# 付録N



# 「観光地 – 支配集合」の学習

#### 学習活動

作った人しか答えがわからない地図を作る。

- (1) いくつかの交差点にアイスクリームワゴンが隠された地図を作る。
- (2) 地図を交換し、どこにアイスクリームワゴンがあるかを当てさせる。

#### 準備物

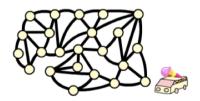
地図を描くワークシート。

### 解説

- 一方向性関数は「A から B を求めるのは容易だが、B から A を推測するのは難しい」性質を持つ。
- 一方向性関数を解くのは難しく、すべての場合を試すやり方だと膨大な時間がかかる。

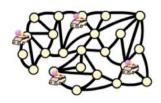
#### 1. クイズ

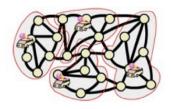
どの道にいる人もその道のどちらかの端にある交差点で買えるように販売車 (アイスクリームワゴン) を置きたい。どこに置けばいちばん少ない台数にできるだろうか。



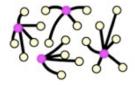
### 2. クイズの答えの説明

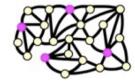
ワゴンのいる交差点が他の交差点の親になっている様子を説明する。

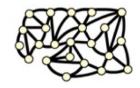




### 3. 地図の作り方の説明







- (1) 交差点の親と子を作る
- (2) 子同士をつなぐ
- (3) 親と子の区別をなくす
- ※(1) か(2) を保存しておかないと、作った本人も答えがわからなくなる可能性がある。

## 4. 地図製作用のプリントを配布

| 例   | 地図製作シート |
|-----|---------|
| 保存用 | 保存用     |
|     |         |
| 交換用 | 交換用     |
|     |         |

### 5. 地図を交換して答え探し

- 生徒は2人一組になる。
- 生徒が制作した地図から「交換用」を切り取って、相手の生徒と交換する。
- 受け取った地図の答えを見つける。

# 6. 先生によるまとめ

- •「作る事は簡単だが、解くことは難しい」ことを確認させる。
- このような性質は「一方向性」と呼ばれることを説明する。
- •「一方向性」は、大きな数の素因数分解などにもあることを説明する。
- 「一方向性」は、情報を安全にやり取りする暗号技術に使われていることを説明する。