots,j_N}$ 的项。类似地处理 Y和 Z。设得到的多项式为 p''，对应的张量为 T'。则 $\underline{R}(T')\le\underline{R}\left(T^{\otimes N}\right)\le(q+2)^N$。这里 p'' 为形如 $X^{[I_1,\dots,I_N]}Y^{[I'_N,\dots,I'_N]}Z^{[I''_N,\dots,I''_N]}$ 的 $M=\binom{N}{N/3,N/3,N/3}$ 项之和，其中每一项恰为 $\left(\langle 1,1,q\rangle\otimes\langle 1,q,1\rangle\otimes\langle q,1,1\rangle\right)^{\otimes N/3}=\langle q,q,q\rangle^{\otimes N/3}$。若项与项之间是独立的（即不同的项不包含相同的变量），则 $T''=\left(\langle q,q,q\rangle^{\otimes N/3}\right)^{\oplus M}$，并可利用渐近和不等式（定理 4.1）得到 ω 的上界。但这并不成立，例如 $N=3$ 时 $X^{[0,1,1]}$ 包含在不同的两项 $X^{[0,1,1]}Y^{[1,1,0]}X^{[1,0,1]}$ 和 $X^{[0,1,1]}Y^{[1,0,1]}X^{[1,1,0]}$ 中。接下来进一步删除一些变量以确保独立性：令 $S=\left\{A,B,C\in\{0,1\}^N:A,B,C\text{ 含有 }N/3\text{ 个 }0\right\}$。有 $|S|=\binom{N}{N/3,N/3,N/3}$。取 S 中尽量大的子集 S' 使得对任意 $(A,B,C),(A',B',C'),(A'',B'',C'')\in S'$，$A+B'+C''=(2,\dots,2)$ 仅当 $(A,B,C)=(A',B',C')=(A'',B'',C'')$。利用定理 7.4 证明中的构造，可得 $|S'|\ge\left((27/4)^{1/3}-o(1)\right)^N$。删除 p'' 中含变量 $X_{i_1,\dots,i_N}$ 的项，如果 $i_1,\dots,i_N$ 不属于任何块 A 使得存在 $(A,B,C)\in S'$。类似地删除 p'' 中含变量 $Y_{i'_1,\dots,i'_N}$ 的项，如果 $i'_1,\dots,i'_N$ 不属于任何块 B 使得存在 $(A,B,C)\in S'$。最后删除 p'' 中含变量 $Z_{i''_1,\dots,i''_N}$ 的项，

如果 $i''_1,\dots,i''_N$ 不属于任何块 C 使得存在 $(A,B,C)\in S'$。设得到的多项式为 P，其对应的张量为 T'。有 $P=\sum_{(A,B,C)\in S'}X^{[A]}Y^{[B]}Z^{[C]}$，且项与项之间是独立的（否则，不失一般性假设 $(A,B,C),(A,B',C'')\in S'$，且 $(A,B,C)\neq(A,B',C'')$，但 $A+B'+C''=(2,\dots,2)$，矛盾）。于是 $T''=\left(\langle q,q,q\rangle^{\otimes N/3}\right)^{\oplus|S'|}$ 并且 $\underline{R}(T'')\leq\underline{R}(T')\leq(q+2)^N$。由渐近和不等式，有 $|S'|q^{N\omega/3}\leq(q+2)^N$，其中 $|S'|\geq((27/4)^{1/3}-o(1))^N$。令 $N\to\infty$ 并令 $q=8$，得 $\omega\leq(3\log_2 10-\log_2(27/4))/\log_2 8=2.403\dots$。这样就重新证明了定理 7.6。

对上述结果可作如下改进：引入变量 X_{q+1} 并设块 $[2]$ 包含 X_{q+1}。对 Y和 Z 作同样的处理。定义张量 T，其对应的多项式为

$$\begin{aligned}p(X,Y,Z)=\sum_{i=1}^{q}(&X_0Y_iZ_i+X_iY_0Z_i+X_iY_iZ_0)\\&+X_0Y_0Z_{q+1}+X_0Y_{q+1}Z_0+X_{q+1}Y_0Z_0.\end{aligned}$$

