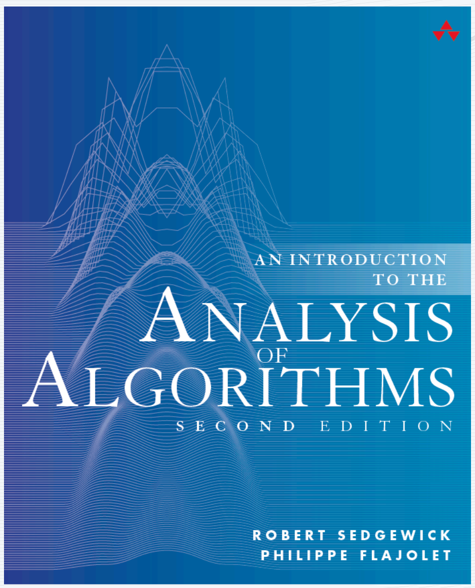


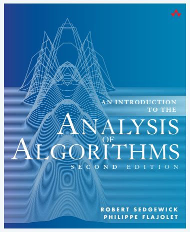
http://aofa.cs.princeton.edu

7. Permutations

Orientation

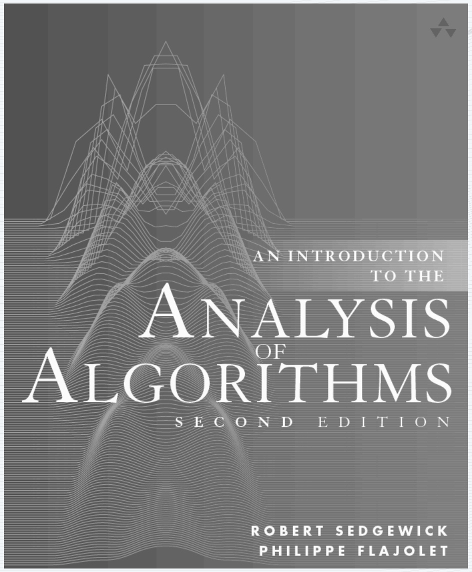
Second half of class

- Surveys fundamental combinatorial classes.
- Considers techniques from analytic combinatorics to study them .
- Includes applications to the analysis of algorithms.



chapter	*combinatorial classes*	*type of class*	*type of GF*
6	Trees	unlabeled	OGFs
7	Permutations	labeled	EGFs
8	Strings and Tries	unlabeled	OGFs
9	Words and Mappings	labeled	EGFs

Note: Many more examples in book than in lectures.



http://aofa.cs.princeton.edu

7. Permutations

- **Basics**
- Sets of cycles
- Left-right-minima
- Other parameters
- BGFs and distributions

Basics

Definition. A permutation is an ordering or the numbers 1 through *N*.

Ex. A group of *N* students who live in single rooms go to a party that leads to a state of inebriation. When returning, they each end up in a random room.

student	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
room	9	12	11	10	5	15	1	3	7	6	13	8	2	16	4	14

Review: permutations

Def. A *permutation* is a sequence of labelled atoms.

1

$P_1 = 1$

1 2
2 1

$P_2 = 2$

1 2 3
2 1 3
3 1 2
1 3 2
2 3 1
3 2 1

$P_3 = 6$

1 2 3 4 | 1 2 4 3
2 1 3 4 | 2 1 4 3
3 1 2 4 | 3 1 4 2
4 1 2 3 | 4 1 3 2
1 3 2 4 | 1 3 4 2
2 3 1 4 | 2 3 4 1
3 2 1 4 | 3 2 4 1
4 2 1 3 | 4 2 3 1
1 4 2 3 | 1 4 3 2
2 4 1 3 | 2 4 3 1
3 4 1 2 | 3 4 2 1
4 3 1 2 | 4 3 2 1

$P_4 = 24$

counting sequence	*EGF*
$P_N = N!$	$\frac{1}{1-z}$

$$\sum_{N\geq 0} \frac{N!z^N}{N!} = \sum_{N\geq 0} z^N = \frac{1}{1-z}$$

Inverse

Alternate def. A *permutation* is a mapping of the numbers 1 through N to itself.

student	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
room	9	12	11	10	5	15	1	3	7	6	13	8	2	16	4	14

Def. The *inverse* of a permutation is the inverse of that mapping.

student	7	13	8	15	5	10	9	12	1	4	3	2	11	16	6	14
room	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

room	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
student	7	13	8	15	5	10	9	12	1	4	3	2	11	16	6	14

Computing the inverse of a permutation

```
public static int[] inverse(int[] a)
{
   int N = a.length;
   int[] b = new int[N];
   for (int i = 0; i < N; i++)
      b[a[i]-1] = i+1;
   return b;
}
```

Java arrays are 0-based

permutation

1	2	3	4	5	6	7	8	9
8	1	3	7	6	2	9	4	5

inverse

							1	
2							1	
2		3					1	
2		3				4	1	
2		3			5	4	1	
2	6	3			5	4	1	
2	6	3			5	4	1	7
2	6	3	8		5	4	1	7
2	6	3	8	9	5	4	1	7

Application: Substitution cipher

Algorithm (traditional)

- Generate random permutation of A-Z (stay tuned).
- Apply as a mapping to encrypt.
- Use inverse to decrypt.

Encryption

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	-
random permutation	W	V	L	Q	I	X	J	A	B	G	-	U	N	F	K	R	Y	C	D	P	Z	E	O	M	H	T	S

plaintext	A	T	T	A	C	K	-	A	T	-	D	A	W	N
ciphertext	W	P	P	W	L	-	S	W	P	S	Q	W	O	F

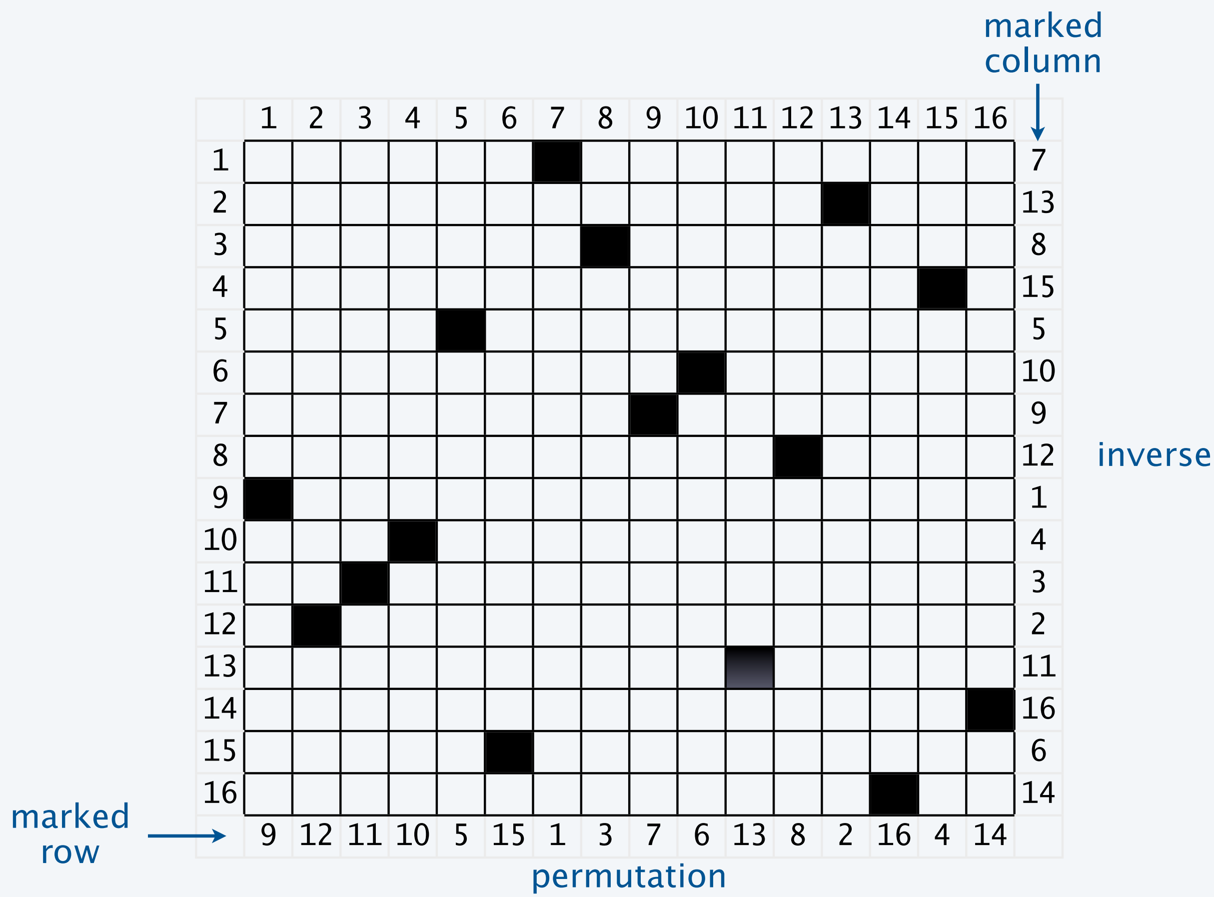
Decryption

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	-
inverse	H	I	R	S	V	N	J	Y	E	G	O	C	X	M	W	T	D	P	-	Z	L	B	A	F	Q	U	K

ciphertext	W	P	P	W	L	-	S	W	P	S	Q	W	O	F
plaintext	A	T	T	A	C	K	-	A	T	-	D	A	W	N

Caveat. Not useful in modern applications because of susceptibility to character frequency analysis.

Lattice representation of a permutation

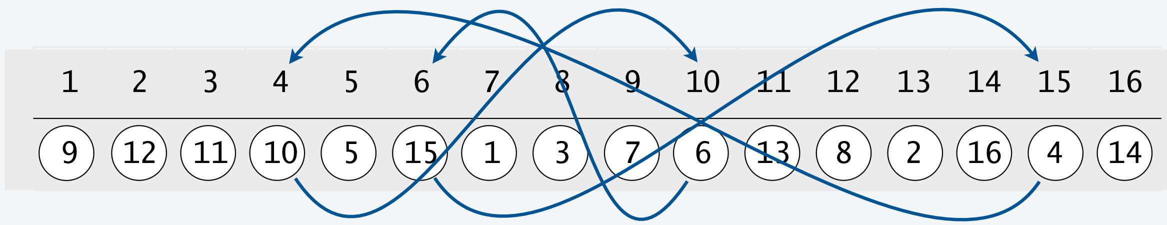


Implication. Representation of inverse is *transpose* of representation of permutation.

