线性代数

张昕渊

October 6, 2023

大纲

- 向量空间：线性独立与线性相关、线性基；
- 矩阵：初等行列变换、高斯消元、行列式、解空间的结构。
- 杂谈：Cramer法则、一般图匹配。

向量空间

Definition (向量空间)

V是一个集合。若V在加法和数乘下封闭，则V被称为一个（域F上的）向量空间。即

1. $\forall x, y \in V$, $x + y \in V$;
2. $\forall x \in V$且$k \in F$, $kx \in V$。

- 数域可以较为简单的看作是一个具有四则运算的集合：如$\mathbb{R}$，F_p（模p下的元素集合）。
- 一些向量空间示例：$\mathbb{R}^n$（域$\mathbf{R}$上），F_p^n（域$\mathbf{F}_p$上）（F_2^n中的加法：长度为n的01异或）。
- 不那么平凡的向量空间示例：三维空间中经过原点的平面。
  - 如$\{(x, y, z) \in \mathbb{R}^3 | 2x + 3y + z = 0\} \subseteq \mathbb{R}^3$。
- 不是向量空间：三维空间中不经过原点的平面。
  - 如$\{(x, y, z) \in \mathbb{R}^3 | 2x + 3y + z = 1\} \subseteq \mathbb{R}^3$。
- 子空间：$S \subseteq V$且仍为向量空间。

线性独立与线性相关

Definition

$a_1, a_2, \ldots, a_n$是向量空间V（在域）中的一列向量。若存在非全0的值$k_1, k_2, \ldots, k_n \in F$使得

$$\sum_{i=1}^{n} k_i a_i = 0,$$

则我们称该组向量为线性相关，否则为线性无关/线性独立。

- $\mathbb{R}^3$中线性独立/线性相关的示例：
  1. 线性相关：$\{(0,1,1),(1,1,0),(1,2,1)\}$、$\{(0,0,0)\}$：
     - $(0,1,1)+(1,1,0)-(1,2,1)=(0,0,0)$，$1\cdot(0,0,0)=(0,0,0)$。
  2. 线性独立：$\{(0,0,1),(0,1,0),(1,0,0)\}$。

线性独立与线性相关

Definition

$a_1, a_2, \ldots, a_n$是向量空间V（在域）中的一列向量。若存在非全0的值$k_1, k_2, \ldots, k_n \in F$使得

$$\sum_{i=1}^{n} k_i a_i = 0,$$

则我们称该组向量为线性相关，否则为线性无关/线性独立。

- 线性相关其实更说明某些向量可以被剩余的向量线性表示（即存在一些“冗余”向量）：不妨假设$k_1 \neq 0$，则

$$a_1 = \sum_{i=2}^{n} \frac{k_i}{k_1} a_i,$$

- 线性独立则说明这一系列向量都是“必要”的。

生成空间

- 很多时候，我们需要知道一列向量能“表示”的向量是什么。

Definition

给定向量集合$S=\{a_1,a_2,\ldots,a_n\}\subseteq V$，我们令

$$\mathrm{span}(S)=\left\{\sum_{i=1}^{n}k_ia_i|k_i\in F\right\}.$$

$\mathrm{span}(S)$通常被为集合S的生成/张成空间。

- 尽管S可能不满足对加法和数乘封闭，可以验证$\mathrm{span}(S)$是V的一个子空间。
- 考虑向量$(1,1,0),(0,1,1),(1,2,1)\in\mathbb{R}^3$。这一系列向量的生成空间为

$$\left\{(k_1,k_1+k_2,k_2)\in\mathbb{R}^3|k_1,k_2\in\mathbb{R}\right\}.$$

极大线性无关组

- 如何用最少的元素“线性表示”一个向量组?

Definition (极大线性无关组)

$a_1, a_2, \ldots, a_n$是向量空间V（在域F）中的一组向量。$a_{i_1}, a_{i_2}, \ldots, a_{i_k}$被称为$a$的一个极大线性无关组，若

1. $a_{i_1}, a_{i_2}, \ldots, a_{i_k}$线性独立；
2. $a_1, a_2, \ldots, a_n$中元素都可以由$a_{i_1}, a_{i_2}, \ldots, a_{i_k}$线性表示。

- 每个元素可以对应到F^k中的元素：

$$a_i = \sum_{j=1}^{k} r_j a_{i_j} \to (r_1, r_2, \ldots, r_k) \in \mathbb{F}^k.$$