对于 $\epsilon>0$，定义张量 $T(\epsilon)$，其对应的多项式为

$$\begin{aligned}&\left(\sum_{i=1}^{q}\epsilon^{-2}(X_0+\epsilon X_i)(Y_0+\epsilon Y_i)(Z_0+\epsilon Z_i)\right)\\&-\epsilon^{-3}\left(X_0+\epsilon^2\sum_{i=1}^{q}X_i\right)\left(Y_0+\epsilon^2\sum_{i=1}^{q}Y_i\right)\left(Z_0+\epsilon^2\sum_{i=1}^{q}Z_i\right)\\&+\left(\epsilon^{-3}-q\epsilon^{-2}\right)(X_0-q\epsilon^3X_{q+1})(Y_0-q\epsilon^3Y_{q+1})(Z_0-q\epsilon^3Z_{q+1})\end{aligned}$$

则 $\lim_{\epsilon\to0}T(\epsilon)=T$ 且 $R(T(\epsilon))\leq q+2$。故 $\underline{R}(T)\leq q+2$。沿用之前的记号，则有

$$\begin{aligned}p(X,Y,Z)=&X^{[0]}Y^{[1]}Z^{[1]}+X^{[1]}Y^{[0]}Z^{[1]}+X^{[1]}Y^{[1]}Z^{[0]}\\&+X^{[0]}Y^{[0]}Z^{[2]}+X^{[0]}Y^{[2]}Z^{[0]}+X^{[2]}Y^{[0]}Z^{[0]}\end{aligned}$$

其中

$$
\begin{aligned}
X^{[0]}Y^{[1]}Z^{[1]} &= \sum_{i=1}^{q} X_0 Y_i Z_i, \\
X^{[1]}Y^{[0]}Z^{[1]} &= \sum_{i=1}^{q} X_i Y_0 Z_i, \\
X^{[1]}Y^{[1]}Z^{[0]} &= \sum_{i=1}^{q} X_i Y_i Z_0, \\
X^{[0]}Y^{[0]}Z^{[2]} &= X_0 Y_0 Z_{q+1}, \\
X^{[0]}Y^{[2]}Z^{[0]} &= X_0 Y_{q+1} Z_0, \\
X^{[2]}Y^{[0]}Z^{[0]} &= X_{q+1} Y_0 Z_0
\end{aligned}
$$

其对应的张量分别为 $\langle 1,1,q\rangle$，$\langle 1,q,1\rangle$，$\langle q,1,1\rangle$，$\langle 1,1,1\rangle$，$\langle 1,1,1\rangle$，$\langle 1,1,1\rangle$。
令

$$
S = \left\{ A,B,C \in \{0,1,2\}^N : \begin{array}{l} (0,1,1),(1,0,1),(1,1,0),(0,0,2),(0,2,0),(2,0,0) \\ \text{在所有 } (A_i,B_i,C_i) \text{ 中出现的次数分别为} \\ (1-\alpha)N/3,(1-\alpha)N/3,(1-\alpha)N/3, \\ \alpha N/3,\alpha N/3,\alpha N/3 \end{array} \right\}.
$$

有 $|S| = \binom{N}{(1-\alpha)N/3,(1-\alpha)N/3,(1-\alpha)N/3,\alpha N/3,\alpha N/3,\alpha N/3}$。取 S 中尽量大的子集 S' 使得对任意 $(A,B,C),(A',B',C'),(A'',B'',C'') \in S'$，$A+B'+C'' = (2,\dots,2)$ 仅当 $(A,B,C)=(A',B',C')=(A'',B'',C'')$。修改定理 7.4 证明中的构造：定义哈希函数 (hash function) $h_1,h_2,h_3 : \{0,1,2\}^N \to \mathbb{F}_m$ 如下

$$
\begin{aligned}
h_1(a) &= \sum_{i=1}^{N} w_i a_i + w_{N+1} \\
h_2(b) &= \sum_{i=1}^{N} w_i b_i + w_{N+2} \\
h_3(c) &= \frac{1}{2}\left(\sum_{i=1}^{N} w_i (2-c_i) + w_{N+1} + w_{N+2} \right).
\end{aligned}
$$