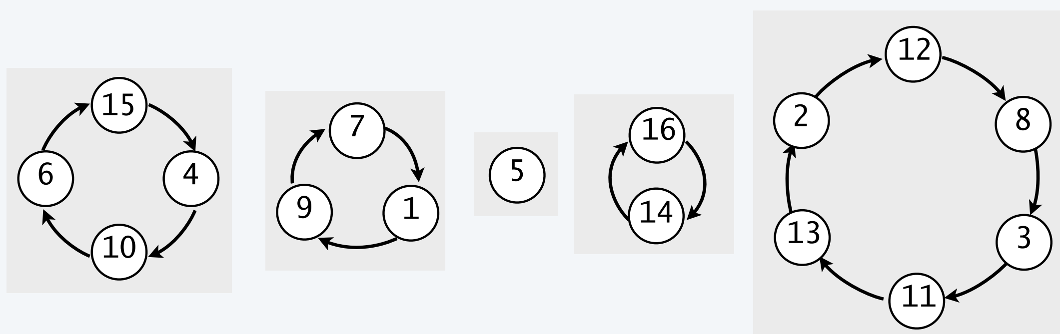
Review: A combinatorial bijection

Alternate def. A permutation is a set of cycles.

Standard representation



Set of cycles representation



Review: The symbolic method for labelled classes (transfer theorem)

Theorem. Let A and B be combinatorial classes of labelled objects with EGFs $A(z)$ and $B(z)$. Then

construction	*notation*	*semantics*	*EGF*
disjoint union	$A + B$	disjoint copies of objects from A and B	$A(z) + B(z)$
labelled product	$A \star B$	ordered pairs of copies of objects, one from A and one from B	$A(z)B(z)$
sequence	$SEQ_k(A)$	k- sequences of objects from A	$A(z)^k$
	$SEQ(A)$	sequences of objects from A	$\frac{1}{1 - A(z)}$
set	$SET_k(A)$	k-sets of objects from A	$A(z)^k/k!$
	$SET(A)$	sets of objects from A	$e^{A(z)}$
cycle	$CYC_k(A)$	k-cycles of objects from A	$A(z)^k/k$
	$CYC(A)$	cycles of objects from A	$\ln \frac{1}{1 - A(z)}$

Review: symbolic method to count permutations

How many permutations of length N?

Class	P, the class of all permutations
Size	$\|p\|$, the length of p
OGF	$P(z) = \sum_{p \in P} \frac{z^{\|p\|}}{\|p\|!} = \sum_{N \geq 0} P_N \frac{z^N}{N!}$

Atom

type	*class*	*size*	*GF*
labelled atom	Z	1	z

Construction $$P = E + Z \star P$$

"a permutation is empty or an atom and a permutation"

OGF equation $$P(z) = 1 + zP(z)$$

Solution $$P(z) = \frac{1}{1-z}$$

$$N![z^N]P(z) = N! \checkmark$$

Application: Sorting algorithms

```
[hundreds of algorithms since 1950]
{
}
```

```
public class Merge
{
}
```

```
public class Quick
{
   private static int partition(Comparable[] a, int lo, int hi)
   {
      int i = lo, j = hi+1;
      while (true)
      {
         while (less(a[++i], a[lo])) if (i == hi) break;
         while (less(a[lo], a[--j])) if (j == lo) break;
         if (i >= j) break;
         exch(a, i, j);
      }
      exch(a, lo, j);
      return j;
   }

   private static void sort(Comparable[] a, int lo, int hi)
   {
      if (hi <= lo) return;
      int j = partition(a, lo, hi);
      sort(a, lo, j-1);
      sort(a, j+1, hi);
   }
}
```

input (maybe not in random order)

T S R P O N M L I

random permutation of the input

N L T R M O I P S

sorted output

I L M N O P R S T

Q. Model for input?

A. Random permutation.

Q. Realistic?

Q. Absolutely, if we put entries in random order before the sort!

Chapter 2

Application: Randomly permuting an array/generate a random permutation

Algorithm (Knuth)

- Move from left to right.
- Exch each entry with a *random* entry to its right.

```
for (int i = 0; i < N; i++)
{
   int r = i + StdRandom.uniform(N-i);
   int t = a[r]; a[r] = a[i]; a[i] = t;
}
```

All permutations are equally likely:

- 1st entry equally likely to be any of the N entries.
- 2nd equally likely to be any of the $N-1$ remaining entries.
- 3rd equally likely to be any of the $N-2$ remaining entries.
- ...

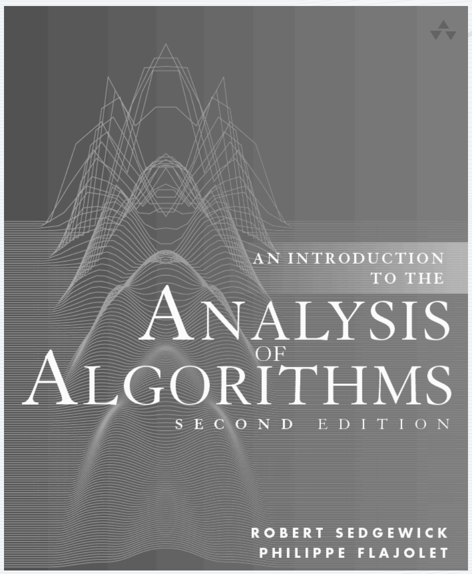
input (maybe not in random order)

T	S	R	P	O	N	M	L	I
N	S	R	P	O	**T**	M	L	I
N	**L**	R	P	O	T	M	**S**	I
N	L	**T**	P	O	**R**	M	S	I
N	L	T	**R**	O	**P**	M	S	I
N	L	T	R	**M**	P	**O**	S	I
N	L	T	R	M	**O**	P	S	I
N	L	T	R	M	O	**I**	S	**P**
N	L	T	R	M	O	I	**P**	**S**

random permutation of the input

N	L	T	R	M	O	I	P	S
6	8	1	3	7	5	9	4	2

use 1 2 3 4 5 6 7 8 9 as input to get a random *permutation* ⟶ 6 8 1 3 7 5 9 4 2



http://aofa.cs.princeton.edu

7. Permutations

- Basics
- **Sets of cycles**
- Left-right-minima
- Other parameters
- BGFs and distributions

Review: Permutations and derangements

How many sets of cycles of length N?

"A permutation is a set of cycles"

Construction	$P^* = SET(CYC(Z))$
EGF equation	$P^*(z) = \exp\left(\ln \frac{1}{1-z}\right) = \frac{1}{1-z}$
Counting sequence	$P^*_N = N![z^N]P^*(z) = N!$

How many derangements of length N?

"Derangements are permutations with no singleton cycles"

Construction	$D = SET(CYC_{>1}(Z))$
EGF equation	$D(z) = e^{z^2/2+z^3/3+z^4/4+\dots} = \exp\left(\ln \frac{1}{1-z} - z\right) = \frac{e^{-z}}{1-z}$
Expansion	$[z^N]D(z) \equiv \frac{D_N}{N!} = \sum_{0\le k\le N} \frac{(-1)^k}{k!} \sim \frac{1}{e}$

Review: generalized derangements

How many permutations of length N have no cycles of length $\leq M$?

Construction $$D_M = SET(CYC_{>M}(Z))$$

OGF equation $$D_M(z) = e^{\frac{z^{M+1}}{M+1}+\frac{z^{M+2}}{M+2}+\ldots} = \exp\Big(\ln\frac{1}{1-z} - z - z^2/2 - \ldots - z^M/M\Big)$$

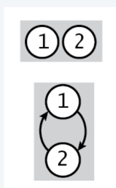
$$= \frac{e^{-z-\frac{z^2}{2}-\frac{z^3}{3}-\ldots\frac{z^M}{M}}}{1-z}$$

Asymptotics $$[z^N]D_M(z) \sim \frac{N!}{e^{H_M}}$$

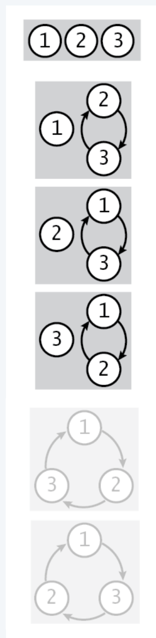
Involutions

are permutations composed of cycles of length 1 or 2.

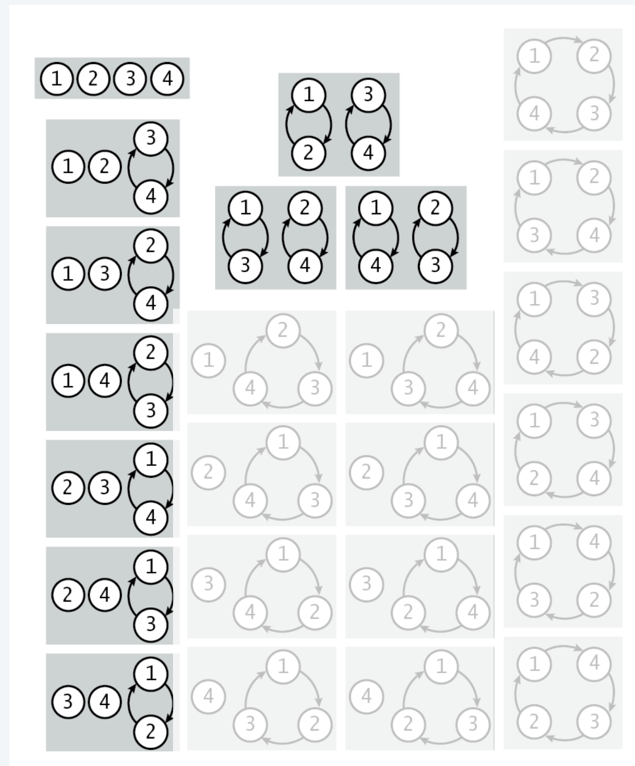
$I_1 = 1$



$I_2 = 2$



$I_3 = 4$



$I_4 = 10$

Review: Inverse

Alternate def. A *permutation* is a mapping of the numbers 1 through *N* to itself.

index	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
permutation	9	12	11	10	5	15	1	3	7	6	13	8	2	16	4	14

Def. The *inverse* of a permutation is the inverse of that mapping.