- 任意两个极大线性无关组的大小是一致的，大小称为秩($rank$)。
  - 若不然，则$\mathbb{F}^k$里面可以找到$k+1$个线性无关的元素。
- 等价刻画：极小的可线性表示$a_1, a_2, \ldots, a_n$的向量组。

基与向量空间的维数

Definition (基与向量空间的维数)

对于F上的向量空间V，我们称$\{v_1, v_2, \ldots, v_n\}$为向量空间$V$的一组基，若满足下面两个条件：

1. $v_1, v_2, \ldots, v_n$线性无关；
2. 向量中的元素可由$v_1, v_2, \ldots, v_n$线性表示。

基的大小被称为向量空间V的维数。

- $\mathbb{R}$上的向量空间$\mathbb{R}^n$与$\mathbb{F}_p$上的向量空间${F_p}^n$维数均为n，一组基为$\{e_1, e_2, \ldots, e_n\}$，其中$e_i$仅在第$i$维取1，其他取0。
- 维度为n的向量空间与F^n一一对应。

F_p^n的子空间计数

Problem

F_p^n的大小为r的子空间个数有多少个?

- 首先考虑有多少组有序向量组$x_1, x_2, \ldots, x_r$线性无关。
  - x_1的选择数有$p^n - 1$种：除去0之外均可；
  - x_2的选择数有$p^n - p$种：除去$\mathrm{span}(\{x_1\})$外的元素均可；
  - x_3的选择有$p^n - p^2$种：除去$\mathrm{span}(\{x_1, x_2\})$外的元素均可；
  - x_i的选择有$p^n - p^{i-1}$种：除去$\mathrm{span}(\{x_1, x_2, \ldots, x_{i-1}\})$外的元素均可；
  - 总方案数为$\prod_{i=1}^{r}(p^n - p^{i-1})$。
- 其次考虑去重问题：每一个大小为r的子空间对应多少组有序向量组$x_1, x_2, \ldots, x_r$线性无关。
  - $\prod_{i=1}^{r}(p^r - p^{i-1})$。
- 子空间个数为$\frac{\prod_{i=1}^{r}(p^n - p^{i-1})}{\prod_{i=1}^{r}(p^r - p^{i-1})}$。

生成空间的表示：线性基

Problem

求解向量空间$V = \mathbb{R}^n$或者$\mathbb{F}_p^n$中子空间$V' = \mathrm{span}(\{x_1, x_2, \ldots, x_m\})$的维数，以及高效判定某个元素是否在此生成空间中。

- 对于向量空间$V = \mathbb{R}^n$或者$\mathbb{F}_p^n$而言，子空间$V' \subseteq V$有且仅有一组典型基$\{a_1, a_2, \ldots, a_r\}$满足如下性质：
  - 令z_i是$a_i = (a_{i,1}, a_{i,2}, \ldots, a_{i,n})$中第一个非0的位置，则$z_1 < z_2 < \ldots < z_r$；
  - $a_{i,z_j} = \begin{cases} 1 & i = j, \\ 0 & i \neq j. \end{cases}$
- 例：向量空间$V' = \{(a_1, a_2, a_3) \in F_2^3 | a_1 + a_2 + a_3 = 0\}$的典型基为$\{(1,0,1),(0,1,1)\}$。
- 唯一性：注意到$\{x \in V' | x_1 = 0\}$也是一个子空间，我们可以考虑使用数学归纳法证明。

生成空间的表示：线性基

- 对于向量空间$V = \mathbb{R}^n$或者$\mathbb{F}_p^n$而言，子空间$V' \subseteq V$有且仅有一组典型基$\{a_1, a_2, \ldots, a_r\}$满足如下性质：
  - 令z_i是$a_i = (a_{i,1}, a_{i,2}, \ldots, a_{i,n})$中第一个非0的位置，则$z_1 < z_2 < \ldots < z_r$；
  - $a_{i,z_j} = \begin{cases} 1 & i = j, \\ 0 & i \neq j. \end{cases}$
- 典型基的构造：线性基算法
  1. 维护向量$\alpha_1, \alpha_2, \ldots, \alpha_n$，其中$x_i$表示当前典型基中第一个非零位置为$i$的向量。若$x_i = 0$，则表示此典型基中不存在第一个非零位置为$i$的向量；
  2. 依次插入元素x_j：我们从α_1遍历到α_n
     2.1 若$\alpha_i = 0$且$x_{j,i} \neq 0$，则说明x_j不可以被当前典型基线性表示，因此我们将α_i置为$\frac{x_j}{x_{j,i}}$，并依次对所有$i < k \leq n$，将α_i 更新为$\alpha_i - \alpha_{i,k}\alpha_k$；最后依次对所有的$1 \leq k < i$，将$\alpha_k$更新为$\alpha_k - \alpha_{k,i}\alpha_i$（用以保证当前是一组典型基）；
     2.2 若$\alpha_i = 0$且$x_{j,i} = 0$，此时不发生任何事；
     2.3 否则，x_j将被更新为$x_j - x_{j,i}\alpha_i$。