定义 $S' = \{(a,b,c) \in S : h_1(a), h_2(b), h_3(c) \in Q\}$，其中 Q 的定义与定理 7.4 证明中相同。定义 S' 的子集 T_1,T_2,T_3 如下：

$$
\begin{aligned}
T_1 &= \{(a,b,c) \in S' : \exists\, (a,b',c') \in S', b \neq b'\} \\
T_2 &= \{(a,b,c) \in S' : \exists\, (a',b,c') \in S', a \neq a'\} \\
T_3 &= \{(a,b,c) \in S' : \exists\, (a',b',c) \in S', a \neq a'\}.
\end{aligned}
$$

并令 $U = S' \setminus (T_1 \cup T_2 \cup T_3)$。类似定理 7.4 的证明可得集合 U 满足要求。令 $m = \Theta\left(\binom{2(1-\alpha)N/3}{(1-\alpha)N/3}\binom{(1+\alpha)N/3}{(1-\alpha)N/3,\alpha N/3,\alpha N/3}\right)$，可得 $|U| = \Omega(|S||Q|/m^2) = \left(\begin{smallmatrix} N \\ (1+\alpha)N/3, 2(1-\alpha)N/3, \alpha N/3 \end{smallmatrix}\right)^{1-o(1)}$。考虑 $T^{\otimes N}$。对任意变量 $X_{j_1,\ldots,j_N}$，设其属于块 $[A]$。若 $0,1,2$ 在 A 中出现的次数不分别为 $(1+\alpha)N/3, 2(1-\alpha)N/3, \alpha N/3$，或者 $h_1(A) \neq Q$，则删除所有含变量 $X^{j_1,\ldots,j_N}$ 的项。类似地处理 Y 和 Z。这样项 $X^{[A]}Y^{[B]}Z^{[C]}$ 出现当且仅当 $(A,B,C) \in S'$。进一步，删除含变量 $X_{i_1,\ldots,i_N}$ 的项，如果 $i_1,\ldots,i_N$ 不属于任何块 A 使得存在 $(A,B,C) \in U$。类似地删除含变量 $Y_{i'_1,\ldots,i'_N}$ 的项，如果 $i'_1,\ldots,i'_N$ 不属于任何块 B 使得存在 $(A,B,C) \in U$。最后删除含变量 $Z_{i''_1,\ldots,i''_N}$ 的项，如果 $i''_1,\ldots,i''_N$ 不属于任何块 C 使得存在 $(A,B,C) \in U$。设得到的多项式为 P，其对应的张量为 T'。有 $P = \sum_{(A,B,C)\in U} X^{[A]}Y^{[B]}Z^{[C]}$，且项与项之间是独立的。于是 $T' = \left(\langle q,q,q\rangle^{\otimes(1-\alpha)N/3} \otimes \langle 1,1,1\rangle^{\otimes \alpha N/3}\right)^{\oplus |U|}$ 并且 $\underline{R}(T') \leq \underline{R}\left(T^{\otimes N}\right) \leq (q+2)^N$。由渐近和不等式，有 $|U| q^{(1-\alpha)N\omega/3} \leq (q+2)^N$。令 $N \to \infty$ 并令 $q = 6$，$\alpha \approx 0.048$，得到：

定理 8.1 ([CW90])：
$\omega \leq 2.388\ldots$

接下来考虑 $T^{\otimes 2}$ 并设其对应多项式 p。修改变量的分块 $[i,j] \mapsto [i+j]$，即：

$$
\begin{aligned}
X^{[0]} &= \{X_{0,0}\}, \\
X^{[1]} &= \{X_{i,0}, X_{0,k} : i,k = 1,\ldots,q\}, \\
X^{[2]} &= \{X_{0,q+1}, X_{i,k}, X_{q+1,0} : i,k = 1,\ldots,q\}, \\
X^{[3]} &= \{X_{i,q+1}, X_{k,q+1} : i,k = 1,\ldots,q\}, \\
X^{[4]} &= \{X_{q+1,q+1}\}.
\end{aligned}
$$

