Welcome to SIGma

SIGma

Outline

Officers in No Particular Order

Computing Fibonacci

Anakin

- Math Major
- SIGPwny Crypto[1] Gang + Admin team
- CA for CS 173 + CS 475
- Research with Sam

[1] Not that one, the other one

Sam

- Summer Amazon Intern
- CS Major
- Doing CS 374 Course Dev
- Doing Theory Research with Sariel Har-Peled
- Research with Anakin

Lou

- CS Major
- Current CS 225 CA (past CS 125 and 374 CA)
- Senior, selling soul to finance after this semester

Aditya

- ECE/Math double degree.
- Quantum error correction research w/Prof. Milenkovic.
- CA for ECE 391.
- Other interests: FP, PL, Crypto.

Hassam

- Intern at Amazon over the summer
- CS Major (takes math classes for fun ???)
- SIGPwny Crypto Gang + Admin team + Infra lead
- CA for CS 233, CS 173
- Compiler research

Phil

- CS/Ling Major, Senior
- CA for CS 233
- SIGecom - game theory, economics, and computation

Section 2

Computing Fibonacci

Recursive

$$F_n = \begin{cases} 0 & n = 0 \\ 1 & n = 1 \\ F_{n-1} + F_{n-2} & n \geq 2 \end{cases}$$

Recursive

$$F_n = \begin{cases} 0 & n = 0 \\ 1 & n = 1 \\ F_{n-1} + F_{n-2} & n \geq 2 \end{cases}$$

F_0	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	F_{13}
0	1	1	2	3	5	8	13	21	34	55	89	144	233

Recursive Computation

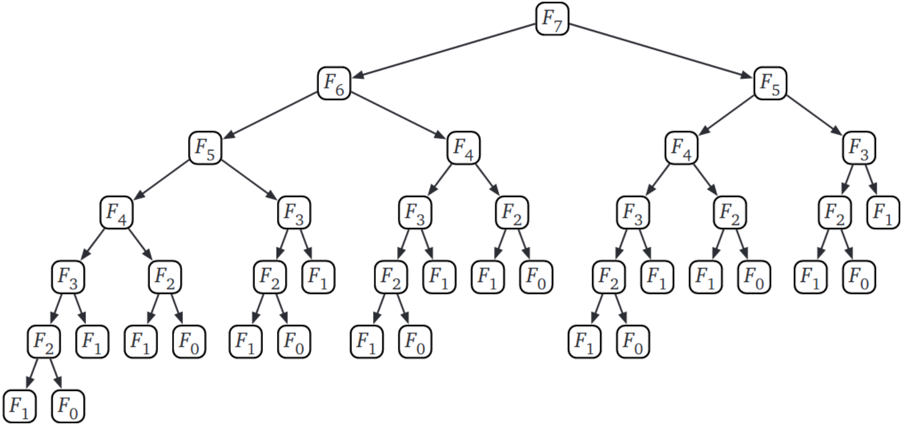


Figure: From [Eri19]

Can We Do Better?

We can use 12 multiplications to compute x^{13} as follows:

$$x \to x^2 \to x^3 \to x^4 \to x^5 \to x^6 \to x^7 \to x^8 \to x^9 \to x^{10} \to x^{11} \to x^{12} \to x^{13}$$

Can We Do Better?

We can use 12 multiplications to compute x^{13} as follows:

$$x \to x^2 \to x^3 \to x^4 \to x^5 \to x^6 \to x^7 \to x^8 \to x^9 \to x^{10} \to x^{11} \to x^{12} \to x^{13}$$

But if we first compute powers as such

$$x^2 \leftarrow x \cdot x$$
$$x^4 \leftarrow x^2 \cdot x^2$$
$$x^8 \leftarrow x^4 \cdot x^4$$

Can We Do Better?

We can use 12 multiplications to compute x^{13} as follows:

$$x \to x^2 \to x^3 \to x^4 \to x^5 \to x^6 \to x^7 \to x^8 \to x^9 \to x^{10} \to x^{11} \to x^{12} \to x^{13}$$

But if we first compute powers as such

$$x^2 \leftarrow x \cdot x$$
$$x^4 \leftarrow x^2 \cdot x^2$$
$$x^8 \leftarrow x^4 \cdot x^4$$

Using these we compute $x^8 \cdot x^4 \cdot x^1 = x^{13}$ in just 5 total multiplications.

