Math 235 Fall 2024, Lecture 7 stenogram: The pigeonhole principle

website: `https://www.cip.ifi.lmu.de/~grinberg/t/24f`

1. The pigeonhole principle

The **pigeonhole principle** is several interconnected principles about finite sets, all intuitively obvious. Here are the pigeonhole principles relating to injections:

Theorem 1.0.1. Let U and V be two finite sets such that $|U| > |V|$. Then, there is no injective map $f : U \to V$.

Theorem 1.0.2. Let U and V be two finite sets such that $|U| = |V|$. Then, any injective map $f : U \to V$ is bijective.

In terms of pigeons and holes, this is saying that

- if k pigeons sit in fewer than k holes, then two pigeons must be in the same hole;
- if k pigeons sit in exactly k holes, then each hole has exactly 1 pigeon.

Here is a corollary that is really a restatement of the first theorem:

Corollary 1.0.3. Let $n, m \in \mathbb{N}$ be such that $m > n$. Let $a_1, a_2, \ldots, a_m$ be m elements of a given n-element set V. Then, at least two of these m elements are equal.

Proof. Consider the map $f : \{1, 2, \ldots, m\} \to V$ that sends each i to a_i. By the first theorem above, this map f cannot be injective. In other words, there exist $i \neq j$ such that $f(i) = f(j)$. But this means $a_i = a_j$. $\square$

There are variants of the pigeonhole principle for non-injections, telling us how non-injective maps have to be depending on the sizes of the sets. Here are the simplest forms, which I call the **multi-injection pigeonhole principles** (the original principles are obtained for $k = 1$):

Theorem 1.0.4. Let U and V be two finite sets. Let $k \in \mathbb{N}$. Let $f : U \to V$ be a map. Assume that every $v \in V$ satisfies

$$(\text{the number of all } u \in U \text{ such that } f(u) = v) \leq k.$$

Then, $|U| \leq k\,|V|$.

Theorem 1.0.5. Let U and V be two finite sets. Let $k \in \mathbb{N}$. Let $f : U \to V$ be a map. Assume that every $v \in V$ satisfies

$$(\text{the number of all } u \in U \text{ such that } f(u) = v) \leq k.$$

Assume that $|U| = k|V|$. Then, every $v \in V$ satisfies

$$(\text{the number of all } u \in U \text{ such that } f(u) = v) = k.$$

In terms of pigeons,

- if each hole contains at most k pigeons, then there are at most k many times as many pigeons as holes;
- if equality holds, then equality holds in each hole.

There are also versions of the pigeonhole principle for surjections:

Theorem 1.0.6. Let U and V be two finite sets such that $|U| < |V|$. Then, there is no surjective map $f : U \to V$.

Theorem 1.0.7. Let U and V be two finite sets such that $|U| = |V|$. Then, any surjective map $f : U \to V$ is bijective.

In terms of pigeons and holes:

- if there are fewer pigeons than holes, then some holes will be empty;
- if there are equally many pigeons and holes, and if no holes are empty, then no pigeons are roommates.

For infinite sets, some of this fails. For example, the map

$$\mathbb{N} \to \mathbb{N},$$
$$n \mapsto n//2$$

is surjective but not injective.

Let us see how these principles can be used. Some examples:

- Among any 13 persons, there are two that are born in the same month.

  Proof. Pigeons = the 13 people; holes = the 12 months. Or, formally:

  $$U = \{\text{the 13 people}\}, \qquad V = \{\text{the 12 months}\},$$
  $$f(u) = (\text{the month when } u \text{ was born}).$$

  By the pigeonhole principle, f cannot be injective, and we are done.

- There are two people alive right now that have the exact same number of hairs of their heads.

  Proof. Any human has at most 5 000 000 hairs on his head (in fact, typically around 100 000). But there are more than 5 000 001 humans. So the pigeonhole principle does its job:

$$U = \{\text{humans}\}, \qquad V = \{0, 1, \ldots, 5\,000\,000\},$$
$$f(u) = (\text{\# of hairs on } u).$$

- If 26 mosquitoes are hanging on a $1\,\text{m} \times 1\,\text{m}$-sized rectangular window, and you have a $20\,\text{cm} \times 20\,\text{cm}$-sized rectangular flyswatter, then you can hit at least two mosquitoes with one strike.

  Proof. Subdivide the window into 25 flyswatter-sized squares. One of these will contain 2 or more mosquitoes. Hit that.

- Consider a triangle ABC, and a straight line ℓ in its plane. Assume that ℓ contains none of the vertices A, B, C. Then, the line ℓ cannot cut more than two sides of $\triangle ABC$.

  Proof. If ℓ cuts a segment XY without passing through either of its endpoints, then the two points X and Y must lie on different sides of ℓ. Thus, if the line ℓ would cut more than two sides of $\triangle ABC$, then any two of A, B, C would lie on different sides of ℓ. But there are only two sides of ℓ.

- Let's make things more complicated by going into 3-dimensional space.

  Consider a tetrahedron $ABCD$, and a plane p that contains none of the vertices A, B, C, D. How many edges of $ABCD$ can this plane p cut?

