Lecture 9

Pseudorandom Number Generators

Linear congruential method

$$x_{n+1} = (ax_n + c) \bmod m$$

We choose four numbers:

- the modulus m
- multiplier a
- increment c
- seed x_0

We generate a sequence of numbers $x_1, x_2, \ldots, x_n, \ldots$ with $0 \le x_i < m$ by using the congruence

Hash Functions $h(k) = k \bmod m$,

$h_0(k) = k \bmod n$

$h_1(k) = (k+1) \bmod n$

...

$h_m(k) = (k+m) \bmod n$

enhance security

Shift Ciphers

$p \in \mathbf{Z}_{26} = \{0, 1, \ldots, 25\}$

$f(p) = (p + k) \bmod 26.$

$f^{-1}(p) = (p - k) \bmod 26.$

$f(p) = (ap + b) \bmod 26.$

How about the decryption? Suppose $\gcd(a, 26) = 1$.

Suppose that $c = (ap + b) \bmod 26$ with $\gcd(a, 26) = 1$. To decrypt, we need to show how to express p in terms of c. That is, we solve the congruence for p:

$$c \equiv ap + b \pmod{26}.$$

Subtract b from both sides, we have $ap \equiv c - b \pmod{26}$. Since $\gcd(a, 26) = 1$, we know that there is an inverse $\bar{a}$ of a modulo 26:

$$p \equiv \bar{a}(c - b) \pmod{26}.$$

Private Key Cryptosystem

RAS Cryptosystem

- RSA as Public Key System
  - Only target recipient can decrypt the message:

Pick two large primes p and q. Let $n = pq$. **Encryption key** (n, e) and **decryption key** (n, d) are selected such that

- $\gcd(e, (p-1)(q-1)) = 1$
- $ed \equiv 1 \pmod{(p-1)(q-1)}$

RSA encryption: $C = M^e \bmod n$

RSA decryption: $M = C^d \bmod n$

RSA as a Public Key System

- Public key: (n, e)
- Private key: d
- p, q must be kept secret!

Encrypt the message "STOP" with key $(n = 2537, e = 13)$. Note that $2537 = 43 \cdot 59$, where $p = 43$ and $q = 59$ are primes, and $\gcd(e, (p-1)(q-1)) = 1$.

Solution:

1. Translate into integers: 18191415
2. Divide this into blocks of 4 digits (because $2525 < 2537 < 252525$): 1819 1415
3. Encrypt each block using the mapping

$$C = M^{13} \bmod 2537.$$

We have $1819^{13} \bmod 2537 = 2081$ and $1415^{13} \bmod 2537 = 2182$. The encrypted message is 2081 2182.

For each block, transform the ciphertext into plaintext message:

$$M = C^d \bmod n$$

Example: What is the decrypted message of 0981 0461 with $e = 13$, $p = 43$, $q = 59$?

Solution: Recall that $ed \equiv 1 \pmod{(p-1)(q-1)}$. Thus, $d = 937$ is an inverse of 13 modulo $42 \cdot 58 = 2436$.

For each block, transform it into plaintext message:

$$M = C^{937} \bmod 2537.$$

Since $0981^{937} \bmod 2537 = 0704$ and $0461^{937} \bmod 2537 = 1115$, the plaintext message is 0704 1115, which is "HELP".

RSA decryption: $M = C^d \bmod n$. Why?

According to (1), the inverse d exists. According to (2), there exists an integer k such that

$$de = 1 + k(p-1)(q-1).$$

It follows that $C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod{n}$.

Assuming that $\gcd(M, p) = \gcd(M, q) = 1$, we have $M^{p-1} \equiv 1 \pmod{p}$ and $M^{q-1} \equiv 1 \pmod{q}$. (see Theorem 3 in Section 4.4)

According to (1), the inverse d exists. According to (2), there exists an integer k such that

$$de = 1 + k(p-1)(q-1).$$

It follows that $C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod{n}$.

Assuming that $\gcd(M, p) = \gcd(M, q) = 1$, we have $M^{p-1} \equiv 1 \pmod{p}$ and $M^{q-1} \equiv 1 \pmod{q}$.

$$C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 = M \pmod{p}$$
$$C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 = M \pmod{q}.$$

Because $\gcd(p, q) = 1$, we have

$$C^d \equiv M \pmod{pq}.$$

This basically implies that

$$M = C^d \bmod n$$

RSA as Digital Signature

$S = M^d \bmod n$ **(RSA signature)**

$M = S^e \bmod n$ **(RSA verification)**

Alice's RSA public key is (n, e) and her private key is d.

Alice can send her message to as many people as she wants and by signing it in this way, every recipient can be sure it came from Alice.

Diffie-Hellman Key Exchange Protocol

Before introducing the protocol:

Definition: A primitive root modulo a prime p is an integer r in $\mathbf{Z}_p$ such that every nonzero element of $\mathbf{Z}_p$ is a power of r.