7	13	8	15	5	10	9	12	1	4	3	2	11	16	6	14
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

index	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
inverse	7	13	8	15	5	10	9	12	1	4	3	2	11	16	6	14

Q. What is the inverse of an *involution*?

Inverse of an involution

An *involution* is a mapping of the numbers 1 through *N* to itself with all 1- or 2-cycles

index	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
involution	9	12	11	4	5	15	7	13	1	10	3	2	8	16	6	14

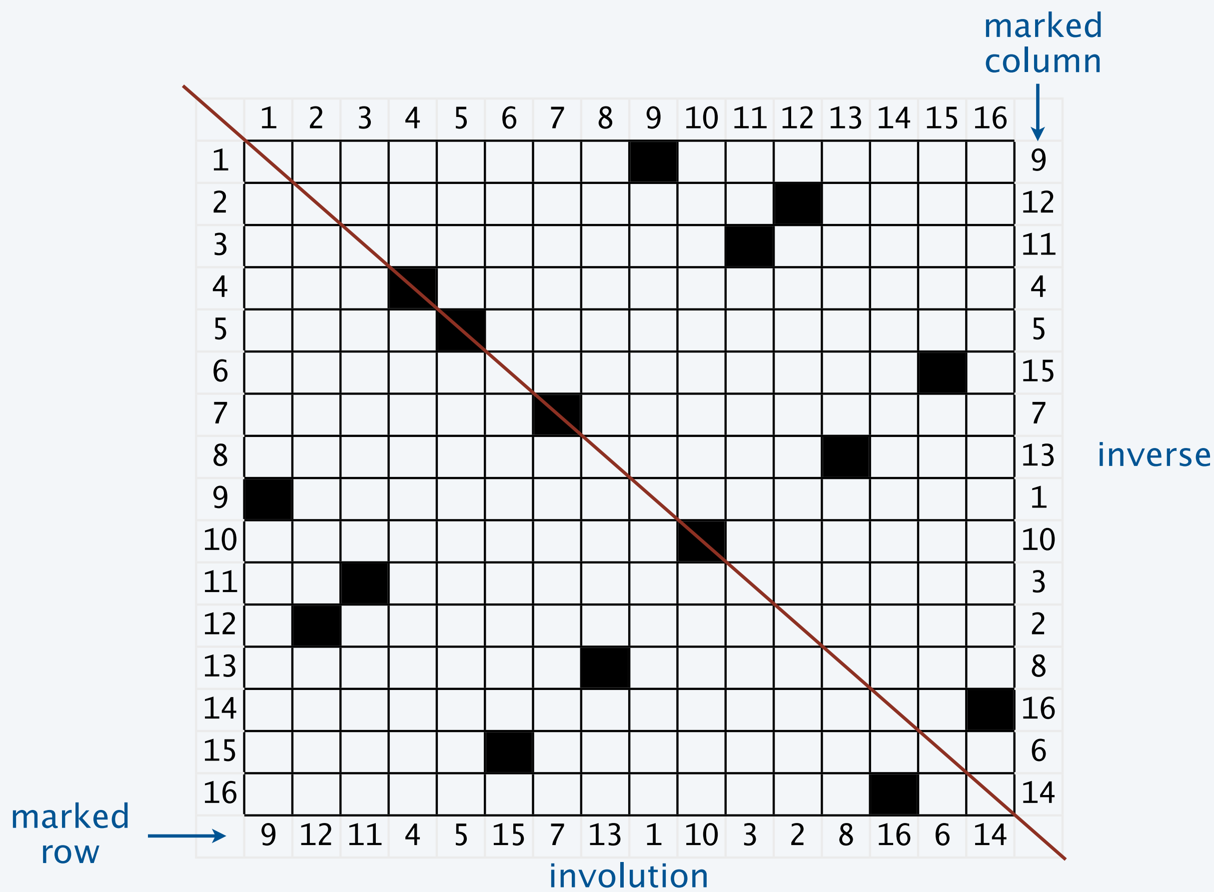
Def. The *inverse* of an involution is the inverse of that mapping.

9	12	11	4	5	15	7	13	1	10	3	2	8	16	6	14
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
inverse	9	12	11	4	5	15	7	13	1	10	3	2	8	16	6	14

Q. What is the inverse of an involution? **A.** ITSELF!

Lattice representation of an involution



Representation of involution is *symmetric* about the main diagonal.

Application: Reciprocal cipher

An *involution* is a permutation that is its own inverse.

Implication: Can encrypt and decrypt with the same machine.

Enigma (WW II)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	-
involution	D	K	R	A	Z	F	U	J	N	J	B	L	X	I	O	S	V	C	P	-	G	Q	Y	M	W	E	T

Encryption

plaintext	A	T	T	A	C	K	-	A	T	-	D	A	W	N
ciphertext	D	K	R	A	Z	F	U	J	N	J	B	L	X	I

Decryption

ciphertext	D	K	R	A	Z	F	U	J	N	J	B	L	X	I
plaintext	A	T	T	A	C	K	-	A	T	-	D	A	W	N

Caveat. Still susceptible to character frequency analysis but can be useful as a *component*.

Application: How many different Enigma settings?

There are several variables for the Enigma machine:

1. **Rotors**
   - you choose 3 rotors from 5
   - if you label the 5 rotors A, B, C, D, E - how many ways can you choose 3 different ones?

2. **Rotor starting position**
   - each rotor has 26 starting positions
   - how many combinations does this give with 3 rotors?

3. **Kickover point**
   - the rotors have the letters from A to Z on them
   - when the first rotor reaches a particular letter, it 'kicks over' to the second rotor
   - 2 rotors therefore kickover to another, and their kickover points can be set independently
   - how many additional choices does this give you?

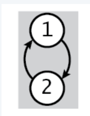
4. **plugboard**
   - six sets of two letters can be transposed using the plugboard
   - how many different ways can you pair six pairs of letters from the alphabet?
   - there is a huge number, so it would probably be a mistake to try to write them all down!
   - try finding out for small numbers, working systematically, then extend your results to larger numbers

When you've calculated all these possibilities, multiply them all together to find the total number of keys for the Enigma machine. The answer should be:

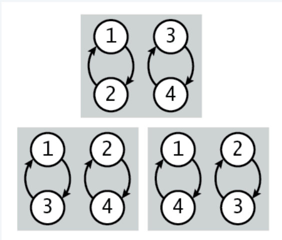
107 458 687 327 250 619 360 000

Warmup

How many perms are comprised entirely of 2-cycles?



$R_2 = 1$



$R_4 = 3$

Example: ROT-13 (world's weakest cryptosystem)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

Encryption	A T T A C K A T D A W N N G G N P X N G Q N J A
Decryption	N G G N P X N G Q N J A A T T A C K A T D A W N

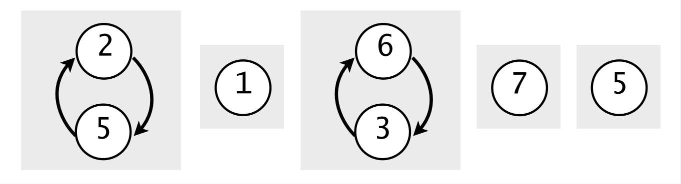
Construction	$R = SET(CYC_2(Z))$
OGF equation	$R(z) = e^{z^2/2}$
Coefficients	$R_N \equiv N![z^N]e^{z^2/2} \dfrac{N!}{2^{N/2}(N/2)!} \sim \sqrt{2}\left(\dfrac{N}{4e}\right)^{N/2}$

Stirling's approximation

$N! \sim (N/e)^N \sqrt{2\pi N}$

Involutions

How many involutions of size N?



Construction $$I = SET(CYC_1(Z)) \star SET(CYC_2(Z))$$

"Involutions are permutations with all cycles of length 1 or 2"

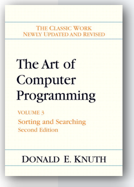
OGF equation $$I(z) = e^{z+z^2/2}$$

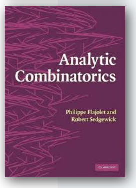
Coefficients $$I_N \equiv N![z^N]e^{z+z^2/2} = \sum_{0 \le 2k \le N} \frac{N!}{k!2^k(N-2k)!}$$

Asymptotics $$\sim \frac{1}{\sqrt{2\sqrt{e}}}\left(\frac{N}{e}\right)^{N/2} e^{\sqrt{N}}$$

Laplace method

Complex asymptotics (stay tuned for Part 2)





Generalized involutions

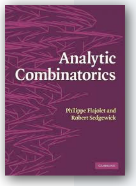
How many permutations of length N have no cycles of length > M ?

Construction $$I_M = SET(CYC_1(Z)) \star SET(CYC_2(Z)) \star \ldots \star SET(CYC_M(Z))$$

OGF equation $$I_M(z) = e^{z + z^2/2 + \ldots + z^M/M}$$

Coefficient asymptotics $$I_{MN} \sim \frac{1}{\sqrt{2\pi\lambda}} \frac{e^{1 + r/2 + \ldots + r^M/M}}{r^N}$$

← Complex asymptotics (stay tuned for Part 2)



In-class exercise

Find $[z^{10}]e^{z + z^2/2 + z^3/3 + z^4/4 + z^5/5}$

$$= [z^{10}]e^{\ln\frac{1}{1-z} - z^6/6 - z^7/7 - z^8/8 - z^9/9 - z^{10}/10 - \dots}$$

$$= [z^{10}]\frac{1}{1-z}e^{-z^6/6}e^{-z^7/7}e^{-z^8/8}e^{-z^9/9}e^{-z^{10}/10}\dots$$

$$= [z^{10}]\frac{1}{1-z}(1-\frac{z^6}{6})(1-\frac{z^7}{7})(1-\frac{z^8}{8})(1-\frac{z^9}{9})(1-\frac{z^{10}}{10})\dots$$

$$= [z^{10}](1+z+z^2+\dots+z^{10})\big(1-\frac{z^6}{6}-\frac{z^7}{7}-\frac{z^8}{8}-\frac{z^9}{9}-\frac{z^{10}}{10}\big)$$

$$= 1-\frac{1}{6}-\frac{1}{7}-\frac{1}{8}-\frac{1}{9}-\frac{1}{10} \doteq 35438$$

100 prisoners

Problem. 100 prisoners, each uniquely identified by a numbered ID card (1 to 100), have been sentenced to death, but are given a last chance.

- The ID cards are collected and put in the drawers of a cabinet with 100 numbered drawers (1 to 100) in random order, one card per drawer
- One at a time, the prisoners are allowed to enter the room containing the cabinet and open, then close again, at most *half* the drawers.
- If *all* prisoners find their own number, they will all be spared.
- If *one prisoner fails*, they will all be executed.

Prisoner A, a mathematician, bemoans their fate, claiming the probability of success is on the order of $2^{-100} \approx 8 \cdot 10^{-31}$.

Prisoner B, who knows analytic combinatorics, claims to know a strategy that gives them better than 30% chance of success.

What is Prisoner B's strategy?

100 prisoners solution

Problem. 100 prisoners, each uniquely identified by a numbered ID card (1 to 100), have been sentenced to death, but are given a last chance.

- The ID cards are collected and put in the drawers of a cabinet with 100 numbered drawers (1 to 100) in random order, one card per drawer.
- One at a time, the prisoners are allowed to enter the room containing the cabinet and open, then close again, at most *half* the drawers.
- If *all* prisoners find their own number, they will all be spared.
- If *one prisoner fails*, they will all be executed.

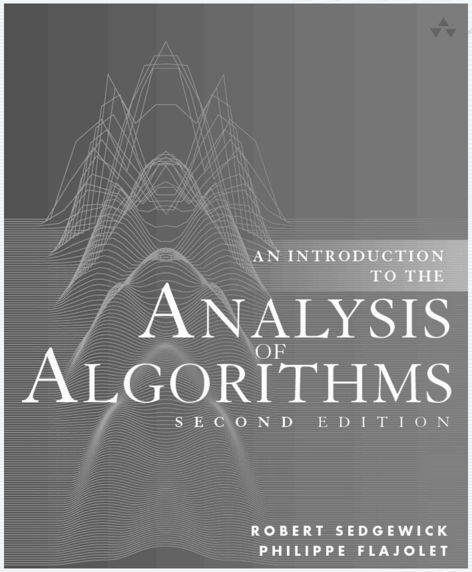
Prisoner B's strategy: Each prisoner "follows the cycle"

- Opens the drawer corresponding to his ID.
- Uses the number in that drawer to decide which drawer to open next.
- Continues until finding the drawer containing his ID.