  Argue similarly to the previous example: The plane p breaks the space into two sides (= halfspaces). If there k vertices of $ABCD$ on one side and $4 - k$ on the other, then the number of edges of $ABCD$ that p cuts is $k(4-k)$. For $k = 0, 1, 2, 3, 4$, this number is $0, 3, 4, 3, 0$, so its maximum value is 4. And indeed, 4 is possible, as you can see by the fact that the midpoints of the segments AB, BC, CD, DA lie on one plane (and in fact form a parallelogram: in terms of vector algebra, this is saying that $\dfrac{A+B}{2} - \dfrac{B+C}{2} = \dfrac{D+A}{2} - \dfrac{C+D}{2}$, which is obvious by computation).

- Let's vary this somewhat:

  Consider a tetrahedron $ABCD$, and a plane p that contains none of the vertices A, B, C, D. How many faces of $ABCD$ can this plane p cut?

  The answer is again 4. The example is again the plane through the midpoints of the segments AB, BC, CD, DA. Clearly, no more than 4 is possible, since $ABCD$ has only 4 faces.

- Another variant:

  Consider a tetrahedron $ABCD$, and a line ℓ that contains none of the vertices A, B, C, D. How many edges of $ABCD$ can this line ℓ cut?

  If ℓ lies on one of the face-planes of $ABCD$, then ℓ can only cut 2 edges at most. If ℓ does not lie on any face-plane of $ABCD$, then ℓ can still only cut 2 edges at most, because any two edges that ℓ cuts cannot have any vertices in common, but this would force $ABCD$ to have 6 vertices if it cut 3 edges. So, in total, the maximum number is 2.

- A final variant:

  Consider a tetrahedron $ABCD$, and a line ℓ that contains none of the vertices A, B, C, D. How many faces of $ABCD$ can this line ℓ cut?

  The maximum is again 2. The reason now is coming from convexity: When ℓ intersects a face, it is either entering or exiting the tetrahedron $ABCD$. But $ABCD$ is convex, so a line cannot enter it twice or exit it twice.

- Among any 25 people, there are three that are born in the same month.

  Proof. Use the multi-injection pigeonhole principle for $k = 2$.

- If n is a positive integer, and if $x_1, x_2, \ldots, x_{n+1}$ are any $n+1$ integers, then at least two of these $n+1$ integers $x_1, x_2, \ldots, x_{n+1}$ are congruent modulo n.

  Proof: The map

  $$f : \{1, 2, \ldots, n+1\} \to \{0, 1, \ldots, n-1\},$$
  $$i \mapsto x_i \% n$$

  cannot be injective (by the pigeonhole principle), since its domain is larger than its target.

- If $n+1$ distinct numbers are selected from the set $\{1, 2, \ldots, 2n\}$ (for some positive integer n), then some two of these $n+1$ numbers sum to $2n+1$.

  Proof: The pigeons are the $n+1$ chosen numbers. The holes are the two-element sets

  $$\{1, 2n\}, \quad \{2, 2n-1\}, \quad \{3, 2n-2\}, \quad \ldots, \quad \{n, n+1\}.$$

  By the pigeonhole principle, two pigeons must lie in the same hole. Being distinct, they must thus sum to $2n+1$.

Another application of the pigeonhole principle is itself a useful fact:

Corollary 1.0.8. Let U and V be two finite sets such that $|U| \leq |V|$. Let $f : U \to V$ and $g : V \to U$ be two maps such that $f \circ g = \mathrm{id}_V$. Then, f and g are mutually inverse.

Proof. The assumption $f \circ g = \mathrm{id}_V$ shows that f is surjective. But the pigeonhole principle for surjections shows that this is only possible if $|U| \geq |V|$, and that in the case $|U| = |V|$, this entails that f is bijective. Since we have $|U| \leq |V|$, we thus can apply this, and conclude that f is bijective. Hence, f has an inverse f^{-1}. Now, $f \circ g = \mathrm{id}_V$ yields $f^{-1} \circ f \circ g = f^{-1} \circ \mathrm{id}_V = f^{-1}$, that is, $g = f^{-1}$. But this means that f and g are mutually inverse. □

Incidentally, similar properties hold in linear algebra:

- If $f : U \to V$ is a linear map between two finite-dimensional vector spaces over a field, and if $\dim U > \dim V$, then f cannot be injective.
- If $f : U \to V$ is an injective linear map between two finite-dimensional vector spaces over a field, and if $\dim U = \dim V$, then f is bijective (thus an isomorphism).
- If $f : U \to V$ is a linear map between two finite-dimensional vector spaces over a field, and if $\dim U < \dim V$, then f cannot be surjective.
- If $f : U \to V$ is a surjective linear map between two finite-dimensional vector spaces over a field, and if $\dim U = \dim V$, then f is bijective (thus an isomorphism).

In terms of matrices, these are known facts about kernels (= nullspaces):

- A wide matrix A has a nonzero right kernel (that is, some $v \neq 0$ such that $Av = 0$).
- A tall matrix A has a nonzero left kernel (that is, some $v \neq 0$ such that $vA = 0$).
- A square matrix with a zero right kernel or a zero left kernel is invertible.