Example: Whether 2 is a primitive root modulo 11?

When we compute the powers of 2 in $\mathbf{Z}_{11}$, we obtain $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^9 = 6$, $2^{10} = 1$. Because every element of $\mathbf{Z}_{11}$ is a power of 2, 2 is a primitive root of 11.

Suppose that Alice and Bob want to share a common key. Consider $\mathbf{Z}_p$.

(1) Alice and Bob agree to use a prime p and a primitive root a of p.
(2) Alice chooses a secret integer k_1 and sends $a^{k_1} \bmod p$ to Bob.
(3) Bob chooses a secret integer k_2 and sends $a^{k_2} \bmod p$ to Alice.
(4) Alice computes $(a^{k_2})^{k_1} \bmod p$.
(5) Bob computes $(a^{k_1})^{k_2} \bmod p$.

Alice and Bob have computed their shared key:

$$(a^{k_2})^{k_1} \bmod p = (a^{k_1})^{k_2} \bmod p.$$

- Public information: p, a, $a^{k_1} \bmod p$, and $a^{k_2} \bmod p$
- Secret: k_1, k_2, $(a^{k_2})^{k_1} \bmod p = (a^{k_1})^{k_2} \bmod p$

Note that it is very hard to determine k_1 with a, p, and $a^{k_1} \bmod p$.

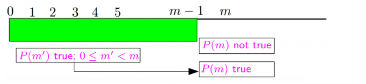
Lecture 10

The statement $P(n)$ is true for all $n = 0, 1, 2, \ldots$

We prove this by

(i) Assume that a counterexample exists, i.e., There is some $n > 0$ for which $P(n)$ is false.
(ii) Let $m > 0$ be the smallest value for which $P(n)$ is false
(iii) Then, use the fact that $P(m')$ is true for all $0 \le m' < m$ to show that $P(m)$ is true, contradicting the choice of m.

Contradiction!



The key step were

- $P(0)$ is true such that the smallest counterexample exists
- proving that

$$P(n-1) \to P(n)$$

Recall that $P(n)$ is the statement

$$0 + 1 + 2 + 3 + \ldots + n = \frac{(n+1)n}{2}.$$

Let $P(n)$ denote $2^{n+1} \ge n^2 + 2$. We just showed that

(a) $P(0)$ is true
(b) If $n > 0$, then $P(n-1) \to P(n)$

What did we do?

- Suppose there is some n for which $P(n)$ is false (*)
- Let n be the smallest counterexample
- From (a) $n > 0$, so $P(n-1)$ is true
- From (b), using direct inference, $P(n)$ is true
- This leads to contradiction.
- Thus, $P(n)$ is true for all $n \in N$.

Principle. (Weak Principle of Mathematical Induction)

(a) Basic Step: the statement $P(b)$ is true
(b) Inductive Step: the statement $P(n-1) \to P(n)$ is true for all $n > b$

Thus, $P(n)$ is true for all integers $n \ge b$.

Example 1

For all $n \ge 0$, $2^{n+1} \ge n^2 + 2$

Let $P(n)$ denote $2^{n+1} \ge n^2 + 2$.

(i) Note that for $n = 0$, $2^{0+1} = 2 \ge 2 = 0^2 + 2$, which is $P(0)$
(ii) Suppose that $n > 0$ and that $2^n \ge (n-1)^2 + 2$ (*)

$$\begin{aligned} 2^{n+1} &\ge 2(n-1)^2 + 4 \\ &= (n^2+2) + (n^2 - 4n + 4) \\ &= n^2 + 2 + (n-2)^2 \\ &\ge n^2 + 2 \end{aligned}$$

Hence, we have just proven that for $n > 0$, $P(n-1) \to P(n)$.

By mathematical induction, $\forall n \ge 0, 2^{n+1} \ge n^2 + 2$.

Principle (Strong Principle of Mathematical Induction):

(a) Basic Step: the statement $P(b)$ is true
(b) Inductive Step: for all $n > b$, the statement

$$P(b) \wedge P(b+1) \wedge \ldots \wedge P(n-1) \to P(n) \text{ is true.}$$

Then, $P(n)$ is true for all integers $n \ge b$.

Recursion

Towers of Hanoi

Running Time: $M(n)$ is number of disk moves needed for n disks.

