13. 群论: 基本概念 (13-group)

姓名： 鲁权锋 **学号：** 201830168

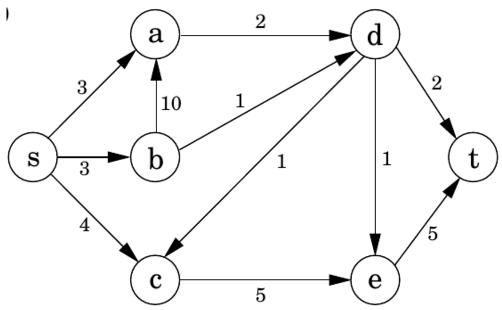
评分： 20 **评阅：** F

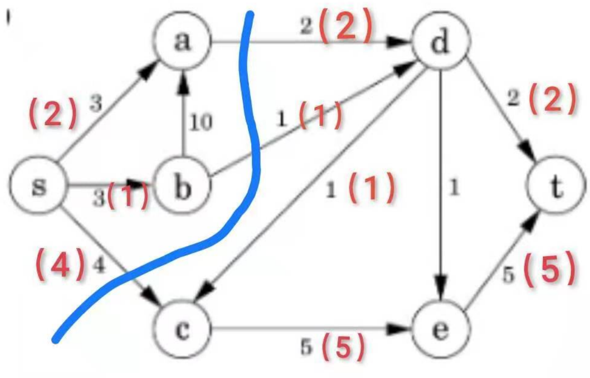
2021 年 6 月 4 日

请独立完成作业，不得抄袭。 若得到他人帮助, 请致谢。 若参考了其它资料，请给出引用。 鼓励讨论，但需独立书写解题过程。

1 作业（必做部分）

题目 1 ([4 分] ⋆⋆)
请给出以下网络的一个最大流与一个最小割。要求给出 Ford-Fulkerson Method 运行过程。





证明：
从 $s-a-d-t$ 有 2 条增广路径;
  从 $s-c-e-t$ 有 4 条增广路径;
  从 $s-b-d-c-e-t$ 有 1 条增广路径.
  除此之外再无从 s 到 t 的增广路径。因此，$max\ val(f) = 2+4+1 = 7$.

4

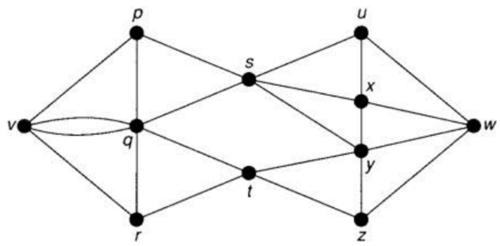
从源点 s 出发，可以通过部分增广路径到达顶点 a, b，因此可以得到如图所示的切割。即 $S = \{s, a, b\}$ $T = \{c, d, e, t\}$ $min\ cap(S, T) = 2+1+4 = 7$.

□

题目 2 ([5 = 1 + 1 + 3 分] ⋆⋆⋆⋆)
考虑下面的定理:

定理 1 (不能告诉你名字的某个著名定理)
设 $G=(V,E)$ 是无向连通图，$v,w\in V$ 是不同的两个顶点。则 v, w 之间的边不相交的 (edge-disjoint) ① 路径的最大条数等于最小 vw-边割集 ② 的大小。

① 设 P_1, P_2 是两条 v、w 间的路径。如果 P_1 与 P_2 没有公共边，则 P_1、P_2 是 v, w 之间的边不相交的路径。
② 设 $F\subseteq E$ 为集。如果 G 删除 F 后，v 与 w 不再连通，则称 F 是 vw-边割集。



(1) 考虑图中的 v, w 顶点。请给出 v、w 间的一个最大边不相交的路径集合。

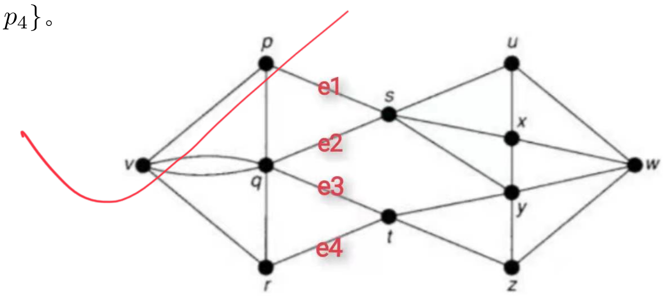
(2) 考虑图中的 v, w 顶点。请给出一个最小的 vw-边割集。

(3) 请使用最大流-最小割定理证明上述定理 ③ 。

③ 恭喜！你刚刚证明了图论中的一个著名定理。

证明：
(1) 记路径 p_1 为 $v-p-s-u-w$;
路径 p_2 为 $v-q-s-x-w$;
路径 p_3 为 $v-q-t-y-w$; (路径 p_3 从 $v-q$ 的部分与路径 p_2 从 $v-q$ 的部分是不同的边)
路径 p_4 为 $v-r-t-z-w$;
v、w 间的一个最大边不相交的路径集合为 $P=\{p_1,\ p_2,\ p_3,\ p_4\}$。

(2) 记边 e_1 为 $p-s$;
边 e_2 为 $q-s$;
边 e_3 为 $q-t$;
边 e_4 为 $r-t$;(如图所示)
一个最小的 vw-边割集为 $E=\{e_1,\ e_2,\ e_3,\ e_4\}$



(3) 用网络流建模：
设源点为 v，汇点为 w , $G=(V,E)$ 的每一条边的容量都赋为 1，且规定从 v 到 w 为正方向，不存在逆向的流.
设 $G=(V,E)$ 的最小 vw-边割集为 E_0，又因为 G 是无向图，且每条边的容量都为 1, 因此，最小割的值为 $min\ cap=|E_0|\times 1=|E_0|$.