且有 $p(X,Y,Z) = \sum_{i+j+k=4} X^{[i]}Y^{[j]}Z^{[k]}$。有：

$$
\begin{aligned}
X^{[0]}Y^{[0]}Z^{[4]} = X^{[0]}Y^{[4]}Z^{[0]} = X^{[4]}Y^{[0]}Z^{[0]} &\simeq \langle 1,1,1\rangle \\
X^{[0]}Y^{[1]}Z^{[3]} = X^{[0]}Y^{[3]}Z^{[1]} &\simeq \langle 1,1,2q\rangle \\
X^{[1]}Y^{[0]}Z^{[3]} = X^{[3]}Y^{[0]}Z^{[1]} &\simeq \langle 1,2q,1\rangle \\
X^{[1]}Y^{[3]}Z^{[0]} = X^{[3]}Y^{[1]}Z^{[0]} &\simeq \langle 2q,1,1\rangle \\
X^{[0]}Y^{[2]}Z^{[2]} &\simeq \langle 1,1,q^2+2\rangle \\
X^{[2]}Y^{[0]}Z^{[2]} &\simeq \langle q^2+2,1,1\rangle \\
X^{[2]}Y^{[2]}Z^{[0]} &\simeq \langle 1,q^2+2,1\rangle
\end{aligned}
$$

但 $X^{[1]}Y^{[1]}Z^{[2]}$，$X^{[1]}Y^{[2]}Z^{[1]}$ 和 $X^{[2]}Y^{[1]}Z^{[1]}$ 不对应任何矩阵乘法。处理这一问题的方法是取对应张量的高次张量幂，并（在删除若干变量后）表示为若干矩阵乘法张量的直和。有下列结论（证明见后）：

引理 8.1 ([CW90])：
令 T_1, T_2, T_3 分别为 $X^{[1]}Y^{[1]}Z^{[2]}$，$X^{[1]}Y^{[2]}Z^{[1]}$ 和 $X^{[2]}Y^{[1]}Z^{[1]}$ 对应的张量，则对于正整数 N 以及 $\tau > 0$，存在正整数 t 以及 $(n_1, m_1, p_1), \ldots, (n_t, m_t, p_t)$ 使得

$$
(T_1 \otimes T_2 \otimes T_3)^{\otimes N} = \left(\oplus_{i=1}^{t} \langle n_i, m_i, p_i\rangle\right) \oplus \ldots
$$

并且有 $\lim_{N\to\infty} \left(\sum_{i=1}^{t} (n_i m_i p_i)^{\tau}\right)^{1/N} \geq 4q^{3\tau}(q^{3\tau}+2)$。

定理 8.2 ([CW90])：
$\omega \leq 2.375\ldots$

证明：考虑 $\left(T^{\otimes 2}\right)^{\otimes N}$。取非负整数 $A_0, \ldots, A_4$ 使得 $\sum_{i=0}^{4} A_i = N$ 并且 $\sum_{i=0}^{4} iA_i = 4N/3$。对 $0 \leq i,j,k \leq 4$ 且 $i+j+k=4$，取非负整数 $\eta_{i,j,k}$ 使得

$$
\begin{aligned}
\sum_{\substack{0\leq i,j,k\leq 4 \\ i+j+k=4}} \eta_{i,j,k} &= N \\
\sum_{\substack{0\leq j,k\leq 4 \\ i+j+k=4}} \eta_{i,j,k} &= A_i \qquad \forall 0 \leq i \leq 4 \\
\sum_{\substack{0\leq i,k\leq 4 \\ i+j+k=4}} \eta_{i,j,k} &= A_j \qquad \forall 0 \leq j \leq 4 \\
\sum_{\substack{0\leq i,j\leq 4 \\ i+j+k=4}} \eta_{i,j,k} &= A_k \qquad \forall 0 \leq k \leq 4
\end{aligned}
$$

令

$$S=\left\{A,B,C\in\{0,\dots,4\}^N:\ (i,j,k)\text{ 在所有 }(A_\ell,B_\ell,C_\ell)\text{ 中出现 }\eta_{i,j,k}\text{ 次}\right\}.$$