Can We Do Better?

We can use 12 multiplications to compute x^{13} as follows:

$$x \to x^2 \to x^3 \to x^4 \to x^5 \to x^6 \to x^7 \to x^8 \to x^9 \to x^{10} \to x^{11} \to x^{12} \to x^{13}$$

But if we first compute powers as such

$$x^2 \leftarrow x \cdot x$$
$$x^4 \leftarrow x^2 \cdot x^2$$
$$x^8 \leftarrow x^4 \cdot x^4$$

Using these we compute $x^8 \cdot x^4 \cdot x^1 = x^{13}$ in just 5 total multiplications.
We can generalize this using binary

1	**1**	**0**	**1**
8	4	2	1

Building an Algorithm

$$13 = 8 + 4 + 1 = \mathbf{1101}_2$$

Building an Algorithm

$$13 = 8 + 4 + 1 = \mathbf{1101}_2$$

Step	Bit	Power	Result
0			1

Building an Algorithm

$$13 = 8 + 4 + 1 = \mathbf{1101}_2$$

Step	Bit	Power	Result
0			1
1	**1**	x	x

Building an Algorithm

$$13 = 8 + 4 + 1 = \mathbf{1101}_2$$

Step	Bit	Power	Result
0			1
1	**1**	x	x
2	**0**	x^2	x

Building an Algorithm

$$13 = 8 + 4 + 1 = \mathbf{1101}_2$$

Step	Bit	Power	Result
0			1
1	**1**	x	x
2	**0**	x^2	x
3	**1**	x^4	x^5

Building an Algorithm

$$13 = 8 + 4 + 1 = \mathbf{1101}_2$$

Step	Bit	Power	Result
0			1
1	**1**	x	x
2	**0**	x^2	x
3	**1**	x^4	x^5
4	**1**	x^8	x^{13}

```
POWER(x, n):
    curr ← 1
    for i ← 1 ... n :
        curr ← curr * x
    return curr
```

```
POWER(x, n):
    curr ← 1
    for i ← 1 ... n :
        curr ← curr * x
    return curr
```

```
SQUAREMULTPOWER(x, n):
    res ← 1
    power ← x
    for bit in BINARY(n):
        if bit = 1:
            res ← res * power
        power ← power * power
    return res
```

Matrices

We have the following two linear equations

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ F_{n-1} &= F_{n-1} \end{aligned}$$

Matrices

We have the following two linear equations

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ F_{n-1} &= F_{n-1} \end{aligned}$$

We can represent this as follows using matrices

$$\begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_{n-1} \\ F_{n-2} \end{bmatrix}$$

Matrices

We have the following two linear equations

$$
\begin{aligned}
F_n &= F_{n-1} + F_{n-2} \\
F_{n-1} &= F_{n-1}
\end{aligned}
$$

We can represent this as follows using matrices

$$
\begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_{n-1} \\ F_{n-2} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^2 \begin{bmatrix} F_{n-2} \\ F_{n-3} \end{bmatrix}
$$

Matrices

We have the following two linear equations

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ F_{n-1} &= F_{n-1} \end{aligned}$$

We can represent this as follows using matrices

$$\begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_{n-1} \\ F_{n-2} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^2 \begin{bmatrix} F_{n-2} \\ F_{n-3} \end{bmatrix} = \cdots = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

We can use SQUAREMULTPOWER to compute this!

Combinatorics

This semester is going to be mainly focused on combinatorics. So let's look at one of the most beautiful combinatorial objects in all of mathematics: **Pascal's Triangle**

Pascal's Triangle

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

Binomial Coefficients and Pascal's Triangle

- Blaise Pascal first discussed his triangle in his *Traité du Triangle Arithmétique* [Pas65]
  - One of the first works on probability theory

Binomial Coefficients and Pascal's Triangle

- Blaise Pascal first discussed his triangle in his *Traité du Triangle Arithmétique* [Pas65]
  - One of the first works on probability theory
- Binomial coefficients were first discussed in detail in India in the tenth–century [Knu97]