生成空间的表示：线性基

- 算法时间复杂度$O(n^2m)$。对于F_2^n，我们可以用bitset加速至$O(n^2m/w)$，$w=32/64$。
- 我们来看一个F_2^3上的一个简单例子：
  - 假设元素分别为$(0,1,1)$, $(1,1,0)$和$(1,1,0)$（注意这里是F_2上，加法等价于异或）。
  - 初始时$\alpha_1=\alpha_2=\alpha_3=(0,0,0)$。
  - 第一个元素根据算法将直接插入到第一个非0元素，即α_2置为$(0,1,1)$；
  - 第二个元素将根据算法插入到α_1，即α_1置为$(1,1,0)$。为了让此时是一组典型基，我们将α_1更新为$\alpha_1-\alpha_2$。此时α_1被更新为$(1,0,1)$。
  - 第三个元素在遍历到α_1时，将元素$x=(1,1,0)$更新为$x+\alpha_1=(0,1,1)$；而在遍历到α_2时，由于此时x的第二位仍然非0，因此将更新为$x+\alpha_2=(0,0,0)$，最终遍历到α_3时，此时两者在第三位均为0，不发生任何事。最终该元素并未插入至向量组中。

生成空间的表示：线性基

Problem

求解向量空间$V=\mathbb{R}^n$或者$\mathbb{F}_p^n$中子空间$V'=\mathrm{span}(\{x_1,x_2,\ldots,x_m\})$的维数，以及高效判定某个元素是否在此生成空间中。

- 判断生成空间的维数：只需数α_i中非零元素个数即可；
- 判断某个元素是否在此生成空间中：简单更改插入过程，当需要插入时返回true，否则返回false即可。
- F_p^n的子空间中字典序第k小的元素：线性基中$\alpha_{t_i}\neq 0$，其他等于0（t_i升序）。将$k-1$写成p进制$(a_1,a_2,\ldots,a_r)$，$\sum_{i=1}^r a_i\alpha_{t_i}$即为所求。
- 如何将某个元素用$x_1,x_2,\ldots,x_m$线性表示：求解线性方程组。

例题：XOR

- 给定n个非负整数$a_1, a_2, \ldots, a_n$，回答q次询问。每次询问求区间$[L, R]$中选一个子集异或能产生的最大数值。
- $n, q \leq 10^5, a_i \leq 10^9$。

例题：XOR

- 线段树合并线性基即可，时间复杂度为$O(n\log^2 A\log n)$。
- 合并两个线性基：将两个线性基中的向量依次插入到一个新的线性基即可。

例题：XOR

- 给定n个非负整数$a_1, a_2, \ldots, a_n$，将他们分成两堆（可以为空），使得两堆异或和相加最大（输出值即可）。
- $n \le 10^5, a_i \le 10^9$。

例题：XOR

- 令S为所有数的异或和。若第i位是1，则无论怎么分两堆中一堆异或和该位是1，一堆是0。
- 因此，我们令$a_i = a_i \& (2^{30} - 1 - S)$，然后用线性基求出最大值$M$即可，答案为$2M + S$。

例题：异或游戏

- 给定n个非负整数$a_1, a_2, \ldots, a_n$以及非负整数k。Alice和Bob交替完成下面的操作：
  - 选择a_i和a_j（可能$i = j$），将$a_i \oplus a_j$加入至序列中。如果$a_i \oplus a_j = k$，则该名玩家获胜。
- 都采取最优策略的前提下，请判定该游戏$Alice/Bob$谁会获胜，或者平局。
- $n \leq 10^6$，$a_i, k \leq 10^9$.