有 $|S|=\binom{N}{\{\eta_{i,j,k}\}}$。取 S 中尽量大的子集 S' 使得对任意 $(A,B,C),(A',B',C'),(A'',B'',C'')\in S'$，$A+B'+C''=(2,\dots,2)$ 仅当 $(A,B,C)=(A',B',C')=(A'',B'',C'')$。修改定理 7.4 证明中的构造：定义哈希函数 (hash function) $h_1,h_2,h_3:\{0,1,2\}^N\to\mathbb{F}_m$ 如下

$$\begin{aligned}h_1(a)&=\sum_{i=1}^N w_ia_i+w_{N+1}\\h_2(b)&=\sum_{i=1}^N w_ib_i+w_{N+2}\\h_3(c)&=\frac{1}{2}\left(\sum_{i=1}^N w_i(4-c_i)+w_{N+1}+w_{N+2}\right).\end{aligned}$$

定义 $S'=\{(a,b,c)\in S:h_1(a),h_2(b),h_3(c)\in Q\}$，其中 Q 的定义与定理 7.4 证明中相同。定义 S' 的子集 T_1,T_2,T_3 如下：

$$\begin{aligned}T_1&=\{(a,b,c)\in S':\exists\,(a,b',c')\in S',b\neq b'\}\\T_2&=\{(a,b,c)\in S':\exists\,(a',b,c')\in S',a\neq a'\}\\T_3&=\{(a,b,c)\in S':\exists\,(a',b',c)\in S',a\neq a'\}.\end{aligned}$$

并令 $U=S'\setminus(T_1\cup T_2\cup T_3)$。类似定理 7.4 的证明可得集合 U 满足要求。令 m_X 为包含某个 $X^{[I]}$ 且 $(I,J,K)\in S$ 的项 $X^{[I]}Y^{[J]}Z^{[K]}$ 的数量。对 Y和 Z 类似地定义 m_Y 和 m_Z。有：

$$m_X=m_Y=m_Z=\frac{\prod_{i=0}^4 A_i!}{\prod_{i+j+k=4}\eta_{i,j,k}!}.$$

另一方面，令 m'_X 为包含某个 $X^{[I]}$ 的项 $X^{[I]}Y^{[J]}Z^{[K]}$ 的数量（其中 I,J,K 中 i 出现的次数均为 A_i）。对 Y和 Z 类似地定义 m'_Y 和 m'_Z。有：

$$m'_X=m'_Y=m'_Z=\sum_{\{\eta_{i,j,k}\}}\frac{\prod_{i=0}^4 A_i!}{\prod_{i+j+k=4}\eta_{i,j,k}!}.$$

注意到上式共有至多 $N^{O(1)}$ 项，故可以取 $\{\eta_{i,j,k}\}$ 使得 $m_X \geq m'_X/N^{O(1)}$。令 $m=\Theta(m'_X)$，可得

$$\begin{aligned}|U|=\Omega(|S||Q|/m^2)=\Omega(|S|/m^{1+o(1)})&=\binom{N}{A_0,\ldots,A_4}^{1-o(1)}N^{-O(1)}\\&=\binom{N}{A_0,\ldots,A_4}^{1-o(1)}.\end{aligned}$$

考虑 $\left(T^{\otimes 2}\right)^{\otimes N}$。对任意变量 $X_{j_1,\ldots,j_N}$，设其属于块 $[A]$。若 $0,\ldots,4$ 在 A 中出现的次数不分别为 $A_0,\ldots,A_4$，或者 $h_1(A)\neq Q$，则删除所有含变量 $X^{j_1,\ldots,j_N}$ 的项。类似地处理 Y和 Z。这样若 $(A,B,C)\in S'$，则项 $X^{[A]}Y^{[B]}Z^{[C]}$ 出现。进一步，删除含变量 $X_{i_1,\ldots,i_N}$ 的项，如果 $i_1,\ldots,i_N$ 不属于任何块 A 使得存在 $(A,B,C)\in U$。类似地删除含变量 $Y_{i'_1,\ldots,i'_N}$ 的项，如果 $i'_1,\ldots,i'_N$ 不属于任何块 B 使得存在 $(A,B,C)\in U$。最后删除含变量 $Z_{i''_1,\ldots,i''_N}$ 的项，如果 $i''_1,\ldots,i''_N$ 不属于任何块 C 使得存在 $(A,B,C)\in U$。设得到的多项式为 P，其对应的张量为 T'。有 $P=\left(\sum_{(A,B,C)\in U}X^{[A]}Y^{[B]}Z^{[C]}\right)+\ldots$，且项与项之间是独立的。于是 $T'=\left(\langle q,q,q\rangle^{\otimes(1-\alpha)N/3}\otimes\langle 1,1,1\rangle^{\otimes\alpha N/3}\right)^{\oplus|U|}$ 并且 $\underline{R}(T')\leq\underline{R}\left(\left(T^{\otimes 2}\right)^{\otimes N}\right)\leq(q+2)^{2N}$。由渐近和不等式，有