Q. When does Prisoner's B strategy succeed?

A. When the random permutation has no cycles of length greater than 50.

Probability of success: $[z^{100}]\exp\left(\frac{z}{1}+\frac{z}{2}+\ldots+\frac{z}{50}\right) = 1-(H_{100}-H_{50}) \doteq 0.31$



http://aofa.cs.princeton.edu

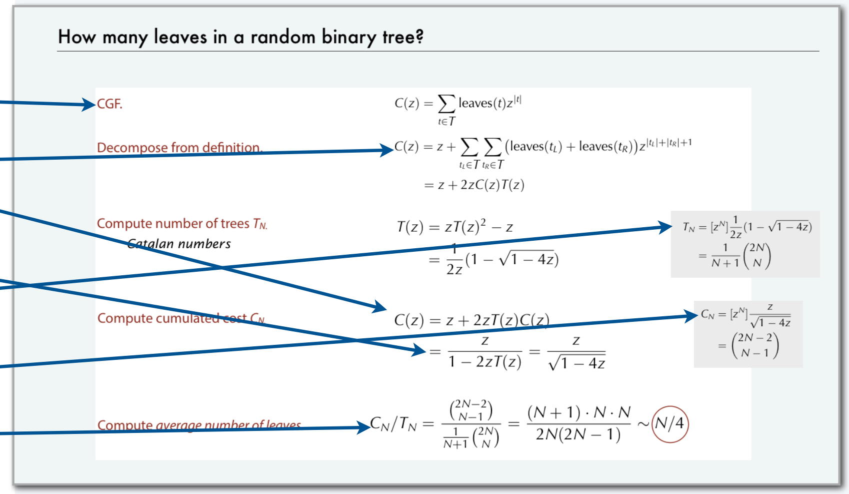
7. Permutations

- Basics
- Sets of cycles
- **Left-right-minima**
- Other parameters
- BGFs and distributions

General approach for analyzing parameters

Review: Cumulated cost approach for parameters

- Define GF for counting sequence and CGF.
- Identify construction to give CGF equation.
- Solve to get explicit formula for CGF.
- Extract coefficients from GF to get counting seq.
- Extract coefficients from CGF to get cumulated cost.
- Divide to compute expected value



Small trick for permutations:

- Use *exponential* CGF.
- Treat as OGF to extract expected value directly.

Why does it work?

- $N!$ is the normalizing factor for ECGF.
- $N!$ is *also* the counting sequence.

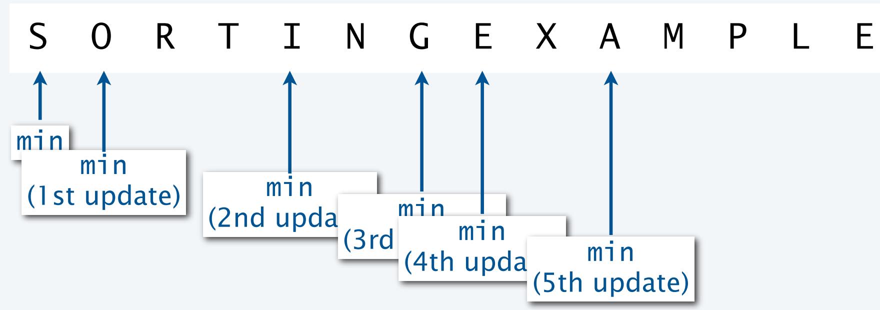
$$B(z) = \sum_{p \in \mathcal{P}} \text{cost}(p) \frac{z^{|p|}}{|p|!} = \sum_{N \geq 0} B_N \frac{z^N}{N!}$$

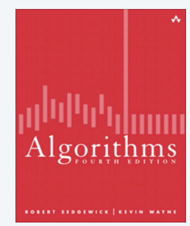
cumulated cost → counting sequence →

$$\frac{N![z^N]B(z)}{N!} = [z^N]B(z) = \frac{B_N}{N!}$$

Application: Selection sort

```
public static void sort(Comparable[] a)
{
   int N = a.length;
   for (int i = 0; i < N; i++)
   {
      int min = i;
      for (int j = i+1; j < N; j++)
         if (less(a[j], a[min])) min = j;
      exch(a, i, min);
   }
}
```





Section 2.1

Q. How many times is `min` updated in the first pass (assuming keys distinct)?

A. The number of left-right minima in the permutation.

Q. How many left-right minima in a random permutation?

Caveat. Cost for whole sort is complicated, but not significant relative to the number of compares.

Left-right minima

Def. A left-right minimum (lrm) in a permutation is a smaller than any item to its left.

Q. How many *lrm* in a random permutation of size N?

1	

$P_1 = 1$

$B_1 = 1$

$B_1/P_1 = 1$

1 2	
2 1	

$P_2 = 2$

$B_2 = 1 + 2 = 3$

$B_2/P_2 = 3/2 = 1.5$

1 2 3	1
2 1 3	2
3 1 2	2
1 3 2	1
2 3 1	2
3 2 1	3

$P_3 = 6$

$B_3 = 2 \cdot 1 + 3 \cdot 2 + 1 \cdot 3 = 11$

$B_3/P_3 = 11/6 \doteq 1.833$

1	1 2 3 4	1 2 4 3	1
2	2 1 3 4	2 1 4 3	2
2	3 1 2 4	3 1 4 2	2
2	4 1 2 3	4 1 3 2	2
1	1 3 2 4	1 3 4 2	1
2	2 3 1 4	2 3 4 1	2
3	3 2 1 4	3 2 4 1	3
3	4 2 1 3	4 2 3 1	3
1	1 4 2 3	1 4 3 2	1
2	2 4 1 3	2 4 3 1	2
2	3 4 1 2	3 4 2 1	3
3	4 3 1 2	4 3 2 1	4

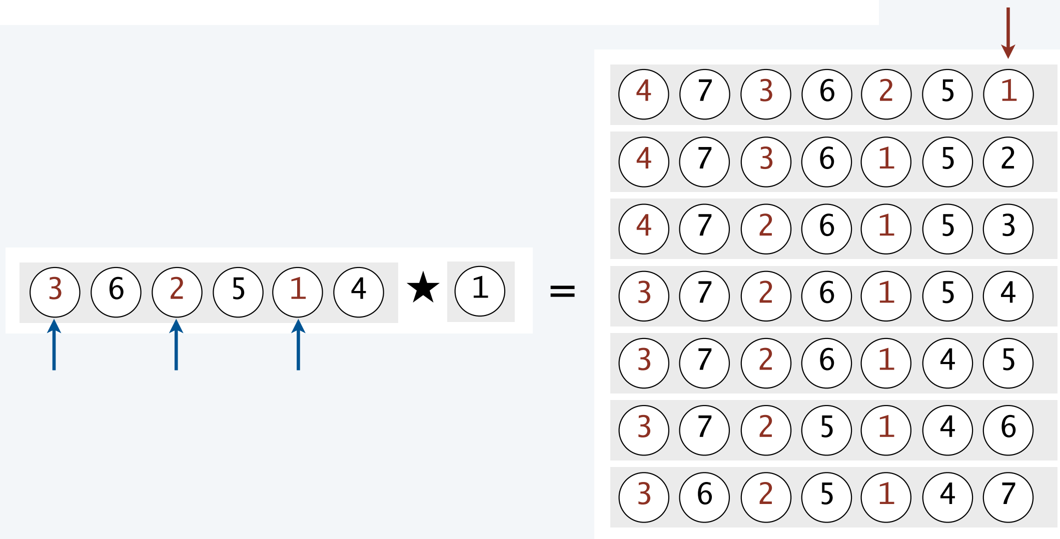
$P_4 = 24$

$B_4 = 6 \cdot 1 + 11 \cdot 2 + 6 \cdot 3 + 1 \cdot 4 = 50$

$B_4/P_4 = 50/24 \doteq 2.083$

Construction for left-right minima

Create |p|+1 perms from a perm p by star product construction.



Original perm has lrm(p) left-right minima.

Q. How many left-right minima in the set of constructed perms?

A. $(|p| + 1)$ lrm(p) $+ 1$

$|p| + 1$ copies of the original perm

only the one ending in 1 adds a lrm

Average number of left-right minima in a random permutation

CGF. $$B(z) = \sum_{p\in\mathcal{P}} \text{lrm}(p)\frac{z^{|p|}}{|p|!} \qquad = \sum_{N\ge 0} B_N \frac{z^N}{N!}$$

Apply construction. $$= \sum_{p\in\mathcal{P}} \big((|p|+1)\text{lrm}(p)+1\big)\frac{z^{|p|+1}}{(|p|+1)!}$$

Simplify. $$= \sum_{p\in\mathcal{P}} \text{lrm}(p)\frac{z^{|p|+1}}{(|p|)!} + \sum_{p\in\mathcal{P}} \frac{z^{|p|+1}}{(|p|+1)!}$$

Substitute. $$= zB(z) + \sum_{k\ge 0} \frac{z^{k+1}}{(k+1)} = zB(z) + \ln\frac{1}{1-z}$$

Solve. $$B(z) = \frac{1}{1-z}\ln\frac{1}{1-z}$$

OGF for the Harmonic numbers

Expand. $$[z^N]B(z) = \frac{B_N}{N!} = H_N$$

cumulated cost

average # lrm in a random permutation

$$H_1 = 1$$
$$H_2 = 1 + \frac{1}{2} = 1.5$$
$$H_3 = 1 + \frac{1}{2} + \frac{1}{3} \doteq 1.833$$
$$H_4 = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \doteq 2.083$$