Binomial Coefficients

- "The number of ways to choose k items from n distinct items"
$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Binomial Coefficients

- "The number of ways to choose k items from n distinct items"

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

- "The number of ways to **not** choose $n-k$ from n distinct items"

$$\binom{n}{k} = \binom{n}{n-k}$$

Pascal's Triangle

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$

$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$

$$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$$

Pascal's Triangle

$$
\begin{array}{ccccccccc}
 & & & & \binom{0}{0} & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4}
\end{array}
$$

$$
\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1
\end{array}
$$

A Pattern in the Triangle

1

1 1

1 2 1

1 3 3 1

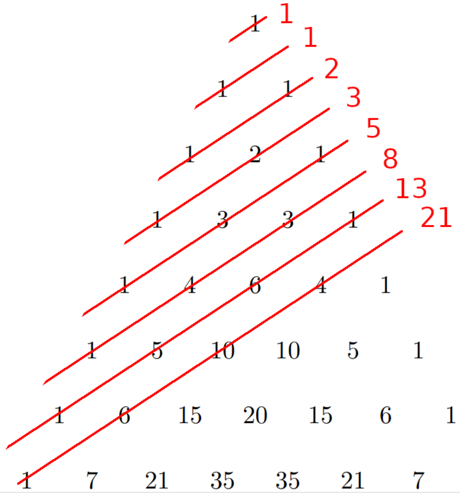
1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

A Pattern in the Triangle



Proving the Pattern

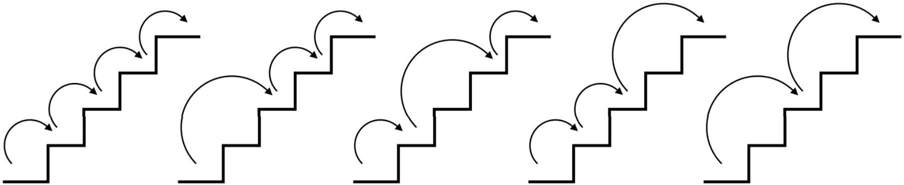
Claim:

$$\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-k}{k} = F_{n+1}$$

We are going to prove this by a **combinatorial argument**

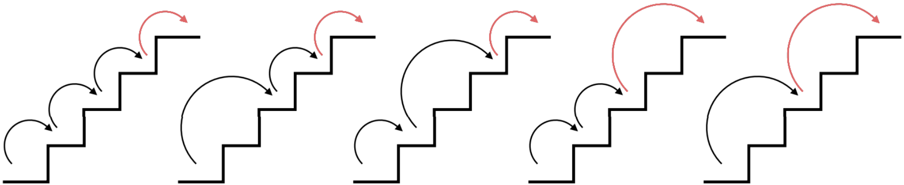
Staircases

Question: How many ways are there to climb a staircase going one or two steps at a time?



Staircases

Question: How many ways are there to climb a staircase going one or two steps at a time?



We can think of this recursively!

Steps to Compute Steps

- Let the starting step be step 0. Assuming we are on step $n \geq 2$, how did we get here?

Steps to Compute Steps

- Let the starting step be step 0. Assuming we are on step $n \geq 2$, how did we get here?
  - Either we took a single step from step $n - 1$

Steps to Compute Steps

- Let the starting step be step 0. Assuming we are on step $n \geq 2$, how did we get here?
  - Either we took a single step from step $n - 1$
  - Or we took two steps from step $n - 2$

Steps to Compute Steps

- Let the starting step be step 0. Assuming we are on step $n \geq 2$, how did we get here?
  - Either we took a single step from step $n-1$
  - Or we took two steps from step $n-2$
- Combining the number of ways to get to step $n-1$ with the number of ways to get to step $n-2$ yields the number of ways to get to step n

Steps to Compute Steps

- Let the starting step be step 0. Assuming we are on step $n \geq 2$, how did we get here?
  - Either we took a single step from step $n - 1$
  - Or we took two steps from step $n - 2$
- Combining the number of ways to get to step $n - 1$ with the number of ways to get to step $n - 2$ yields the number of ways to get to step n
- $S_n = S_{n-1} + S_{n-2}$