$$\binom{N}{A_0,\ldots,A_4}^{1-o(1)}\left((2q)^{6b}(q^2+2)^{3c}\right)^{\omega/3}(4q^\omega(q^\omega+2))^d\leq(q+2)^{2N}$$

其中

$$\begin{aligned}&\eta_{0,0,4}=\eta_{0,4,0}=\eta_{4,0,0}=a,\\&\eta_{0,1,3}=\eta_{0,3,1}=\eta_{1,0,3}=\eta_{1,3,0}=\eta_{3,0,1}=\eta_{3,1,0}=b,\\&\eta_{0,2,2}=\eta_{2,0,2}=\eta_{2,2,0}=c,\\&\eta_{1,1,2}=\eta_{1,2,1}=\eta_{2,1,1}=d.\end{aligned}$$

（可以验证使得 m_X 在 m'_X 中最大的 $\{\eta_{i,j,k}\}$ 满足上述条件。）
令 $\bar{a}=a/N$ 并类似地定义 $\bar{b},\bar{c},\bar{d}$。令 $N\to\infty$ 并对上式两边开 N 次方，得到：

$$\frac{(2q)^{2\bar{b}\omega}(q^2+2)^{\bar{c}\omega}(4q^\omega(q^\omega+2))^{\bar{d}}}{(2\bar{a}+2\bar{b}+\bar{c})^{2\bar{a}+2\bar{b}+\bar{c}}(2\bar{b}+2\bar{d})^{2\bar{b}+2\bar{d}}(2\bar{c}+\bar{d})^{2\bar{c}+\bar{d}}(2\bar{b})^{2\bar{b}}\bar{a}^{\bar{a}}}\leq(q+2)^2.$$

令 $\bar{a}=0.000233$, $\bar{b}=0.012506$, $\bar{c}=0.102546$, $\bar{d}=0.205542$, $q=6$，解得 $\omega \le 2.375\ldots$。证毕。

证明（引理 8.1）：

$$\begin{aligned} X^{[1]}Y^{[1]}Z^{[2]} &= \sum_{i=1}^{q} x_{i,0}^{[1,0]} y_{i,0}^{[1,0]} z_{0,q+1}^{[0,2]} + \sum_{k=1}^{q} x_{0,k}^{[0,1]} y_{0,k}^{[0,1]} z_{q+1,0}^{[2,0]} \\ &\quad + \sum_{i,k=1}^{q} x_{i,0}^{[1,0]} y_{0,k}^{[0,1]} z_{i,k}^{[1,1]} + \sum_{i,k=1}^{q} x_{0,k}^{[0,1]} y_{i,0}^{[1,0]} z_{i,k}^{[1,1]} \end{aligned}$$

其对应的张量为 T_1。考虑 $T_1^{\otimes 2N}$。取非负整数 L, G 使得 $L+G=N$。删除项 $X^{[I]}Y^{[J]}Z^{[K]}$，如果 I 中 $[1,0]$ 与 $[0,1]$ 的数量不同，或者 J 中 $[1,0]$ 与 $[0,1]$ 的数量不同，或者 K 中 $[2,0]$，$[0,2]$ 与 $[1,1]$ 的数量不分别为 $L, L, 2G$。设得到的张量为 T_1'。类似地考虑 $X^{[1]}Y^{[2]}Z^{[1]}$ 和 $X^{[2]}Y^{[1]}Z^{[1]}$ 并得到 T_2' 和 T_3'。考虑 $T'' = T_1' \otimes T_2' \otimes T_3'$。在 T'' 中有 $\binom{2N}{N}^2 \binom{2N}{L,L,2G}$ 个可能的 X 块，每块出现在 $\binom{N}{L}^4 \binom{2G}{G}$ 个项 $X^{[I]}Y^{[J]}K^{[K]}$ 中。利用与定理 8.2 的证明相同的哈希函数进一步删除变量以保证独立性，则剩余至少 $t = \Omega\left(\left(\binom{2N}{N}^2 \binom{2N}{L,L,2G}\right)^{1-o(1)}\right)$ 项，其中每一项对应一个矩阵乘法 $\langle n_i, m_i, p_i \rangle$，并且 $n_i m_i p_i = (q^2)^{6G} q^{6L} = q^{12G+6L}$。于是有