设 G 的一个最大的边不相交的路径的集合为 P_0. 又因为 G 是无向图，且每条边的容量都为 1, 可得最大流的值为 $max\ val(f)=|P_0|\times 1=|P_0|$.
仅需将集合 P_0 里的每一条边的流全部赋为 1 即可得到最大流的构造。
除此之外再也没有更大的可行流了：
对任意从 v 到 w 的路径 p, $p\notin P_0$.
那么，集合 P_0 必然存在一条路径 (不妨记为 p_i), p 和 p_i 存在公共边（因为 P_0 是 G 的一个最大的边不相交的路径的集合）(不妨设其中一条公共边是 e)。
因为 G 是无向图，且每条边的容量都为 1, 因此路径 p 必然不是增广路径 (因为 e 已经达到最大流量).
因此，不会有更大的最大流。

又因为 $max\ val(f)=min\ cap$，故得 $|E_0|=|P_0|$
即 v, w 之间的边不相交的路径的最大条数等于最小 vw-边割集的大小。

□

题目 3 ([3 分] ★★)
在整数集 $\mathbb{Z}$ 中, 规定运算 $\oplus$ 如下:

$$\forall a, b \in \mathbb{Z}, a \oplus b = a + b - 2.$$

请证明: $(\mathbb{Z}, \oplus)$ 构成群。

证明:
(1)

$$\forall a, b \in \mathbb{Z},\ \ a \oplus b = a + b - 2 \in \mathbb{Z}.$$

因此 $(\mathbb{Z}, \oplus)$ 是封闭的。
(2)

$$\forall a, b, c \in \mathbb{Z},$$

3

$$\begin{aligned}(a \oplus b) \oplus c &= (a + b - 2) \oplus c \\ &= (a + b - 2) + c - 2 \\ &= a + b + c - 4\end{aligned}$$

$$\begin{aligned}a \oplus (b \oplus c) &= a \oplus (b + c - 2) \\ &= a + (b + c - 2) - 2 \\ &= a + b + c - 4\end{aligned}$$

因此

$$(a \oplus b) \oplus c = a \oplus (b \oplus c)$$

因此 $(\mathbb{Z}, \oplus)$ 具有结合律。
(3)

$$\forall a \in \mathbb{Z},$$

$$a \oplus 2 = a + 2 - 2 = a.$$

$$2 \oplus a = 2 + a - 2 = a.$$

即

$$a \oplus 2 = 2 \oplus a == a.$$

因此 $(\mathbb{Z}, \oplus)$ 有单位元 $e = 2$。
(4)

$$\forall a \in \mathbb{Z}.\ \exists b = 4 - a \in \mathbb{Z}.$$

使得

$$a \oplus b = a + (4 - a) - 2 = 2 = e$$

$$b \oplus a = (4 - a) + a - 2 = 2 = e$$

即

$$a \oplus b = b \oplus a = e$$

即 $(\mathbb{Z}, \oplus)$ 中每一个元素都存在逆元。

结合 (1)(2)(3)(4), $(\mathbb{Z}, \oplus)$ 构成群。 □

题目 4 ([5 分] ⋆⋆⋆)
设 G 是群。请证明：如果 $\forall x \in G.\ x^2 = e$，则 G 是交换群。

证明：

5

$$\forall a, b \in G,$$

有

$$ab \in G, ba \in G$$

根据题设，有

$$a^2 = b^2 = (ab)(ab) = e \qquad (1)$$

因此可得

$$\begin{aligned}(ab)(ba) &= a(bb)a \\ &= aea \\ &= aa \\ &= e \qquad (2)\end{aligned}$$

结合 (1)(2)，有

$$\begin{aligned} & (ab)(ba) = (ab)(ab) \\ \iff & \quad ab = ba \end{aligned}$$

因此，G 是交换群。 □

题目 5 ([3 分] ⋆⋆)
请求出 3^{83} 的最后两位数 ④ 。要求给出计算过程。

④ https://www.wolframalpha.com/input/?i=3%5E83

证明：
可以构造一个单位元 $e = 1$ 的模 100 剩余类乘法群：

3

$$\mathbb{U}_{(100)} = \{a \in \mathbb{Z}_{(100)} | (a, 100) = 1\}$$

其中 $\mathbb{Z}_{(100)}$ 是模 100 剩余类加法群。又因为

$$\begin{aligned}|\mathbb{U}_{(100)}| &= \varphi(100) \\ &= 100 * (1 - \frac{1}{2}) * (1 - \frac{1}{5}) \\ &= 40\end{aligned}$$

又因为 $\mathbb{U}_{(100)}$ 是交换群（因为该群的操作符乘号是存在交换律的），故有

$$\forall a \in \mathbb{U}_{(100)}.\ a^{40} = e = 1$$

显然 $3 \in \mathbb{U}_{(100)}$，结合上式，即得

$$3^{40} \equiv 1 (mod \ \ 100)$$

因此，

$$3^{83} = 3^{40+40+3} = (3^{40})^2 * 3^3 \equiv 1^2 * 27 \equiv 27 (mod \ \ 100)$$

即 3^{83} 的最后两位数是 27。 □