- $M(1) = 1$
- if $n > 1$, then $M(n) = 2M(n-1) + 1$

$$M(n) = 2^n - 1.$$

Recurrence

Theorem: If $T(n) = rT(n-1) + a$, $T(0) = b$, and $r \ne 1$, then

$$T(n) = r^n b + a\frac{1 - r^n}{1 - r}$$

Formula of Recurrences

- Basis step: We verify that $T(0)$ holds:
- Inductive step: We show that the conditional statement "if $T(n-1)$ holds, then $T(n)$ holds" for all $n \ge 1$:
  Now assume that $n > 0$ and

$$T(n-1) = r^{n-1}b + a\frac{1 - r^{n-1}}{1 - r}.$$

Thus,

$$\begin{aligned} T(n) &= rT(n-1) + a \\ &= r\left(r^{n-1}b + a\frac{1 - r^{n-1}}{1-r}\right) + a \\ &= r^n b + \frac{ar - ar^n}{1-r} + a \\ &= r^n b + \frac{ar - ar^n + a - ar}{1-r} \\ &= r^n b + a\frac{1 - r^n}{1 - r}. \end{aligned}$$

First-Order Linear Recurrences

A recurrence of the form $T(n) = f(n)T(n-1) + g(n)$ is called a first-order linear recurrence.

- **First Order**: because it only depends upon going back one step, i.e., $T(n-1)$
- If it depends upon $T(n-2)$, then it would be a second-order recurrence, e.g., $T(n) = T(n-1) + 2T(n-2)$.
- **Linear**: because $T(n-1)$ only appears to the first power.
- Something like $T(n) = (T(n-1))^2 + 3$ would be a non-linear first-order recurrence relation. $T(n) = f(n)T(n-1) + g(n)$

$$\begin{aligned} T(n) &= rT(n-1) + g(n) \\ &= r(rT(n-2) + g(n-1)) + g(n) \\ &= r^2T(n-2) + rg(n-1) + g(n) \\ &= r^3T(n-3) + r^2g(n-2) + rg(n-1) + g(n) \\ &\vdots \\ &= r^nT(0) + \sum_{i=0}^{n-1} r^i g(n-i) \end{aligned}$$

$$T(n) = \begin{cases} rT(n-1) + g(n), & \text{if } n > 0 \\ a, & \text{if } n = 0 \end{cases}$$

$$T(n) = r^n a + \sum_{i=1}^{n} r^{n-i} g(i)$$

Solve $T(n) = 4T(n-1) + 2^n$ with $T(0) = 6$.

$$\begin{aligned} T(n) &= 6 \cdot 4^n + \sum_{i=1}^{n} 4^{n-i} \cdot 2^i \\ &= 6 \cdot 4^n + 4^n \sum_{i=1}^{n} 4^{-i} \cdot 2^i \\ &= 6 \cdot 4^n + 4^n \sum_{i=1}^{n} (\tfrac{1}{2})^i \\ &= 6 \cdot 4^n + (1 - \tfrac{1}{2^n}) \cdot 4^n \\ &= 7 \cdot 4^n - 2^n. \end{aligned}$$

Theorem. For any real number $x \ne 1$,

$$\sum_{i=1}^{n} ix^i = \frac{nx^{n+2} - (n+1)x^{n+1} + x}{(1-x)^2}.$$

Divide and conquer algorithms

Iterating recurrences

Three different behaviors

Growth Rates of Solutions to Recurrences

$$T(n) = \begin{cases} T(1), & \text{if } n = 1, \\ 2T(n/2) + n, & \text{if } n \ge 2. \end{cases}$$

$$\begin{aligned} T(n) &= 2T\left(\tfrac{n}{2}\right) + n && = 2\left(2T\left(\tfrac{n}{4}\right) + \tfrac{n}{2}\right) + n \\ &= 4T\left(\tfrac{n}{4}\right) + 2n && = 4\left(2T\left(\tfrac{n}{8}\right) + \tfrac{n}{4}\right) + 2n \\ &= 8T\left(\tfrac{n}{8}\right) + 3n \\ &\vdots \\ &= 2^iT\left(\tfrac{n}{2^i}\right) + in \\ &\vdots \\ &= 2^{\log_2 n}T\left(\tfrac{n}{2^{\log_2 n}}\right) + (\log_2 n)n \end{aligned}$$

End when $i = \log_2 n$

$nT(1) + n\log_2 n$

$$T(n) = \begin{cases} 1, & \text{if } n = 1, \\ T(n/2) + 1, & \text{if } n \ge 2. \end{cases}$$

$$\begin{aligned} T(n) &= T\left(\tfrac{n}{2}\right) + 1 && = \left(T\left(\tfrac{n}{2^2}\right) + 1\right) + 1 \\ &= T\left(\tfrac{n}{2^2}\right) + 2 && = \left(T\left(\tfrac{n}{2^3}\right) + 1\right) + 2 \\ &= T\left(\tfrac{n}{2^3}\right) + 3 \\ &\vdots \\ &= T\left(\tfrac{n}{2^i}\right) + i \\ &\vdots \\ &= T\left(\tfrac{n}{2^{\log_2 n}}\right) + \log_2 n && = 1 + \log_2 n \end{aligned}$$