例题：异或游戏

- 如果存在i,j使得$a_i \oplus a_j = k$，则Alice获胜；
- 如果对于任意的i,j，存在x使得$a_i \oplus a_j = k \oplus a_x$，则Bob获胜；
- 否则平局。
- 第二个条件等价于$(a_i \oplus k) \oplus (a_j \oplus k) = k \oplus a_x$，
  即$S = \{(a_i \oplus k) | 1 \le i \le n\}$是一个向量子空间，
  即$|S| = 2^{\mathrm{rank}(S)}$。

例题：异或游戏2

- 给定n个正整数$a_1, a_2, \ldots, a_n$以及长度为n的01串s。有一个初始为0的变量x，$Alice/Bob$按照如下规则进行操作：
  - 第i次操作中，如果$s_i = 0$，则Alice进行操作，否则Bob进行操作；
  - 在本轮操作中，玩家可以将x置为$x \oplus a_i$，或者保持不变。

  Alice的目标是使得最终$x = 0$，Bob的目标是使得最终$x \neq 0$。在都采取最优策略的前提下，请你判断该游戏$Alice/Bob$谁会获胜，或者平局。
- $n \leq 100, a_i \leq 10^{18}$。
- AGC045A

矩阵与线性映射

Definition (线性映射)

给定两个F上的向量空间U, V，映射$T: U \to V$被称为线性映射，如果

- $\forall x, y \in U,\ T(x+y) = Tx + Ty$;
- $\forall x \in U, k \in F,\ T(kx) = kTx$.

- 线性映射的简单例子：
  - $T: F_2^2 \to F_2^2,\ T(x_1, x_2) = (x_1 + x_2, x_1)$;
  - $T: \mathbb{R}^3 \to \mathbb{R}^2$: $T(x, y, z) = (x, 2x)$。
- 不是线性映射的例子：
  - $T: F_2^2 \to F_2^2,\ Tx = x \oplus 1$（线性映射作用到0上一定为0）。
  - $T: \mathbb{R} \to \mathbb{R}$，$Tx = x^2$（$T2 \neq 2T1$）

矩阵与线性映射

Definition (线性映射)

给定两个F上的向量空间U, V，映射$T: U \to V$被称为线性映射，如果

- $\forall x, y \in U,\ T(x+y) = Tx + Ty$;
- $\forall x \in U, k \in F,\ T(kx) = kTx$.

- $TU = \{Tu | u \in V\}$被称为T的像(image)，也是一个向量空间。
- $\{u_1, u_2, \ldots, u_n\}$为$U$的一组基，则$T$完全由$Tu_i$的取值决定。
  - 令$x \in U$，则$x = \sum_{i=1}^n \lambda_i u_i$，则$Tx = \sum_{i=1}^n \lambda_i Tu_i$。
- 令$\{v_1, v_2, \ldots, v_m\}$为$V$的一组基，则$Tu_i = \sum_{j=1}^m a_{j,i} v_j$。
- 因此，一个线性映射本质上就是一个矩阵$A = (a_{i,j})_{1 \le i \le m, 1 \le j \le n}$。
- 反过来，一个域F上的矩阵$M \in F^{n \times m}$也对应着一个线性映射$T_M: F^m \to F^n$，$T_M e_i = \sum_{j=1}^n a_{j,i} e_j$。

矩阵与线性映射

- 矩阵的基础运算：
  - 加法：$A, B \in F^{n\times m}$, $(A+B)_{i,j} = A_{i,j} + B_{i,j}$。
  - 这对应着两个线性映射的加法：$T_A + T_B$。
  - 乘法$A \in F^{n\times m}$, $B \in F^{m\times r}$，$(AB)_{i,k} = \sum_{j=1}^{m} A_{i,j}B_{j,k}$。
  - 这对应两个线性映射的复合：

$$(T_A \circ T_B)e_k = T_A \sum_{j=1}^{m} b_{j,k}e_j = \sum_{j=1}^{m} b_{j,k} T_A e_j$$

$$= \sum_{j=1}^{m} b_{j,k} \sum_{i=1}^{n} a_{i,j}e_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{i,j}b_{j,k} \right) e_i.$$

  - 转置：$(A^T)_{i,j} = A_{j,i}$。
  - $(AB)^T = B^T A^T$。
- 一个小的计算若干个矩阵乘法的技巧：当你需要计算向量$x \in \mathbb{R}^n$乘以矩阵$A, B \in \mathbb{R}^{n\times n}$时，利用矩阵结合律$x^T(AB) = (x^T A)B$可以在$O(n^2)$而非$O(n^3)$时间完成计算。