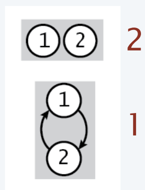
✓

Cycles

Q. How many *cycles* in a random permutation of size N?

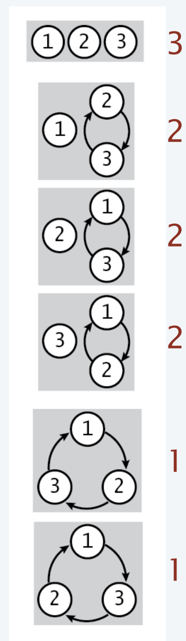
$B_1 = 1$

$B_1/P_1 = 1$



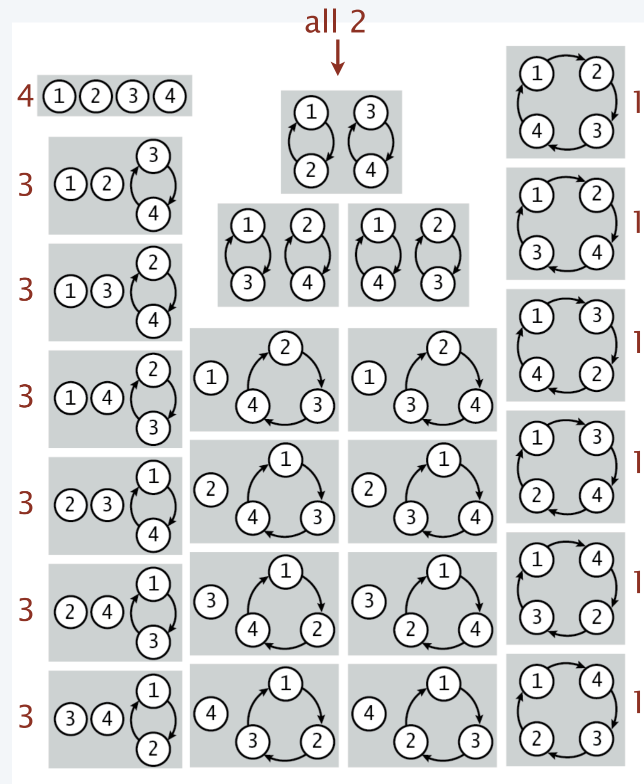
$B_2 = 1 + 2 = 3$

$B_2/P_2 = 3/2 = 1.5$



$B_3 = 2 \cdot 1 + 3 \cdot 2 + 1 \cdot 3 = 11$

$B_3/P_3 = 11/6 \doteq 1.833$

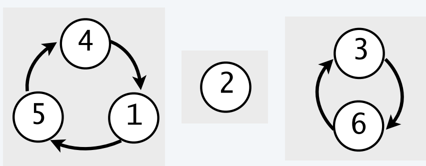


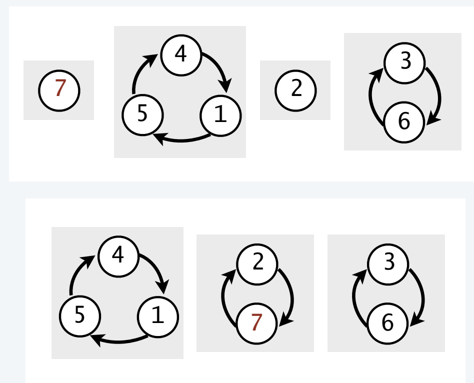
$B_4 = 6 \cdot 1 + 11 \cdot 2 + 6 \cdot 3 + 1 \cdot 4 = 50$

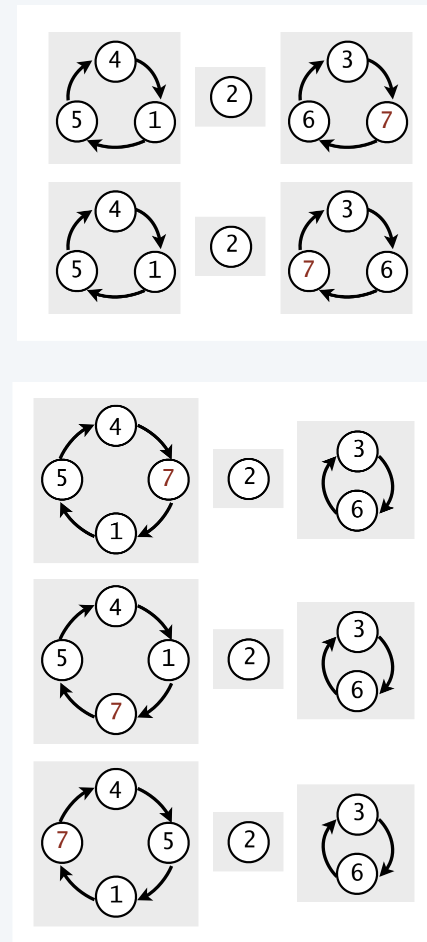
$B_4/P_4 = 50/24 \doteq 2.083$

Construction for cycles

Create $|p|+1$ perms from a perm p by inserting $|p|+1$ into every position in every cycle (including the null cycle)







Original perm has cycles(p) cycles.

Q. How many cycles in the set of constructed perms?

A. $(|p| + 1)$ cycles(p) $+ 1$ ← same as for lrm (!)

$|p| + 1$ copies of the original perm

from the null cycle

Average number of cycles in a random permutation (same derivation as for lrm)

CGF. $$B(z) = \sum_{p\in\mathcal{P}} \text{cycles}(p)\frac{z^{|p|}}{|p|!} = \sum_{N\geq 0} B_N \frac{z^N}{N!}$$

Decompose. $$= \sum_{p\in\mathcal{P}} \big((|p|+1)\text{cycles}(p)+1\big)\frac{z^{|p|+1}}{(|p|+1)!}$$

Simplify. $$= \sum_{p\in\mathcal{P}} \text{cycles}(p)\frac{z^{|p|+1}}{(|p|)!} + \sum_{p\in\mathcal{P}} \frac{z^{|p|+1}}{(|p|+1)!}$$

Substitute. $$= zB(z) + \sum_{k\geq 0} \frac{z^{k+1}}{(k+1)} = zB(z) + \ln\frac{1}{1-z}$$

Solve. $$B(z) = \frac{1}{1-z}\ln\frac{1}{1-z}$$

← OGF for the Harmonic numbers

Expand. $$[z^N]B(z) = \frac{B_N}{N!} = H_N$$

cumulated cost

average # cycles in a random permutation

$$H_1 = 1$$
$$H_2 = 1 + \frac{1}{2} = 1.5$$
$$H_3 = 1 + \frac{1}{2} + \frac{1}{3} \doteq 1.833$$
$$H_4 = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \doteq 2.083$$

✓

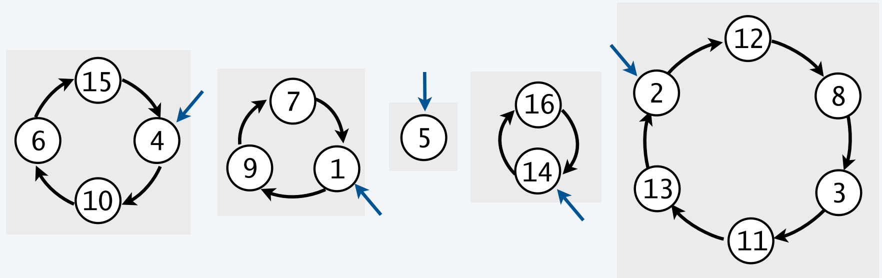
Left-right minima and cycles

Q. Is there a 1:1 correspondence?

A. Yes!

To build a permutation from a set of cycles:

- Identify smallest as the *leader* in each cycle.
- Write cycles in *decreasing* order of leader.

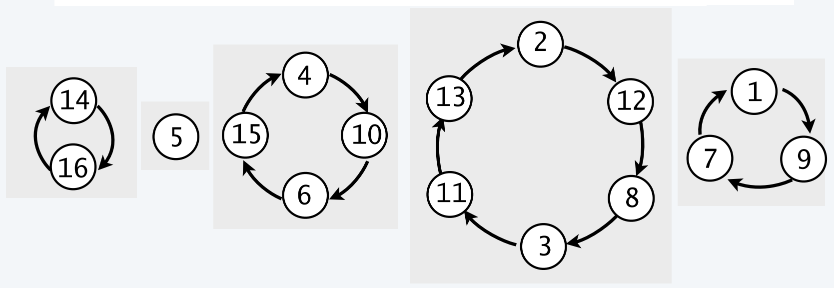


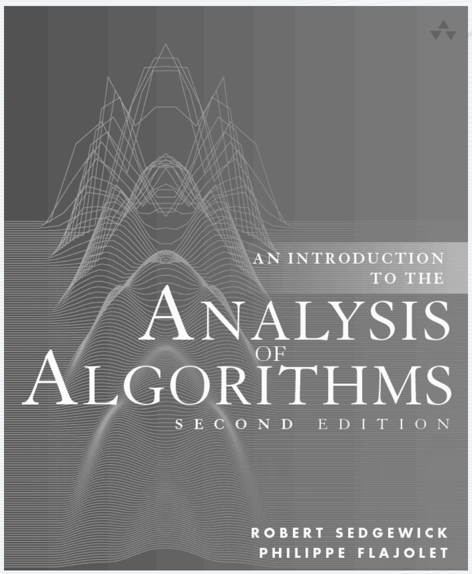
14 16 5 4 10 6 15 2 12 8 3 11 13 1 7 9

14 16 5 4 10 6 15 2 12 8 3 11 13 1 7 9

To build a set of cycles from a permutation:

- Identify left-right minima.
- Build cycles with entries delimited by lrms (start a new cycle with each lrm).





http://aofa.cs.princeton.edu

7. Permutations

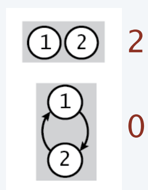
- Basics
- Sets of cycles
- Left-right-minima
- **Other parameters**
- BGFs and distributions

1-Cycles

Q. How many *1-cycles* in a random permutation of size N?

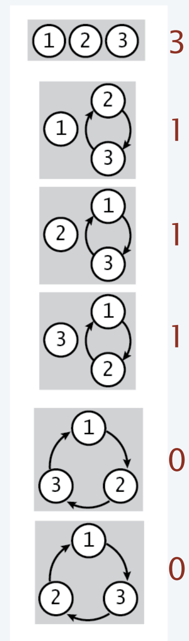
$B_1 = 1$

$B_1/P_1 = 1$



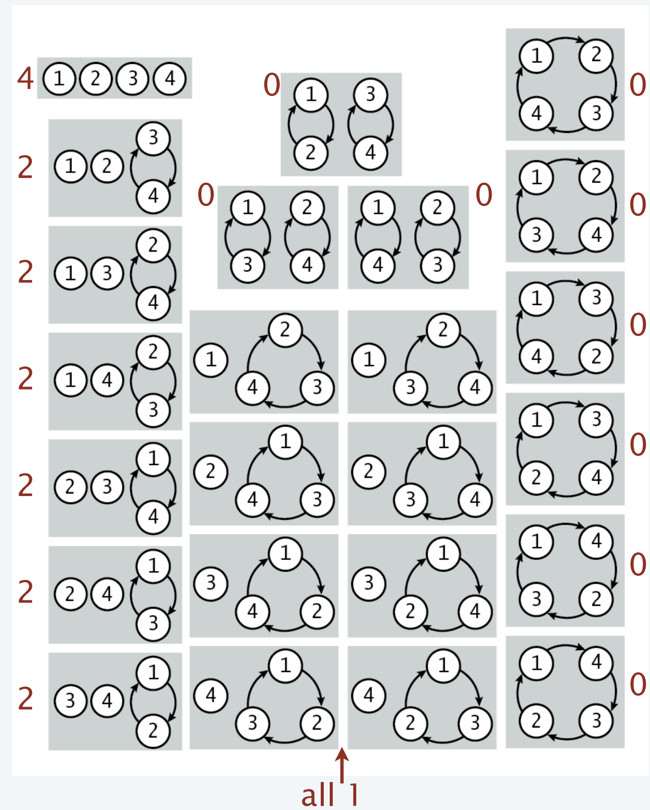
$B_2 = 0 + 2 = 2$

$B_2/P_2 = 2/2 = 1$



$B_3 = 2\cdot 0 + 3\cdot 1 + 1\cdot 3 = 6$

$B_3/P_3 = 1$

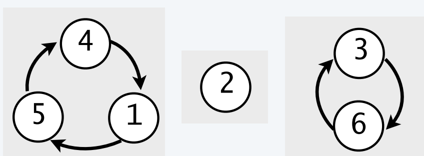


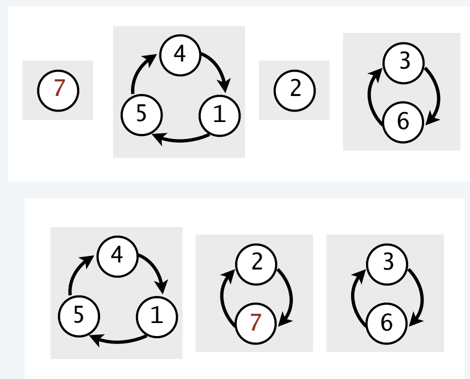
$B_4 = 9\cdot 0 + 8\cdot 1 + 6\cdot 2 + 1\cdot 4 = 24$