$$T(n) = \begin{cases} 1, & \text{if } n = 1, \\ T(n/2) + n, & \text{if } n \ge 2. \end{cases}$$

$$\begin{aligned} T(n) &= T\left(\tfrac{n}{2}\right) + n \\ &= T\left(\tfrac{n}{2^2}\right) + \tfrac{n}{2} + n \\ &= T\left(\tfrac{n}{2^3}\right) + \tfrac{n}{2^2} + \tfrac{n}{2} + n \\ &\vdots \\ &= T\left(\tfrac{n}{2^i}\right) + \tfrac{n}{2^{i-1}} + \cdots + \tfrac{n}{2^2} + \tfrac{n}{2} + n \\ &\vdots \\ &= T\left(\tfrac{n}{2^{\log_2 n}}\right) + \tfrac{n}{2^{\log_2 n - 1}} + \cdots + \tfrac{n}{2^2} + \tfrac{n}{2} + n \\ &= 1 + 2 + 2^2 + \cdots + \tfrac{n}{2^2} + \tfrac{n}{2} + n \end{aligned}$$

$\Theta(n)$

Theorem: Suppose that we have a recurrence of the form

$$T(n) = aT(n/2) + n,$$

where a is a positive integer and $T(1)$ is nonnegative. Then we have the following big Θ bounds on the solution:

- If $a < 2$, then $T(n) = \Theta(n)$.
- If $a = 2$, then $T(n) = \Theta(n \log_2 n)$.
- If $a > 2$, then $T(n) = \Theta(n^{\log_2 a})$.

We will now prove the case with $a > 2$.

Assume that $n = 2^i$.

$$T(n) = a^iT\left(\tfrac{n}{2^i}\right) + \left(\tfrac{a^{i-1}}{2^{i-1}} + \tfrac{a^{i-2}}{2^{i-2}} + \cdots \tfrac{a}{2} + 1\right)n$$

$$T(n) = a^{\log_2 n}T(1) + n\sum_{i=0}^{\log_2 n - 1} \left(\tfrac{a}{2}\right)^i$$

Work at "bottom" | Iterated Work

Since $a > 2$, the geometric series is Θ of the largest term.

$$n\sum_{i=0}^{\log_2 n - 1}\left(\tfrac{a}{2}\right)^i = n\frac{1 - (a/2)^{\log_2 n}}{1 - a/2} = n\Theta((a/2)^{\log_2 n - 1})$$

n times the largest term in the geometric series is

$$n\left(\tfrac{a}{2}\right)^{\log_2 n - 1} = \frac{2}{a} \cdot \frac{n \cdot a^{\log_2 n}}{2^{\log_2 n}} = \frac{2}{a} \cdot \frac{n \cdot a^{\log_2 n}}{n} = \frac{2}{a} \cdot a^{\log_2 n}$$

Notice that

$$a^{\log_2 n} = \left(2^{\log_2 a}\right)^{\log_2 n} = \left(2^{\log_2 n}\right)^{\log_2 a} = n^{\log_2 a}$$

Theorem: Suppose that we have a recurrence of the form

$$T(n) = aT(n/b) + cn^d,$$

where a is a positive integer, $b \ge 1$, c, d are real numbers with c positive and d nonnegative, and $T(1)$ is nonnegative. Then we have the following big Θ bounds on the solution:

- If $a < b^d$, then $T(n) = \Theta(n^d)$.
- If $a = b^d$, then $T(n) = \Theta(n^d \log_2 n)$.
- If $a > b^d$, then $T(n) = \Theta(n^{\log_b a})$.

Lecture 11 Pigeonhole Principle Counting

The Pigeonhole Principle: If k is a positive integer and $k+1$ or more objects are placed into k boxes, then there is at least one box containing two or more of the objects.

Proof by Contradiction: Suppose that none of the k boxes contains more than one object. Then the total number of objects would be at most k. This is a contradiction, because there are at least $k+1$ objects.

There are 5 bins and 12 objects. Then there must be a bin with at least 3 objects. Why?

If N objects are placed into k bins, then there is at least one bin containing at least $\lceil N/k \rceil$ objects.

Proof: Suppose that none of the boxes contains more than $\lceil N/k \rceil$ objects. Then, the total number of objects is at most

$$k\left(\left\lceil \frac{N}{k} \right\rceil - 1\right) < k\left(\left(\frac{N}{k} + 1\right) - 1\right) = N$$

This is a contradiction because there are a total of N objects.

Theorem: Every sequence of $n^2 + 1$ distinct real numbers contains a subsequence of length $n+1$ that is either strictly increasing or strictly decreasing.

Suppose that $a_1, a_2, \ldots, a_N$ is a sequence of real numbers:

- A subsequence of this sequence is a sequence of the form $a_{i_1}, a_{i_2}, \ldots, a_{i_m}$, where $1 \le i_1 < i_2 < \ldots < i_m \le N$.
- A sequence is called strictly increasing if each term is larger than the one that precedes it.