Exercise 1. Let $n \geq 2$ be an integer. At a conference, some n people have met and exchanged handshakes. Prove that there are two people that have shaken hands with the same number of people. (We assume that no one shakes his own hands.)

Solution. Let

- the pigeons be the n people;

- the holes be the numbers $0, 1, \ldots, n-1$;
- the pigeon-hole assignment is that each person gets assigned the number of hands he has shaken.

We would like to apply the pigeonhole principle, but there is a problem: the # of holes = the # of pigeons. So what we get is that the assignment is bijective.

More rigorously: Assume the contrary (i.e., no two people have shaken the same # of hands). We let

$$U = \{\text{the } n \text{ people}\}, \qquad V = \{0, 1, \ldots, n-1\},$$
$$f(u) = (\text{\# of hands shaken by } u).$$

Then, $f : U \to V$ is injective (by assumption). Hence, by the pigeonhole principle, f is bijective (since $|U| = |V|$). So some person u satisfies $f(u) = 0$, and some person v satisfies $f(v) = n-1$. These u and v are distinct (since $n \geq 2$). Now, $f(u) = 0$ yields that u has not shaken v's hands, whereas $f(v) = n-1$ yields that v has shaken u's hands. Contradiction!

Theorem 1.0.9 (the Chinese Remainder Theorem, simplest form)**.** Let a and b be two coprime positive integers. Then, for any integers y and z, there exists an integer x such that

$$x \equiv y \bmod a \qquad \text{and} \qquad x \equiv z \bmod b.$$

Proof. Consider the map

$$f : \{0, 1, \ldots, ab-1\} \to \{0, 1, \ldots, a-1\} \times \{0, 1, \ldots, b-1\},$$
$$x \mapsto (x\%a,\ x\%b).$$

Claim 1: This map f is injective.

Proof of Claim 1. Let u and v be two elements of $\{0, 1, \ldots, ab-1\}$ such that $f(u) = f(v)$. We must show that $u = v$.

We have $f(u) = (u\%a,\ u\%b)$ and $f(v) = (v\%a,\ v\%b)$. Thus, $f(u) = f(v)$ entails that $u\%a = v\%a$ and $u\%b = v\%b$. In other words, $u \equiv v \bmod a$ and $u \equiv v \bmod b$. In other words, $a \mid u - v$ and $b \mid u - v$. Since a and b are coprime, this entails that $ab \mid u - v$. In other words, $u \equiv v \bmod ab$. But u and v are two elements of $\{0, 1, \ldots, ab-1\}$, so $u \equiv v \bmod ab$ entails $u = v$. This proves Claim 1.

But f is a map from the set $\{0, 1, \ldots, ab-1\}$ to the set $\{0, 1, \ldots, a-1\} \times \{0, 1, \ldots, b-1\}$. Both of these sets have size ab. So the map f, being injective, must be bijective (by the pigeonhole principle). In particular, it is surjective.

Now, the pair $(y\%a,\ z\%b)$ lies in the set $\{0, 1, \ldots, a-1\} \times \{0, 1, \ldots, b-1\}$. Since f is surjective (being bijective), there must thus be an $x \in \{0, 1, \ldots, ab-1\}$ such that $f(x) = (y\%a,\ z\%b)$. Thus, it satisfies $(x\%a,\ x\%b) = f(x) = (y\%a,\ z\%b)$, so that $x\%a = y\%a$ and $x\%b = z\%b$, so that $x \equiv y \mod a$ and $x \equiv z \mod b$. This proves the theorem. □

Theorem 1.0.10. Let X be a finite set. Let $n = |X|$. Let $f : X \to X$ be a map. Let $x \in X$. Then:

(a) There exist two nonnegative integers $i < j \leq n$ such that $f^i(x) = f^j(x)$.

(b) Let i and j be two nonnegative integers with $i < j$ and $f^i(x) = f^j(x)$. Then, the sequence

$$\left(f^i(x),\ f^{i+1}(x),\ f^{i+2}(x),\ \ldots\right)$$

is $(j-i)$-periodic.

(c) If f is a permutation (= a bijection), then there exists a positive integer $j \leq n$ such that $f^j(x) = x$, and the whole sequence $\left(f^0(x),\ f^1(x),\ f^2(x),\ \ldots\right)$ is j-periodic.

Proof. (See the notes – Theorems 6.2.5 and 6.2.8 – for details.)

(a) The $n+1$ elements $f^0(x),\ f^1(x),\ \ldots,\ f^n(x)$ of the n-element set X cannot be all distinct (by the pigeonhole principle).

(b) Rigorously, this is an induction argument. Informally, this is because once this sequence cycles back to its start, it must proceed exactly as it did the first time over.

(c) Apply part **(a)**, but notice that i cannot be positive, since $f^i(x) = f^j(x)$ entails $f^{i-1}(x) = f^{j-1}(x)$ by the injectivity of f. □

See the notes for further properties of maps $f : X \to X$ on a finite set X.