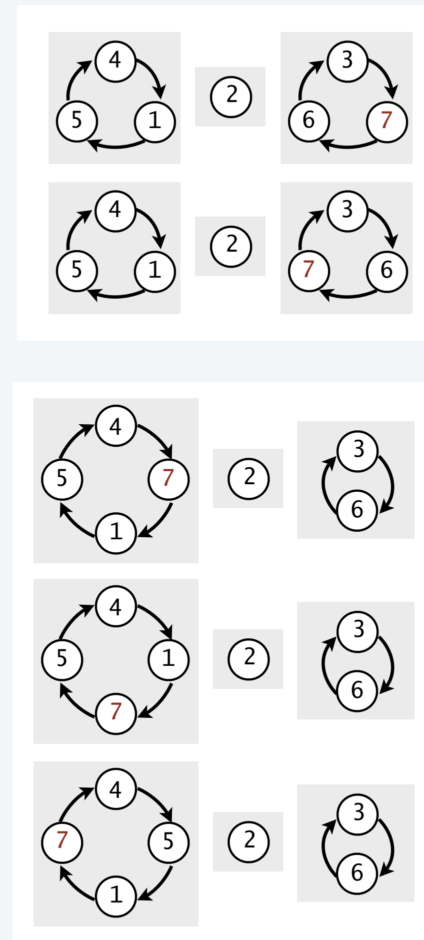
$B_4/P_4 = 24/24 = 1$

Construction for 1-cycles

Create $|p|+1$ perms from a perm p by inserting $|p|+1$ into every position in every cycle (including the null cycle)







Original perm has $\text{cyc}_1(p)$ 1-cycles.

Q. How many 1-cycles in the set of constructed perms?

A. $(|p| + 1)\,\text{cyc}_1(p) \quad + 1 \quad - \text{cyc}_1(p) \quad = |p|\,\text{cyc}_1(p) + 1$

- $(|p| + 1)\,\text{cyc}_1(p)$: $|p| + 1$ copies of the original perm
- $+1$: from the null cycle
- $-\,\text{cyc}_1(p)$: 1-cycles changed to 2-cycles

Average number of 1-cycles in a random permutation

CGF. $$B(z) = \sum_{p \in \mathcal{P}} \text{cyc}_1(p) \frac{z^{|p|}}{|p|!} = \sum_{N \geq 0} B_N \frac{z^N}{N!}$$

Apply construction. $$= \sum_{p \in \mathcal{P}} (|p|\text{cyc}_1(p) + 1) \frac{z^{|p|+1}}{(|p|+1)!}$$

Differentiate. $$B'(z) = \sum_{p \in \mathcal{P}} |p|\text{cyc}_1(p) \frac{z^{|p|}}{|p|!} + \sum_{p \in \mathcal{P}} \frac{z^{|p|}}{|p|!} = zB'(z) + \frac{1}{1-z}$$

Solve. $$B'(z) = \frac{1}{(1-z)^2}$$

Integrate. $$B(z) = \frac{1}{1-z}$$

Expand. $$[z^N]B(z) = \frac{B_N}{N!} = 1$$

cumulated cost (B_N)

average # 1-cycles in a random permutation (1)

Application: Students and rooms revisited

A group of N students who live in single rooms go to a party that leads to a state of inebriation. When returning, they each end up in a random room.

Q. What is the average number of students who wind up in their own room?

A. One (!)

In-class exercises

Q. How many *2-cycles* in a random permutation of size N?

A. 1/2

Q. How many *r-cycles* in a random permutation of size N?

A. $1/r$

Inversions

Def. An **inversion** in a permutation is the number of pairs (i)(j) with `i > j`.

Equivalent: Sum number of entries larger and to the left of each entry.

Q. How many *inversions* in a random permutation of size N?

1	0

$P_1 = 1$

$B_1 = 0$

$B_1/P_1 = 0$

1 2	0
2 1	1

$P_2 = 2$

$B_2 = 0 + 1 = 1$

$B_2/P_2 = 1/2 = 0.5$

1 2 3	0
2 1 3	1
3 1 2	2
1 3 2	1
2 3 1	2
3 2 1	3

$P_3 = 6$

$B_3 = 2\cdot1 + 2\cdot2 + 1\cdot3 = 9$

$B_3/P_3 = 9/6 = 1.5$

0	1 2 3 4	1 2 4 3	1
1	2 1 3 4	2 1 4 3	2
2	3 1 2 4	3 1 4 2	3
2	4 1 2 3	4 1 3 2	4
1	1 3 2 4	1 3 4 2	2
2	2 3 1 4	2 3 4 1	4
3	3 2 1 4	3 2 4 1	4
3	4 2 1 3	4 2 3 1	4
2	1 4 2 3	1 4 3 2	3
3	2 4 1 3	2 4 3 1	4
4	3 4 1 2	3 4 2 1	5
5	4 3 1 2	4 3 2 1	6

$P_4 = 24$

$B_4 = 3\cdot1 + 7\cdot2 + 5\cdot3 + 6\cdot4 + 2\cdot5 + 1\cdot6 = 72$

$B_4/P_4 = 72/24 = 3$

Application: Insertion sort

```
public static void sort(Comparable[] a)
{
   int N = a.length;
   for (int i = 1; i < N; i++)
   {
      for (int j = i; j > 0; j--)
         if (less(a[j], a[j-1]))
            exch(a, j, j-1);
         else break;
   }
}
```

sorted before i | i = 10 | untouched after i

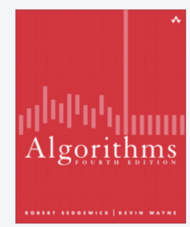
A	E	G	I	N	O	R	S	T	X	M	P	L	E	D	Q	Z
A	E	G	I	N	O	R	S	T	M	X	P	L	E	D	Q	Z
A	E	G	I	N	O	R	S	M	T	X	P	L	E	D	Q	Z
A	E	G	I	N	O	R	M	S	T	X	P	L	E	D	Q	Z
A	E	G	I	N	O	M	R	S	T	X	P	L	E	D	Q	Z
A	E	G	I	N	M	O	R	S	T	X	P	L	E	D	Q	Z
A	E	G	I	M	N	O	R	S	T	X	P	L	E	D	Q	Z

exchanges put M in place among elements to its left

Q. How many exchanges during the sort?

A. The number of inversions in the permutation.

Q. How many inversions in a random permutation?



Section 2.1

Construction for inversions

Create $|p|+1$ perms from a perm p by "largest" construction.

3 6 2 5 1 4 ★ 1 =

3 6 2 5 1 4 7	
3 6 2 5 1 7 4	← adds 1 inversion
3 6 2 5 7 1 4	← adds 2 inversions
3 6 2 7 5 1 4	← adds 3 inversions
3 6 7 2 5 1 4	← adds 4 inversions
3 7 6 2 5 1 4	← adds 5 inversions
7 3 6 2 5 1 4	← adds 6 inversions

Original perm has inv(p) inversions.

Q. How many inversions in the set of constructed perms?

A. $(|p| + 1)\ \mathrm{inv}(p) \quad + (|p| + 1)\ |p|\ /\ 2$

$|p| + 1$ copies of the original perm

all the inversions caused by $|p| + 1$

Average number of inversions in a random permutation

CGF. $$B(z) = \sum_{p \in \mathcal{P}} \text{inv}(p) \frac{z^{|p|}}{|p|!} \qquad = \sum_{N \ge 0} B_N \frac{z^N}{N!}$$

Apply construction. $$= \sum_{p \in \mathcal{P}} \big((|p|+1)\text{inv}(p) + (|p|+1)|p|/2\big) \frac{z^{|p|+1}}{(|p|+1)!}$$

Simplify. $$= \sum_{p \in \mathcal{P}} \text{inv}(p) \frac{z^{|p|+1}}{(|p|)!} + \frac{1}{2} \sum_{p \in \mathcal{P}} |p| \frac{z^{|p|+1}}{(|p|)!} \quad = zB(z) + \frac{z}{2} \sum_{k \ge 0} k z^k$$