Proof: Let $a_1, a_2, \ldots, a_{n^2+1}$ be a sequence of $n^2 + 1$ distinct real numbers. Associate (i_k, d_k) to the term a_k:

- i_k: the length of the longest increasing subsequence starting at a_k
- d_k: the length of the longest decreasing subsequence starting at a_k.

Suppose that there are no increasing or decreasing subsequences of length $n+1$. I.e., $i_k \le n$ and $d_k \le n$ for $k = 1, 2, \ldots, n^2 + 1$.

By the product rule there are n^2 possible ordered pairs for (i_k, d_k). By the pigeonhole principle, two of these $n^2 + 1$ ordered pairs are equal. $d_s = d_t$.

That is, there exist terms a_s and a_t with $s < t$ such that $i_s = i_t$ and

Proof: There exist terms a_s and a_t with $s < t$ such that $i_s = i_t$ and $d_s = d_t$. We will show that this is impossible.

The terms of the sequence are distinct, either $a_s < a_t$ or $a_s > a_t$:

- $a_s < a_t$: Since $i_s = i_t$, an increasing subsequence of length $i_t + 1$ can be built, i.e., a_s, a_t, ... (followed by an increasing subsequence of length i_t beginning at a_t)
- $a_s > a_t$, Since $d_s = d_t$, an decreasing sequence of length $d_t + 1$ can be built, i.e., a_s, a_t, ...

Permutations $P(n, r) = n(n-1)(n-2)\cdots(n-r+1)$

$$P(n, r) = \frac{n!}{(n-r)!}.$$

Inclusion-Exclusion Principle 容斥原理

Let $E_1, E_2, \ldots, E_n$ be finite sets:

$$|E_1 \cup E_2 \cup \cdots \cup E_n| = \sum_{1 \le i \le n} |E_i| - \sum_{1 \le i < j \le n} |E_i \cap E_j| + \sum_{1 \le i < j < k \le n} |E_i \cap E_j \cap E_k| - \ldots + (-1)^{n+1}|E_1 \cap E_2 \cap \ldots \cap E_n|.$$

$$|\cup_{i=1}^n E_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}|$$

Combinations $C(n, r)$ $\binom{n}{r}$

$$\binom{n}{r} = C(n, r) = \frac{P(n, r)}{r!} = \frac{n!}{r!(n-r)!}$$

$$P(n, r) = C(n, r)P(r, r)$$

The Binomial Theorem

Let x and y be variables, and let n be a nonnegative integer:

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j}y^j = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

Example 2: What is the coefficient of $x^{12}y^{13}$ in the expansion of $(2x - 3y)^{25}$?

First, note that this expression equals $(2x + (-3y))^{25}$

$$(2x + (-3y))^{25} = \sum_{j=0}^{25} \binom{25}{j} (2x)^{25-j}(-3y)^j.$$

The coefficient of $x^{12}y^{13}$ in the expansion is obtained when $j = 13$:

$$\binom{25}{13} 2^{12}(-3)^{13} = -\frac{25!}{13!\,12!} 2^{12} 3^{13}.$$

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n. \quad \sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n$$

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

Pascal's identity

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

Other Identities Involving Binomial Coefficients

Let n and r be nonnegative integers with $r \le n$.

$$\sum_{k=r+1}^{n+1} \binom{k-1}{r} = \sum_{j=r}^{n} \binom{j}{r} \qquad \binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r}$$

Labelling and Trinomial Coefficients

How many different ways to label n distinct objects?

- There are $\binom{n}{k_1}$ ways to choose the red items
- There are then $\binom{n-k_1}{k_2}$ ways to choose the blue items from the remaining $n - k_1$.

$$\begin{aligned} \binom{n}{k_1}\binom{n-k_1}{k_2} &= \frac{n!}{k_1!(n-k_1)!} \frac{(n-k_1)!}{(k_2)!(n-k_1-k_2)!} \\ &= \frac{n!}{k_1!k_2!(n-k_1-k_2)!} = \frac{n!}{k_1!k_2!k_3!} \end{aligned}$$

This is called a trinomial coefficient and denote it as

$$\binom{n}{k_1\ k_2\ k_3} = \frac{n!}{k_1!k_2!k_3!},$$

where $k_1 + k_2 + k_3 = n$.

What is the coefficient of $x^{k_1}y^{k_2}z^{k_3}$ in $(x + y + z)^n$?

Lecture 13 Solving Linear Recurrence Relations

- Linear Homogeneous Recurrence Relations
- Linear Nonhomogeneous Recurrence Relations

Definition: A linear homogeneous relation of degree k with constant coefficients is a recurrence relation of the form

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots + c_ka_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \ne 0$.