矩阵与常系数线性递推

- 考虑形如$f_n = \sum_{i=1}^{k} a_i f_{n-i} + c$的线性递推形式，如何求解$f_n$。
- 齐次化（将c变为0）：
  1. 若$\sum_{i=1}^{k} a_i \neq 1$，则我们可以待定系数$A$，将$f_i$替换为$f_i + A$；
  2. 否则，我们待定系数Ai，将f_i替换为$f_i + Ai$。
- 考虑矩阵：$A = \begin{pmatrix} a_i & a_{i-1} & a_{i-2} & \dots & a_1 & a_0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ & & \dots & & & \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}$.
- 则$(f_n, f_{n-1}, \dots, f_{n-k+1})^T = A(f_{n-1}, f_{n-2}, \dots, f_{n-k})^T$。
- 因此，$(f_n, f_{n-1}, \dots, f_{n-k+1})^T = A^{n-k+1}(f_{k-1}, f_{k-2}, \dots, f_0)$。
- 类似一般的快速幂，我们可以对矩阵使用快速幂，时间复杂度是$O(k^3 \log n)$。

*常系数线性递推

- 假设k比较大（比如10^5），能否做得比矩阵快速幂更好?
- 从多项式的角度来看，常系数线性递推等价于我们可以将x^n替换为$\sum_{i=1}^{k} a_i x_{n-i}$，最终求$x^0, x^1, \ldots, x^{k-1}$的系数。
- 上述操作等价于模$f = x^k - \sum_{i=1}^{k} a_i x_{k-i}$。因此我们只需利用多项式快速幂求解$x^n \mod f$即可，这可以通过在$O(m \log m \log n)$的时间内求解。

例题：Exponent

- 已知复数x满足$x + \frac{1}{x} = \alpha$，求$x^\beta + \frac{1}{x^\beta} \mod m$的值
- $\alpha, \beta, m \le 10^9$。

例题：Exponent

- 注意到

$$(x^n + 1/x^n)(x + 1/x) = x^{n+1} + 1/x^{n+1} + x^{n-1} + 1/x^{n-1},$$

则$\alpha f_n = f_{n+1} + f_{n-1}$，这是常系数线性递推。

例题：Recursive sequence

- 给定递推$f_n = f_{n-1} + f_{n-2} + n^4$，求$f_n \mod 998244353$的值。
- $n \leq 10^9$。

例题：Recursive sequence

- 方法1：待定系数A, B, C, D, E，令f_n变为$f_n + An^4 + Bn^3 + Cn^2 + Dn + E$消去$n^4$项，转为齐次线性递推（缺点：相对来说比较麻烦，如果f_{n-1}, f_{n-2}前系数未定，还需要额外的讨论）。
- 方法2：将$n^4, n^3, n^2, n, 1$嵌入到向量中，写出向量$v_n = (f_n, f_{n-1}, n^4, n^3, n^2, n^1, 1)^T$到$v_{n-1}$的线性变换。

例题：Recursive sequence

- 方法1：待定系数A, B, C, D, E，令f_n变为$f_n + An^4 + Bn^3 + Cn^2 + Dn + E$消去$n^4$项，转为齐次线性递推（缺点：相对来说比较麻烦，如果f_{n-1}, f_{n-2}前系数未定，还需要额外的讨论）。
- 方法2：将$n^4, n^3, n^2, n, 1$嵌入到向量中，写出向量$v_n = (f_n, f_{n-1}, n^4, n^3, n^2, n^1, 1)^T$到$v_{n-1}$的线性变换。

例题：Hanjo 2

- 1×2的矩形铺满$H \times W$的矩形有多少种填法，答案模998244353。
- $H \leq 6, W \leq 10^{12}$。

初等行列变换与高斯消元

Problem

给定$A \in F^{n\times m}$以及$b \in \mathbb{F}^n$，求解线性方程组$Ax = b$，以及给出线性方程解空间的刻画。

- 怎么求出解：
- 初等行列变换（我们其实已经在求解线性基的过程中隐含的用到了初等行列变换的思想）：
  1. 调换两行：从方程组角度而言，没有变化。
  2. 将一行的某个倍数加到另一行：从方程组角度而言，将某个方程乘以
  3. 将一行乘以某个非0倍数。
- 通过初等行列变换将A变为一个典型基的形式，化为此形式后可以直接求出解或者判定无解。

初等行列变换与高斯消元

- 示例：$\mathbb{R}$上的线性方程组：

$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 5 \\ 0 & -1 & 3 \end{pmatrix} x = \begin{pmatrix} 4 \\ 7 \\ -1 \end{pmatrix}.$$

- 第一步：写出增广矩阵$A' = \begin{pmatrix} 1 & 2 & 1 & 4 \\ 2 & 3 & 5 & 7 \\ 0 & -1 & 3 & -1 \end{pmatrix}$
- 第二步：通过初等行列变换变为典型基的形式：

$$\begin{pmatrix} 1 & 2 & 1 & 4 \\ 2 & 3 & 5 & 7 \\ 0 & -1 & 3 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & 4 \\ 0 & -1 & 3 & -1 \\ 0 & -1 & 3 & -1 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 2 & 1 & 4 \\ 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 7 & 2 \\ 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