Steps to Compute Steps

- Let the starting step be step 0. Assuming we are on step $n \geq 2$, how did we get here?
  - Either we took a single step from step $n - 1$
  - Or we took two steps from step $n - 2$
- Combining the number of ways to get to step $n - 1$ with the number of ways to get to step $n - 2$ yields the number of ways to get to step n
- $S_n = S_{n-1} + S_{n-2}$
  - How many ways are there to get to step 0? **Exactly 1** ($S_0 = 1$)

Steps to Compute Steps

- Let the starting step be step 0. Assuming we are on step $n \geq 2$, how did we get here?
  - Either we took a single step from step $n-1$
  - Or we took two steps from step $n-2$
- Combining the number of ways to get to step $n-1$ with the number of ways to get to step $n-2$ yields the number of ways to get to step n
- $S_n = S_{n-1} + S_{n-2}$
  - How many ways are there to get to step 0? **Exactly 1** ($S_0 = 1$)
  - How many ways are there to get to step 1? **Exactly 1** ($S_1 = 1$)

Steps to Compute Steps

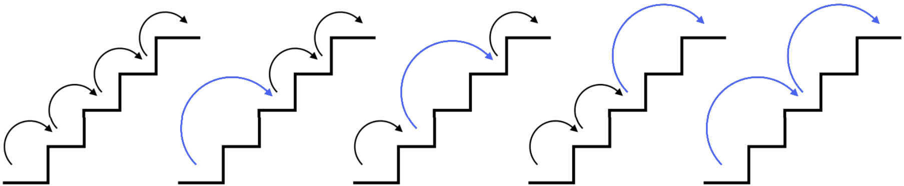
- Let the starting step be step 0. Assuming we are on step $n \geq 2$, how did we get here?
  - Either we took a single step from step $n-1$
  - Or we took two steps from step $n-2$
- Combining the number of ways to get to step $n-1$ with the number of ways to get to step $n-2$ yields the number of ways to get to step n
- $S_n = S_{n-1} + S_{n-2}$
  - How many ways are there to get to step 0? **Exactly 1** ($S_0 = 1$)
  - How many ways are there to get to step 1? **Exactly 1** ($S_1 = 1$)
- $S_n = F_{n+1}$

Making Choices

- There is another angle to the staircase problem

Making Choices

- There is another angle to the staircase problem
- We can just choose which steps to take two steps from, and fill the rest with single steps



Placing Steps

- We have to choose where to place our steps of size 2
- If we have n steps, how many ways can we place k steps of size 2?

Placing Steps

- We have to choose where to place our steps of size 2
- If we have n steps, how many ways can we place k steps of size 2?

$$\binom{n-k}{k} \text{ ways}$$

Placing Steps

- We have to choose where to place our steps of size 2
- If we have n steps, how many ways can we place k steps of size 2?

$$\binom{n-k}{k} \text{ ways}$$

- How many possible values of k are there?

Placing Steps

- We have to choose where to place our steps of size 2
- If we have n steps, how many ways can we place k steps of size 2?

$$\binom{n-k}{k} \text{ ways}$$

- How many possible values of k are there?

$$\left\lfloor \frac{n}{2} \right\rfloor$$

Placing Steps

- We have to choose where to place our steps of size 2
- If we have n steps, how many ways can we place k steps of size 2?

$$\binom{n-k}{k} \text{ ways}$$

- How many possible values of k are there?

$$\left\lfloor \frac{n}{2} \right\rfloor$$

$$\text{Thus, } \sum_{k=0}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n-k}{k} = S_n = F_{n+1}$$

Questions?

[Combinatorics] has a relation to almost every species of useful knowledge that the mind of man can be employed upon.

— JAMES BERNOULLI, Ars Conjectandi ("The Art of Conjecturing") (1713)

Bibliography

Jeff Erickson.
Algorithms.
1st edition, 06 2019.

Donald E. Knuth.
The Art of Computer Programming, Vol. 1: Fundamental Algorithms.
Addison-Wesley, Reading, Mass., third edition, 1997.

Blaise Pascal.
Traité du triangle arithmétique , avec quelques autres petits traitez sur la mesme matière. Par Monsieur Pascal.
G. Desprez, 1665.