- linear: it is a linear combination of previous terms
- homogeneous: all terms are multiples of a_j's
- degree k: a_n is expressed by the previous k terms
- constant coefficients: coefficients are constants

Example:

- $P_n = 1.11 \cdot P_{n-1}$ linear homogeneous recurrence relation of degree 1
- $f_n = f_{n-1} + f_{n-2}$ linear homogeneous recurrence relation of degree 2
- $a_n = a_{n-1} + a_{n-2}^2$ NOT linear
- $H_n = 2H_{n-1} + 1$ NOT homogeneous
- $B_n = nB_{n-1}$ coefficients are not constants

Degree Two

Theorem: Let c_1 and c_2 be real numbers. Suppose that $r^2 - c_1r - c_2 = 0$ has two distinct roots r_1 and r_2.

Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2}$ if and only if

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n \text{ for } n = 0, 1, 2, \ldots,$$

where α_1 and α_2 are constants.

Proof: To show that both $\{a_n\}$ and $\{\alpha_1r_1^n + \alpha_2r_2^n\}$ are the solutions of the recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2}$ and satisfy the initial conditions.

- $\{\alpha_1r_1^n + \alpha_2r_2^n\}$ is a solution of the recurrence relation.
- For every recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2}$, there exist α_1 and α_2 that satisfy the initial conditions.

Solve Linear Recurrence Relations:

- Solve r_1 and r_2 with $r^2 - c_1r - c_2 = 0$.
- Solve α_1 and α_2 with the initial conditions.

Theorem: If the $r^2 - c_1r - c_2 = 0$ has only 1 root r_0, then

$$a_n = (\alpha_1 + \alpha_2 n)r_0^n,$$

for all $n \ge 0$ and two constants α_1 and α_2.

Degree k

$$a_n = \sum_{i=1}^{t}\left(\sum_{j=0}^{m_i - 1} \alpha_{i,j} n^j\right) r_i^n$$

$$\begin{aligned} a_n = &(\alpha_{1,0} + \alpha_{1,1}n + \cdots + \alpha_{1,m_1-1}n^{m_1-1})r_1^n \\ &+ (\alpha_{2,0} + \alpha_{2,1}n + \cdots + \alpha_{2,m_2-1}n^{m_2-1})r_2^n \\ &+ \cdots + (\alpha_{t,0} + \alpha_{t,1}n + \cdots + \alpha_{t,m_t-1}n^{m_t-1})r_t^n \end{aligned}$$

for all $n \ge 0$ and constants $\alpha_{i,j}$.

Linear Nonhomogeneous Recurrence Relations

Definition: A linear nonhomogeneous relation with constant coefficients may contain some terms $F(n)$ that depend only on n

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \dots + c_ka_{n-k} + F(n).$$

The recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2} + \dots + c_ka_{n-k}$ is called the associated homogeneous recurrence relation.

Theorem: If $\{a_n^{(p)}\}$ is any particular solution to the linear nonhomogeneous relation with constant coefficients,

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \dots + c_ka_{n-k} + F(n),$$

Then all its solutions are of the form

$$a_n = a_n^{(p)} + a_n^{(h)},$$

where $\{a_n^{(h)}\}$ is any solution to the associated homogeneous recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2} + \dots + c_ka_{n-k}$.

$a_n = 3a_{n-1} + 2n.$

To compute $a_n^{(h)}$:
The characteristic equation is

$$r^2 - 3r = 0.$$

The roots are $r_1 = 3$ and $r_2 = 0$. By So, assume that

$$a_n^{(h)} = \alpha 3^n.$$

To compute $a_n^{(p)}$: Try $a_n^{(p)} = cn + d$. Thus,

$$cn + d = 3(c(n-1) + d) + 2n.$$

We get $c = -1$ and $d = -3/2$. Thus, $a_n^{(p)} = -n - 3/2$.

Initial condition:

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha 3^n - n - 3/2.$$

Base on the initial condition $a_1 = 3$. We have $3 = -1 - 3/2 + 3\alpha$, which implies $\alpha = 11/6$. Thus, $a_n = -n - 3/2 + (11/6)3^n$.

For previous two examples, we made a guess that there are solutions of a particular form. This was not an accident.

