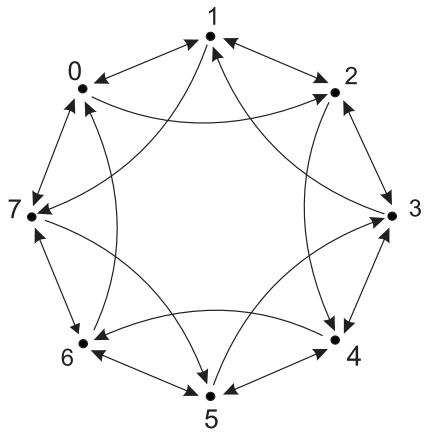
50 Граф

Задача. В функции хэширования `Bash` план криптографического перемешивания задается специальным ориентированным графом. Это граф на 8 вершинах, из каждой вершины выходит 3 дуги, в каждую вершину заходит 3 дуги, любые 2 вершины можно соединить маршрутом длины 2, в любую вершину можно вернуться за 2 шага ровно 2 способами. Докажите, что любой подходящий граф перенумерацией вершин можно преобразовать в следующий:



Решение. Из вершины v можно вернуться в саму себя за 2 шага 2 способами: по маршруту (v, v', v) и по маршруту (v, v'', v). Эти маршруты описывают двойные (двунаправленные) дуги $[v, v']$ (между v и v') и $[v, v'']$ (между v и v''). Двойные дуги индуцируют двойные циклы: двойной цикл $[v_0, v_1, v_2, \ldots, v_{n-1}, v_0]$ состоит из двойных дуг $[v_0, v_1], [v_1, v_2], \ldots, [v_{n-1}, v_0]$.

Из вершины v выходит еще одна дуга (v, v'''), которая не лежит двойных циклах. Назовем эту дугу ординарной. Ординарные дуги индуцируют ординарные циклы: ординарный цикл $(v_0, v_1, v_2, \ldots, v_{n-1}, v_0)$ состоит из ординарных дуг $(v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_0)$.

Двойные циклы длины 1 и 2 запрещены. Поэтому возможны 3 варианта двойного циклового строения:

1. Полный двойной цикл длины 8.

2. Два двойных цикла длины 4.

3. Двойной цикл длины 5 и двойной цикл длины 3.

Второй вариант невозможен. Действительно, если $[v_0, v_1, v_2, v_3, v_0]$ — искомый цикл, то вершина v_0 соединяется с v_2 двумя маршрутами длины 2: (v_0, v_1, v_2) и (v_0, v_3, v_2). Это запрещено.

Рассмотрим третий вариант. Пусть $[v_0, v_1, v_2, v_0]$ — двойной цикл длины 3. Из каждой вершины v_i выходит одна дуга за пределы цикла. Пусть это дуга в вершину u_i. Вершины u_i лежат на двойном цикле длины 5. Поэтому сушествует две вершины u_i, между которыми имеется двойная дуга. Пусть это вершины u_0 и u_1. Тогда v_0 соединяется с u_1 двумя маршрутами длины 2: (v_0, u_0, u_1) и (v_0, v_1, u_1). Это запрещено.

Остается первый вариант двойного циклового строения. Перенумерацией вершин добъемся того, что двойной цикл имеет вид $[0, 1, 2, \ldots, 7, 0]$. Остается определиться с одинарными дугами. Докажем, что они могут иметь только следующий вид: $(i, i+2)$ или $(i, i-2)$ (здесь и далее сложение и вычитание выполняются по модулю 8).

Действительно,

а) при наличии дуги $(i, i+1)$ из i можно попасть только в 2 вершины за 1 шаг и, следовательно, не более чем в 6 вершин за два шага;

b) если есть дуга $(i, i+3)$, то в $i+3$ нельзя попасть из i за два шага: можно попасть или из $i+2$, или из $i+4$, но дуги $(i, i+2)$ и $(i, i+4)$ отсутствуют;

c) если есть дуга $(i, i+4)$, то в $i+4$ нельзя попасть из i за два шага: можно попасть или из $i+3$, или из $i+5$, но дуги $(i, i+3)$ и $(i, i+5)$ отсутствуют;

d) дуга $(i, i+5)$ запрещается также, как дуга $(i, i+3)$, дуга $(i, i+7)$ — также, как $(i, i+1)$.

В силу ограничений на ординарные дуги, ординарные циклы могут иметь только следующий вид: $(i, i+2, i+4, i+6, i)$ (цикл по часовой стрелке) или $(i, i-2, i-4, i-6, i)$ (против часовой). Циклы должны иметь разное направление. Циклически свигая номера вершин графа можно привести его к виду, изображенному на рисунке. □