Substitute. $$= zB(z) + \frac{1}{2} \frac{z^2}{(1-z)^2}$$

Solve. $$B(z) = \frac{1}{2} \frac{z^2}{(1-z)^3}$$

Expand. $$[z^N]B(z) = \frac{B_N}{N!} = \frac{N(N-1)}{4}$$

cumulated cost

average # inversions in a random permutation

$$B_1/1! = \frac{1 \cdot 0}{4} = 0$$

$$B_2/2! = \frac{2 \cdot 1}{4} = 0.5$$

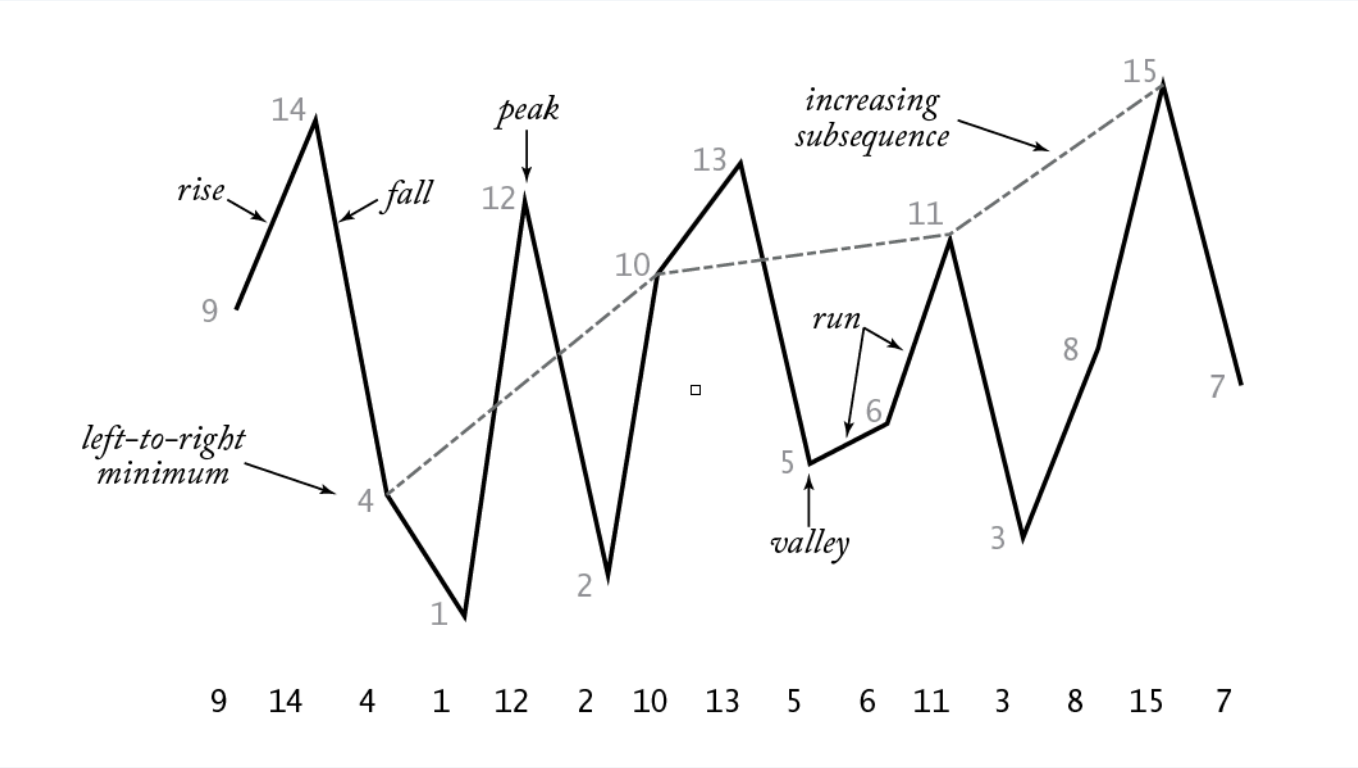
$$B_3/3! = \frac{3 \cdot 2}{4} = 1.5$$

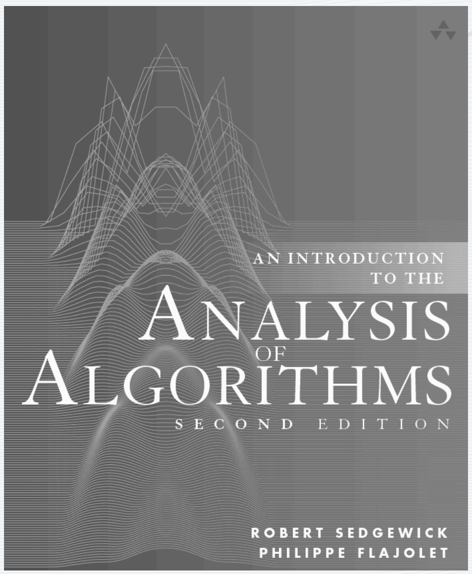
$$B_4/4! = \frac{4 \cdot 3}{4} = 3$$

✓

Parameters of permutations

all can be handled in a similar manner





http://aofa.cs.princeton.edu

7. Permutations

- Basics
- Sets of cycles
- Left-right-minima
- Other parameters
- BGFs and distributions

Bivariate generating functions

are the method of choice in analyzing combinatorial parameters.

Definition. A *combinatorial class* is a set of combinatorial objects and an associated size function that may have an associated parameter.

Definition. The *bivariate generating function* (BGF) associated with a class is the formal power series

$$A(z,u) = \sum_{a \in A} \frac{z^{|a|}}{|a|!} u^{cost(a)} \quad \text{(labelled)}$$

where |a| is the size and cost(a) is the value of the parameter.

Advantages of BGFs:

- Carry full information.
- Easy to compute counting sequence and CGF (see next slide).
- Full distribution often available via analytic combinatorics.

Basic BGF calculations

Definition. The *bivariate generating function* (BGF) associated with a labelled class is the formal power series $A(z,u) = \sum_{a \in A} \frac{z^{|a|}}{|a|!} u^{cost(a)}$

z marks size.
u marks the parameter.

Define A_{Nk} to be the number of elements of size N with parameter value k.

Fundamental (elementary) identity $A(z,u) = \sum_{a \in A} \frac{z^{|a|}}{|a|!} u^{cost(a)} = \sum_{N \geq 0} \sum_{k \geq 0} A_{Nk} \frac{z^N}{N!} u^k$

Q. How many objects of size N with value k ?

A. $N![z^N][u^k]A(z,u) = A_{Nk}$

Q. Average value of a parameter of a permutation ?

A. $[z^N]A_u(z,1) \equiv \frac{\partial}{\partial u} A(z,u)\Big|_{u=1}$

$$\frac{\partial}{\partial u} A(z,u) = \sum_{N \geq 0} \sum_{k \geq 0} k A_{Nk} \frac{z^N}{N!} u^{k-1}$$

$$A_u(z,1) \equiv \frac{\partial}{\partial u} A(z,u)\Big|_{u=1} = \sum_{N \geq 0} \sum_{k \geq 0} k A_{Nk} \frac{z^N}{N!}$$

$$[z^N]A_u(z,1) = \frac{\partial}{\partial u} A(z,u)\Big|_{u=1} = \sum_{k \geq 0} k \frac{A_{Nk}}{N!}$$

Review: Average number of cycles in a random permutation with CGFs

CGF. $$B(z) = \sum_{p \in \mathcal{P}} \text{cycles}(p) \frac{z^{|p|}}{|p|!} = \sum_{N \geq 0} B_N \frac{z^N}{N!}$$

Decompose. $$= \sum_{p \in \mathcal{P}} \big((|p|+1)\text{cycles}(p) + 1\big) \frac{z^{|p|+1}}{(|p|+1)!}$$

Simplify. $$= \sum_{p \in \mathcal{P}} \text{cycles}(p) \frac{z^{|p|+1}}{(|p|)!} + \sum_{p \in \mathcal{P}} \frac{z^{|p|+1}}{(|p|+1)!}$$

Substitute. $$= zB(z) + \sum_{k \geq 0} \frac{z^{k+1}}{(k+1)} = zB(z) + \ln \frac{1}{1-z}$$

Solve. $$B(z) = \frac{1}{1-z} \ln \frac{1}{1-z}$$ ← OGF for the Harmonic numbers

Expand. $$[z^N]B(z) = \frac{B_N}{N!} = H_N$$

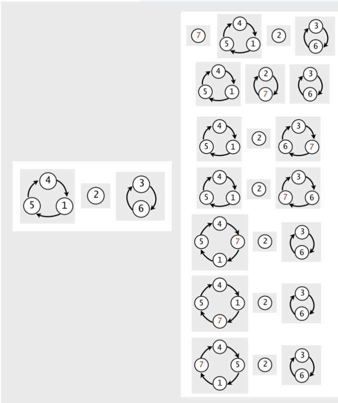
cumulated cost

average # cycles in a random permutation

Average number of cycles in a random permutation with BGFs

BGF. $$B(z,u) = \sum_{p \in \mathcal{P}} \frac{z^{|p|}}{|p|!} u^{cycles(p)}$$

Apply construction . $$= \sum_{p \in \mathcal{P}} \frac{z^{|p|+1}}{(|p|+1)!} \left(u^{cycles(p)+1} + |p| u^{cycles(p)}\right)$$



Differentiate wrt z. $$B_z(z,u) = \sum_{p \in \mathcal{P}} \frac{z^{|p|}}{(|p|)!} u^{cycles(p)+1} + \sum_{p \in \mathcal{P}} \frac{z^{|p|}}{(|p|)!} |p| u^{cycles(p)}$$

Substitute. $$= uB(z,u) + zB_z(z,u)$$

Solve for $B_z(z, u)$. $$B_z(z,u) = \frac{u}{1-z} B(z,u)$$

Solve ODE. $$B(z,u) = \frac{1}{(1-z)^u}$$

Average number of cycles. $$B_u(z,1) = \frac{1}{1-z} \ln \frac{1}{1-z}$$

$$[z^N]B_u(z,1) = H_N \quad ✓$$

Average number of cycles in a random permutation with BGFs and the symbolic method

Combinatorial class. P, the class of all permutations

Construction. $$P = SET(uCYC(Z))$$

BGF equation $$P(z,u) = \exp\left(u \ln \frac{1}{1-z}\right) = \frac{1}{(1-z)^u}$$

immediate from transfer theorem.

Average number of cycles. $$P_u(z,1) = \frac{1}{1-z} \ln \frac{1}{1-z}$$

$$[z^N]P_u(z,1) = H_N \ ✓$$

Bottom line: BGFs are the *method of choice* in analyzing parameters

Average number of cycles of a given size in a random permutation

Combinatorial class. P, the class of all permutations

Construction.

$$P = SET(CYC_{\neq r} + uCYC_r(Z))$$

BGF equation

$$P(z,u) = e^{\ln \frac{1}{1-z} - \frac{z^r}{r} + \frac{uz^r}{r}}$$

immediate from transfer theorem.

Average number of cycles.

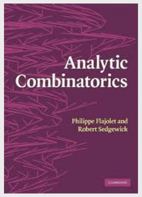
$$P_u(z,1) = \frac{z^r}{r}\frac{1}{1-z}$$

$$[z^N]P_u(z,1) = \frac{1}{r} \quad \text{for} \quad N \geq r \checkmark$$

BGFs are the *method of choice* in analyzing parameters.

Many, many examples to follow.

Stay tuned for Part 2

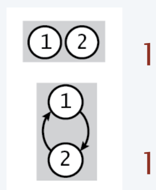


Number of permutations of size N with k cycles

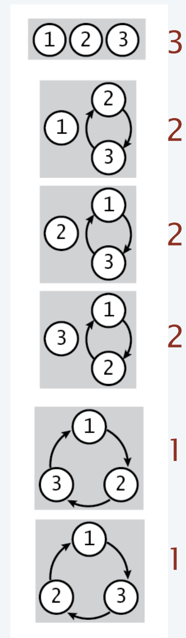
are known as *Stirling numbers of the first kind.*

Notation: $\begin{bmatrix} N \\ k \end{bmatrix}$

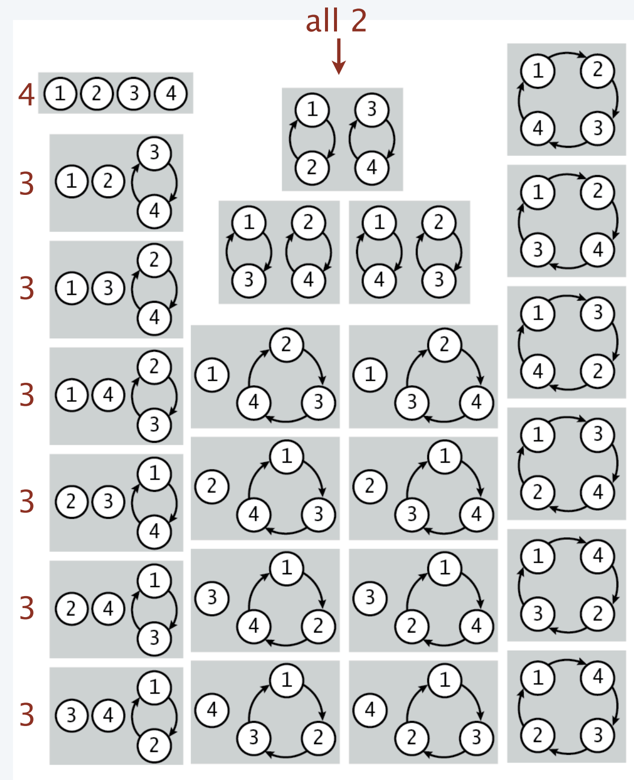
$\begin{bmatrix} 1 \\ 1 \end{bmatrix} = 1$