Suppose that $\{a_n\}$ satisfies the linear nonhomogeneous recurrence relation

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \dots + c_ka_{n-k} + F(n),$$

where $c_1, c_2, \dots, c_k$ are real numbers, and

$$F(n) = (b_tn^t + b_{t-1}n^{t-1} + \dots + b_1n + b_0)s^n,$$

where $b_0, b_1, \dots, b_t$ and s are real numbers. When s is not a root of the characteristic equation of the associated linear homogeneous recurrence relation, there is a particular solution of the form

$$(p_tn^t + p_{t-1}n^{t-1} + \dots + p_1n + p_0)s^n.$$

When s is a root of this characteristic equation and its multiplicity is m, there is a particular solution of the form

$$n^m(p_tn^t + p_{t-1}n^{t-1} + \dots + p_1n + p_0)s^n.$$

Generating Function

$$G(x) = a_0 + a_1x + \dots + a_kx^k + \dots = \sum_{k=0}^{\infty} a_kx^k$$

For $|x| < 1$, function $G(x) = 1/(1-x)$ is the generating function of the sequence 1, 1, 1, 1, . . . ,

$$1/(1-x) = 1 + x + x^2 + \dots$$

For $|ax| < 1$, function $G(x) = 1/(1-ax)$ is the generating function of the sequence 1, a, a^2, a^3, . . . ,

$$1/(1-ax) = 1 + ax + a^2x^2 + \dots$$

For $|x| < 1$, $G(x) = 1/(1-x)^2$ is the generating function of the sequence 1, 2, 3, 4, 5, . . .

$$1/(1-x)^2 = 1 + 2x + 3x^2 + \dots$$

Operations of Generating Functions

Theorem: Let $f(x) = \sum_{k=0}^{\infty} a_kx^k$, and $g(x) = \sum_{k=0}^{\infty} b_kx^k$. Then,

$$f(x) + g(x) = \sum_{k=0}^{\infty}(a_k + b_k)x^k \qquad f(x)g(x) = \sum_{k=0}^{\infty}\Big(\sum_{j=0}^{k} a_jb_{k-j}\Big)x^k$$

Example 1: To obtain the corresponding sequence of $G(x) = 1/(1-x)^2$: Consider $f(x) = 1/(1-x)$ and $g(x) = 1/(1-x)$. Since the sequence of $f(x)$ and $g(x)$ corresponds to 1, 1, 1, ..., we have

$$G(x) = f(x)g(x) = \sum_{k=0}^{\infty}(k+1)a^kx^k \qquad G(x) = f(x)g(x) = \sum_{k=0}^{\infty}(k+1)x^k.$$

Example 2: To obtain the corresponding sequence of $G(x) = 1/(1-ax)^2$ for $|ax| < 1$:

Consider $f(x) = 1/(1-ax)$ and $g(x) = 1/(1-ax)$. Since the sequence of $f(x)$ and $g(x)$ corresponds to 1, a, a^2, ..., we have

Example 1

$a_n = 6a_{n-1} - 9a_{n-2} + F(n)$ with $F(n) = n^22^n$ and $F(n) = (n^2+1)3^n$.

To compute $a_n^{(h)}$: $a_n^{(h)} = (\alpha_1 + \alpha_2n)3^n$.

To compute $a_n^{(p)}$ of $F(n) = n^22^n$:

Since $s = 2$ is not a root of the characteristic equation, we have

$$a_n^{(p)} = (p_2n^2 + p_1n + p_0)2^n.$$

Substituting $a_n^{(p)}$ into $a_n = 6a_{n-1} - 9a_{n-2} + F(n)$ to derive p_2, p_1, and p_0:

$$(p_2n^2 + p_1n + p_0)2^n = 6(p_2(n-1)^2 + p_1(n-1) + p_0)2^{n-1} - 9(p_2(n-2)^2 + p_1(n-2) + p_0)2^{n-2} + n^22^n.$$

To compute $a_n^{(p)}$ of $F(n) = (n^2+1)3^n$:

Since $s = 3$ is a root of the characteristic equation with multiplicity $m = 2$, we have

$$a_n^{(p)} = n^2(p_2n^2 + p_1n + p_0)3^n.$$

Substituting $a_n^{(p)}$ into $a_n = 6a_{n-1} - 9a_{n-2} + F(n)$ to derive p_2, p_1, and p_0:
...

$a_n = a_n^{(h)} + a_n^{(p)} = (\alpha_1 + \alpha_2n)3^n + n^2(p_2n^2 + p_1n + p_0)3^n.$

Example 2: The Term n^m

$a_n = 5a_{n-1} - 6a_{n-2} + 2^n$

Solution:

- $a_n^{(h)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n$
- $a_n^{(p)}$ should be in the form of np_02^n.
- Try $a_n^{(p)} = p_0 \cdot 2^n$:

$$p_0 \cdot 2^n = 5p_0 \cdot 2^{n-1} - 6p_0 \cdot 2^{n-2} + 2^n.$$

Since $s = 2$ is a root of the characteristic equation,

$$p_0 \cdot 2^n = 5p_0 \cdot 2^{n-1} - 6p_0 \cdot 2^{n-2}$$

always holds. Thus, we obtain $0 = 4$.