$$\sum_{i=1}^{t} (n_i m_i p_i)^{\tau} = \Omega\left(\left(\binom{2N}{N}^2 \binom{2N}{L,L,2G}\right)^{1-o(1)} q^{12G+6L}\right)$$

令 $L = \frac{2N}{q^\tau+2}$，$G = \frac{q^\tau N}{q^\tau+2}$。对上式左右两边开 N 次方并令 $N \to \infty$，得到

$$\lim_{N\to\infty} \left(\sum_{i=1}^{t} (n_i m_i p_i)^{\tau}\right)^{1/N} \ge 4q^{3\tau}(q^{3\tau}+2).$$

证毕。

Stothers [Sto10] 和 Williams [Wil12] 分析了 $T^{\otimes 4}$，并分别得到 $\omega \le 2.3736\ldots$ 和 $\omega \le 2.3729\ldots$。Williams [Wil12] 进一步分析了 $T^{\otimes 8}$，并得到：

定理 8.2 ([Wil12])：
$\omega \le 2.3726\ldots$

参考文献：

[BCRL79] Dario Bini, Milvio Capovani, Francesco Romani, and Grazia Lotti. $O(n^{2.7799})$ Complexity for $n \times n$ Approximate Matrix Multiplication. Inf. Process. Lett., 8 (1979), 234-235.

[Blä09] Markus Bläser. Complexity of Bilinear Problems (lecture notes scribed by Fabian Bendun). 2009.

[BLR80] Dario Bini, Grazia Lotti, and Francesco Romani. Approximate Solutions for the Bilinear Form Computational Problem, SIAM J. Comput., 9 (1980), 692-697.

[CKSU05] Henry Cohn, Robert Kleinberg, Balázs Szegedy, and Christopher Umans. Group-theoretic Algorithms for Matrix Multiplication. Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 379-388, 2005.

[CU03] Henry Cohn and Christopher Umans. A Group-theoretic Approach to Fast Matrix Multiplication. Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 438-449, 2003.

[CW90] Don Coppersmith and Shmuel Winograd. Matrix Multiplication via Arithmetic Progressions. J. Symb. Comput., 9 (1990), 251-280.

[Hås90] Johan Håstad. Tensor Rank is NP-complete. J. Algorithms, 11 (1990), 644-654.

[Lan84] Serge Lang. Algebra. Addison Wesley, second edition, 1984.

[Pan66] Victor Pan. Methods for Computing Values of Polynomials. Russian Math. Surveys, 21 (1966), 105-136.

[Sch81] Arnold Schönhage. Partial and Total Matrix Multiplication. SIAM J. Comp., 10 (1981), 434-455.

[SS42] Raphaël Salem and Donald C. Spencer. On Sets of Integers Which Contain No Three in Arithmetic Progression. Proc. Nat. Acad. Sci. (USA), 28 (1942), 561-563.

[Sto10] Andrew Stothers. Ph.D. Thesis, U. Edinburgh, 2010.

[Str69] Volker Strassen. Gaussian Elimination is not Optimal. Numer. Math., 13 (1969), 354-356.

[Str73] Volker Strassen. Vermeidung von Divisionen. J. Reine Angew. Math., 264 (1973), 184-202.

[Str87] Volker Strassen. Relative Bilinear Complexity and Matrix Multiplication. J. Reine Angew. Math., 375/376 (1987), 406-443.

[Wil12] Virginia Vassilevska Williams. Multiplying Matrices Faster Than Coppersmith-Winograd. Proceedings of the 44th Symposium on Theory of Computing, 887-898, 2012.