初等行列变换与高斯消元

- 第三步：求出一个可行解$x^\star$ — 对于$A' = [A, b]$中每一个非0的行i而言，令第$j = f(i)$个列是第一个非0的位置，则$x_j^\star = b_i$。其余的位置填0即可。如

$$A' = \begin{pmatrix} 1 & 0 & 7 & 2 \\ 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

  一组解为$(2, 1, 0)$。
- 如何求得通解:
  1. 通解是特解$x^\star$加上$Ax = 0$的解。
  2. 给定进行完初等行变换的增广矩阵A'，如何求$Ax = 0$的解?
  3. 对于所有非$f(1), f(2), \ldots, f(n)$的位置j而言，我们令$x_j = 1$，剩余的非$f(1), f(2), \ldots, f(n)$的位置为0，剩余的位置通过A'反解出来，这将构成$Ax = 0$解空间的一组基。

初等行列变换与高斯消元

- 考虑

$$A' = \begin{pmatrix} 1 & 0 & 7 & 2 \\ 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

- 特解是$(2,1,0)$，$Ax = 0$的解空间一组基为$\{(-7,3,1)\}$，因此$Ax = b$的解集为$\{(2-7k, 1+3k, k) | k \in \mathbb{R}\}$.
- 通过上述算法可以看出，$Ax = 0$解空间维数为m减去非0的行数。
- 令A的秩为A的行向量（或者列向量，可以证明是等价的）极大线性无关组的个数，则解空间维数为$m - \mathrm{rank}(A)$.
- $rank(A)$的更直观的意义：向量空间$Im(A) = \{Ax | x \in F^m\}$的维数！

初等行列变换与高斯消元

- 考虑

$$A' = \begin{pmatrix} 1 & 0 & 7 & 2 \\ 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

- 特解是$(2,1,0)$，$Ax = 0$的解空间一组基为$\{(-7,3,1)\}$，因此$Ax = b$的解集为$\{(2-7k, 1+3k, k) | k \in \mathbb{R}\}$.
- 通过上述算法可以看出，$Ax = 0$解空间维数为m减去非0的行数。
- 令A的秩为A的行向量（或者列向量，可以证明是等价的）极大线性无关组的个数，则解空间维数为$m - \mathrm{rank}(A)$.
- $rank(A)$的更直观的意义：$Im(A) = \{Ax | x \in F^m\}$的维数。

总结

- 如何求解$Ax=b$的通解：对增广矩阵进行初等行变换变成“典型基”的形式，特解令自由变量置为0得到，$Ax=0$解的一组基可由单个自由变元置为1得到。
- $\mathrm{rank}(A)+\mathrm{dimKer}(A)=m$，$\mathrm{Ker}(A)=\{x|Ax=0\}$。

常见异或方程模型–矩阵模型

- 对于$n \times m$的矩阵，如何填数使得每一行的奇偶性条件r_i、每一列的奇偶性条件c_j被满足。有多少种填法?
- 矩阵到奇偶性条件可以看成是$\mathbb{R}^{n\times m} \to \mathbb{R}^{n+m}$的线性变换。
- 可以被满足当且仅当$\sum_{i=1}^{n} r_i = \sum_{j=1}^{m} c_j$（因此有解的话解的个数为$2^{nm-n-m+1}$，这是因为像空间的维度是$n+m-1$）。
- 只需最后按照奇偶性条件确定最后一行和最后一列即可，其他随便填。
- 对于矩阵模型而言，大多数时候的充要条件都与行、列之和的不变量有关。

常见异或方程模型–图模型

- 给定连通图$G=(V,E)$，每一个顶点有一个权重0/1，给边赋值0,1，使得顶点权重是边权重之和(模2)，问是否可行以及方案数。
- 可行当且仅当顶点权重和是0。找一颗生成树，剩余边随意赋值，树边自底向上赋值即可，方案数为2^{m-n+1}。

例题：Cross Xor

- 给一个初始为0的$n \times m$矩阵。可以选择任意一个节点，将行号和其一致或者列号和其一致的格子值异或上1。
- 给定一个填有0, 1和?的格子，问有多少种将?替换为0/1的方案，使得该方案可以由若干次上述操作得到。
- $n, m \le 1000$。
- CF 1672G。