$\begin{bmatrix} 2 \\ 1 \end{bmatrix} = 1$ $\begin{bmatrix} 2 \\ 2 \end{bmatrix} = 1$



$\begin{bmatrix} 3 \\ 1 \end{bmatrix} = 2$ $\begin{bmatrix} 3 \\ 2 \end{bmatrix} = 3$ $\begin{bmatrix} 3 \\ 3 \end{bmatrix} = 1$



$\begin{bmatrix} 4 \\ 1 \end{bmatrix} = 6$ $\begin{bmatrix} 4 \\ 2 \end{bmatrix} = 11$ $\begin{bmatrix} 4 \\ 3 \end{bmatrix} = 6$ $\begin{bmatrix} 4 \\ 4 \end{bmatrix} = 1$

Stirling numbers of the first kind (cycle numbers)

Fundamental identity

$$P(z,u) = \sum_{p \in p} \frac{z^{|p|}}{|p|!} u^{cycles(p)} = \sum_{N \ge 0} \sum_{k \ge 0} \begin{bmatrix} N \\ k \end{bmatrix} \frac{z^N}{N!} u^k = \frac{1}{(1-z)^u}$$

Distribution

$$P(z,u) = \sum_{N \ge 0} u(u+1)\ldots(u+N-1)\frac{z^N}{N!}$$

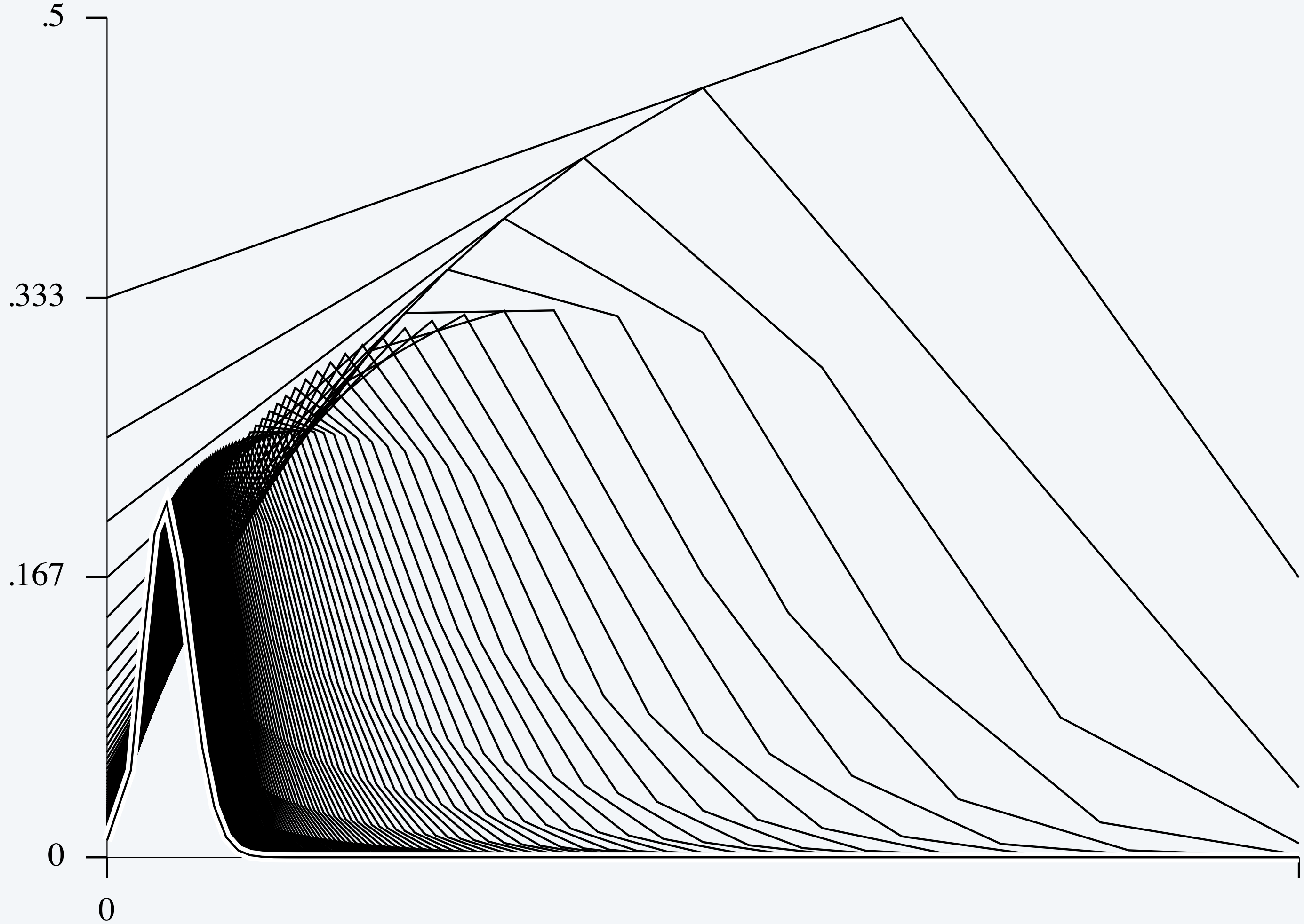
(Taylor's theorem)

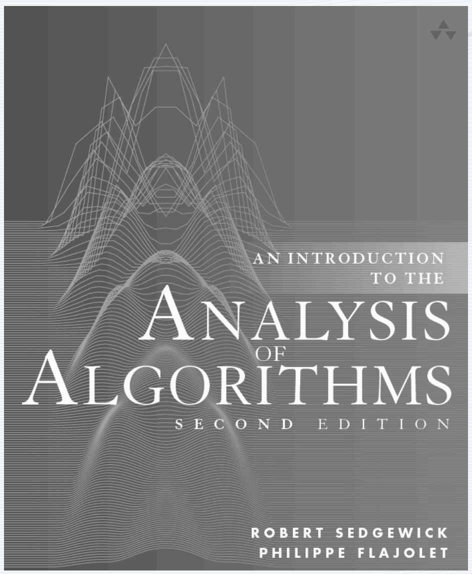
$\begin{bmatrix} N \\ k \end{bmatrix}$

N \ k	1	2	3	4	5	6	7
1	1						
2	1	1					
3	2	3	1				
4	6	11	6	1			
5	24	50	35	10	1		
6	120	274	225	85	15	1	

$[u^k]u(u+1)(u+2)(u+3) \longrightarrow$ row 4

Stirling numbers of the first kind (cycle numbers) distribution





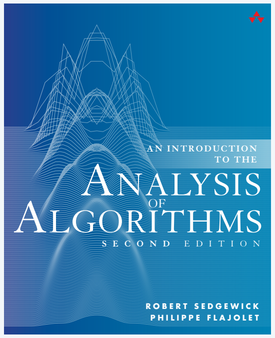
http://aofa.cs.princeton.edu

7. Permutations

- Basics
- Sets of cycles
- Left-right-minima
- Other parameters
- BGFs and distributions
- **Exercises**

Exercise 7.29

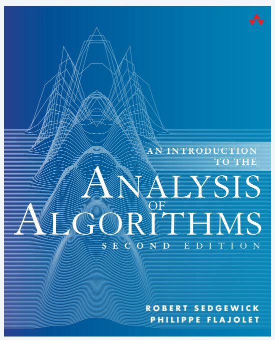
Arrangements.



Exercise 7.29 An *arrangement* of N elements is a sequence formed from a subset of the elements. Prove that the EGF for arrangements is $e^z/(1-z)$. Express the coefficients as a simple sum and give a combinatorial interpretation of that sum.

Exercise 7.45

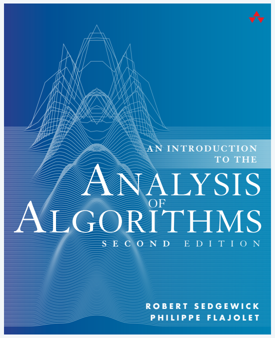
Inversions in involutions.



Exercise 7.45 Find the CGF for the total number of inversions in all involutions of length N. Use this to find the average number of inversions in an involution.

Exercise 7.61

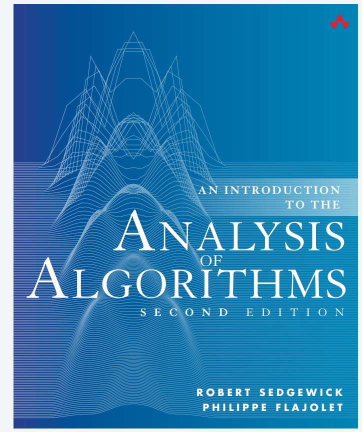
Cycle length distribution.



Exercise 7.61 Use asymptotics from generating functions (see §5.5) or a direct argument to show that the probability for a random permutation to have j cycles of length k is asymptotic to the Poisson distribution $e^{-\lambda}\lambda^j/j!$ with $\lambda = 1/k$.

Assignments for next lecture

1. Read pages 345-413 in text.



2. Run experiments to validate mathematical results.

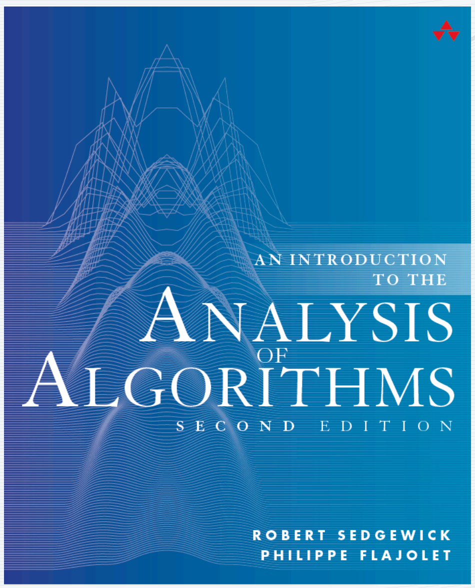
Experiment 1. Generate 1000 random permutations for $N = 100$, 1000, and 10,000 and compare the average number of cycles and 1-cycles with the values predicted by analysis.

Experiment 2. *Extra credit.* Validate the results of Exercise 7.61 for N = 1000 and k = 10 by generating 10,000 random permutations and plotting the histogram of occurences of cycles of length 10.

3. Write up solutions to Exercises 7.29, 7.45, and 7.61.

ANALYTIC COMBINATORICS

PART ONE



http://aofa.cs.princeton.edu

7. Permutations