例题：Cross Xor

- 寻找不变量：若n为奇数时，每一列的异或和经过一次操作均变化1，即列的异或和始终保持一致；若m为奇数时，每一行的异或和经过一次操作变化均为1，即行的异或和始终保持一致。
- 可以猜想只需满足上述条件即可通过操作得到（证明需要一些构造方式，这里不详细说明）。
- 我们仅仅处理n, m是奇数的情形（其他情形更为简单）。此时，我们构建一个二分图，$a_{(i,j)}$是问号则连一条i到j的边，其余顶点上有一些奇偶性限制，问题又转化为图模型问题。

行列式

Definition

对于矩阵$A \in F^{n\times n}$，矩阵A的行列式$\det(A)$为

$$\det(A) = \sum_{p\in S(n)} (-1)^{\mathrm{inv}(\sigma)} \prod_{i=1}^{n} A_{i,p_i}.$$

- 行列式的意义：绝对值指代矩阵A所代表的线性变换缩放的程度。
- 若$\det(A) = 0$，则A将n维空间映射到维度更低的空间，这时候说明A的秩小于n，即列向量/行向量线性相关。

行列式

- 一些简单矩阵的行列式：
  - 单位矩阵I：对角线元素为1，其他元素为0。行列式为1。
  - 下/上三角矩阵：$A=(a_{i,j})$满足对于任意的$1 \le i < j \le n$，$a_{i,j}=0$/ $a_{j,i}=0$。行列式为对角线元素乘积。（这包括了初等变换矩阵中一行加上另一行的某个倍数、以及一行乘以某个倍数的情形）。
  - 行/列交换矩阵：$P_{i,j}$为I交换两行/两列。行列式为-1。
- 矩阵行列式的性质：$|AB|=|A||B|$，$|A^T|=|A|$。
- 如何求解矩阵行列式：利用初等行变换，将矩阵化为上三角矩阵（初等行变换等价于左乘一些初等矩阵/交换矩阵），时间复杂度为$O(n^3)$。

行列式

- 举例：一个3×3的矩阵：

$$\begin{pmatrix}1 & 2 & 1\\ 2 & 4 & 5\\ 0 & -1 & 5\end{pmatrix}\to\begin{pmatrix}1 & 2 & 1\\ 0 & 0 & 3\\ 0 & -1 & 5\end{pmatrix}\to\begin{pmatrix}1 & 2 & 1\\ 0 & -1 & 5\\ 0 & 0 & 3\end{pmatrix}$$

$$\to\begin{pmatrix}1 & 2 & 1\\ 0 & 1 & -5\\ 0 & 0 & 3\end{pmatrix}\to\begin{pmatrix}1 & 0 & 11\\ 0 & 1 & -5\\ 0 & 0 & 3\end{pmatrix}\to\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$$

- A的特征值乘以$1*(-1)*(-1)*1*1/3$等于1，因此特征值为3。

行列式

- 行列式的另外求解方式：递归求解。

$$\det(A) = \sum_{i=1}^{n} (-1)^{i-1} \det(A_{-1,-i}).$$

  其中$A_{-1,-i}$是去掉第一行和第i列的矩阵。

- 举例：

$$\det \begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 5 \\ 0 & -1 & 5 \end{pmatrix} = \det \begin{pmatrix} 4 & 5 \\ -1 & 5 \end{pmatrix} - 2\det \begin{pmatrix} 2 & 5 \\ 0 & 5 \end{pmatrix} + \det \begin{pmatrix} 2 & 4 \\ 0 & -1 \end{pmatrix}.$$

- 当矩阵具有特殊结构的时候可以采用这种方式建立递推式。但一般的矩阵递归求解效率极低。

特殊矩阵行列式

- 范德蒙行列式：
  - $A=(a_{i,j})$,$a_{i,j}=x_i^j$。$\det(A)=\prod_{1\le i<j\le n}(x_i-x_j)$。
- 分块矩阵行列式：当A,C为方阵时（即行数和列数相等），

$$\det\begin{pmatrix} A & 0 \\ B & C \end{pmatrix}=\det(A)\det(C).$$

$$\det\begin{pmatrix} 0 & A \\ B & C \end{pmatrix}=(-1)^{nm}\det(A)\det(B)(n,m\text{分别为}A\text{和}B\text{的大小}).$$

$$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix}=\det(A)\det(D-CA^{-1}B)(\text{若}A\text{可逆}).$$

例题：XOR determinant

- 给定序列$a_1, a_2, \ldots, a_n$和$b_1, b_2, \ldots, b_n$，求矩阵$C = (c_{i,j})$的行列式模998244353的值，其中

$$c_{i,j} = a_i \oplus b_j.$$

- $n \leq 5000$, $0 \leq a_i, b_i < 2^{60}$.

例题：行列式的值

- 注意到每一个行向量可以写成$b^{(i)}$和全1向量的线性组合，其中$b_j^{(i)}$表示b_i二进制下的第j位是否为1。因此，当$n > 61$时，$\mathrm{rank}(A) < n$，即$\det(A) = 0$。

矩阵的逆

- 矩阵A的逆: $A^{-1}A = AA^{-1} = I$。
- 矩阵A的逆存在当且仅当$\det(A) \neq 0$。
- 如何求解矩阵A的逆：构造$n \times 2n$的矩阵$[A, I]$，通过初等行变换将矩阵变为$[I, C]$，则C为矩阵A的逆。
- 可以当作同时求解n个线性方程组。

矩阵特征值与特征多项式

- 给定方阵$A \in \mathbb{R}^{n\times n}$。
- $Ax = \lambda x$，λ称为特征值，$x \neq 0$是特征向量。
- 有解当且仅当$|\lambda I - A| = 0$。
- 当A是对称矩阵时，λ均为实数，我们可以找到一个对称矩阵P，使得$P^{-1}AP = \mathrm{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$.

矩阵特征值与特征多项式

- 给定方阵$A \in \mathbb{R}^{n \times n}$。
- $Ax = \lambda x$，λ称为特征值，$x \neq 0$是特征向量。
- 有解当且仅当$|\lambda I - A| = 0$。
- 当A是对称矩阵时，λ均为实数，我们可以找到一个对称矩阵P，使得$P^{-1}AP = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$.

*Cramer 法则

- 给定方阵$A \in \mathbb{F}^{n\times n}$，$Ax = b$有唯一解当且仅当$\det(A) \neq 0$，$x_i = \frac{\det(A_i)}{\det(A)}$，其中$A_i$是将第$i$列替换为$b$。

一般图匹配

Problem

给定图$G=(V,E)$，如何求图的最大匹配大小?

- 带花树算法（Erdos' Blossom Algorithm），$O(n^3)$，不过这不是我们今天讨论的做法。
- 首先看二部图：考虑矩阵$A=(a_{i,j})_{i\in L,j\in R}$，其中$a_{i,j}=x_{i,j}e_{i,j}$，其中$x_{i,j}$为变量，$e_{i,j}=1$当且仅当$(i,j)$这条边在图中。
  - 当$|L|=|R|$时，图有完美匹配当且仅当$\det(A)\neq 0$（即$\mathrm{rank}(A)=|L|$）；
  - 图的最大匹配大小为$\mathrm{rank}(A)$。
  - 如何判断$\det(A)$是否等于0，或者计算$\mathrm{rank}(A)$：给定充分大的素数p（比如998244353），在F_p下计算，变量$x_{i,j}$随机取值。

一般图匹配

Problem

给定图$G = (V, E)$，如何求图的最大匹配大小?

- 一般图：考虑Tutte矩阵$A = (a_{i,j})$，其中

$$a_{i,j} = \begin{cases} a_{i,j}x_{i,j} & i < j, \\ -a_{j,i}x_{j,i} & i > j, \\ 0 & i = j. \end{cases}$$

- 图有完美匹配当且仅当$\det(A) = n$：行列式计算中这一项$(-1)^{\tau(\sigma)} \prod_{i=1}^{n} a_{i,\sigma_i}$，当排列$\sigma$出现奇环时，$\sigma$的值加$\sigma^{-1}$的值等于0，两者抵消，因此只计算偶环。
- 图的最大匹配大小等于$\mathrm{rank}(A)/2$。

例题：Divisible Matching

- 给定一个带边权的二部图以及正整数k，每一侧的顶点个数为n。问是否存在完美匹配使得边权之和是k的倍数。
- $n, k \leq 100$。

例题：Divisible Matching

- 考虑素数p满足$p \equiv 1 \mod k$，且g为原根，$g_0 = g^{(p-1)/k}$；
- 令$A^r(i,j) = (x_{i,j} g_0^{w_{i,j}})$ (如果不存在边则该项为0)，此时一个权值和为S的完美匹配给$\det(A^r)$的贡献为（忽略正负号）

$$g_0^S \prod_{i=1}^{n} x_{i,m_i},$$

因此权值和S的完美匹配给$\sum_{i=0}^{k-1} \det(A^r)$的贡献为

$$\sum_{i=0}^{k-1} g_0^S x_{i,m_i},$$

该项不等于0当且仅当$k|S$。