$$(1+x)^n = \sum_{k=0}^{n} C(n,k)x^k$$
$$(1+ax)^n = \sum_{k=0}^{n} C(n,k)a^kx^k$$
$$(1+x^r)^n = \sum_{k=0}^{n} C(n,k)x^{rk}$$
$$\frac{1-x^{n+1}}{1-x} = \sum_{k=0}^{n} x^k = 1 + x + x^2 + \dots + x^n$$
$$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k = 1 + x + x^2 + \dots$$
$$\frac{1}{1-ax} = \sum_{k=0}^{\infty} a^kx^k = 1 + ax + a^2x^2 + \dots$$
$$\frac{1}{1-x^r} = \sum_{k=0}^{\infty} x^{rk} = 1 + x^r + x^{2r} + \dots$$
$$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty}(k+1)x^k = 1 + 2x + 3x^2 + \dots$$
$$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)x^k$$
$$\frac{1}{(1+x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)(-1)^kx^k$$
$$\frac{1}{(1-ax)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)a^kx^k$$
$$e^x = \sum_{k=0}^{\infty}\frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$
$$\ln(1+x) = \sum_{k=0}^{\infty}\frac{(-1)^{k+1}x^k}{k} = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \dots$$

Generating Function Example 1

Solve the recurrence relation $a_k = 3a_{k-1}$ for $k = 1, 2, 3, \dots$ and initial condition $a_0 = 2$.

Let $G(x)$ be the generating function for the sequence $\{a_k\}$, that is, $G(x) = \sum_{k=0}^{\infty} a_kx^k$. We aim to first derive the formulation of $G(x)$.

$$G(x) - 3xG(x) = \sum_{k=0}^{\infty} a_kx^k - 3\sum_{k=1}^{\infty} a_{k-1}x^k = a_0 + \sum_{k=1}^{\infty}(a_k - 3a_{k-1})x^k = 2,$$

$$G(x) = \frac{2}{(1-3x)}$$

Example 2

$a_n = 8a_{n-1} + 10^{n-1}$, $a_1 = 9$. **Solution**: We extend this sequence by setting $a_0 = 1$. We have $a_1 = 8a_0 + 10^0 = 8 + 1 = 9$. Let $G(x) = \sum_{n=0}^{\infty} a_nx^n$.

$$G(x) - 1 = \sum_{n=1}^{\infty} a_nx^n = \sum_{n=1}^{\infty}(8a_{n-1}x^n + 10^{n-1}x^n)$$
$$= 8\sum_{n=1}^{\infty} a_{n-1}x^n + \sum_{n=1}^{\infty} 10^{n-1}x^n$$
$$= 8x\sum_{n=1}^{\infty} a_{n-1}x^{n-1} + x\sum_{n=1}^{\infty} 10^{n-1}x^{n-1}$$
$$= 8x\sum_{n=0}^{\infty} a_nx^n + x\sum_{n=0}^{\infty} 10^nx^n$$
$$= 8xG(x) + x/(1-10x),$$

$$G(x) = \frac{1-9x}{(1-8x)(1-10x)} = G(x) = \frac{1}{2}\left(\frac{1}{1-8x} + \frac{1}{1-10x}\right)$$

$$G(x) = \frac{1}{2}\left(\sum_{n=0}^{\infty} 8^nx^n + \sum_{n=0}^{\infty} 10^nx^n\right) = \sum_{n=0}^{\infty}\frac{1}{2}(8^n + 10^n)x^n.$$

Cartesian Product

Let $A = \{a_1, a_2, \dots, a_m\}$ and $B = \{b_1, b_2, \dots, b_n\}$, the Cartesian product $A \times B$ is the set of pairs

$$\{(a_1,b_1), (a_2,b_2), \dots, (a_1,b_n), \dots, (a_m,b_n)\}.$$

Cartesian product defines a set of all ordered arrangements of elements in the two sets.

A subset R of the Cartesian product $A \times B$ is called a relation from the set A to the set B.

Definition: Let A and B be two sets. A binary relation from A to B is a subset of a Cartesian product $A \times B$.

Let $R \subseteq A \times B$ denote R is a set of ordered pairs of the form (a,b) where $a \in A$ and $b \in B$.

We use the notation aRb to denote $(a,b) \in R$, and $a \not R b$ to denote $(a,b) \notin R$.

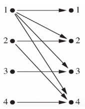
Example: Let $A = \{a,b,c\}$ and $B = \{1,2,3\}$

- Is $R = \{(a,1), (b,2), (c,2)\}$ a relation from A to B?
- Is $Q = \{(1,a), (2,b)\}$ a relation from A to B?
- Is $P = \{(a,a), (b,c), (b,a)\}$ a relation from A to A?

R	u	v
0	×	×
1	×	
2		×

Example: Let $A = \{0,1,2\}$ and $B = \{u,v\}$, and $R = \{(0,u), (0,v), (1,v), (2,u)\}$. $(R \subseteq A \times B)$

$R_{div} = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\}$



R	1	2	3	4
1	×	×	×	×
2		×		×
3			×	
4				×

Number of Binary Relations

Theorem: The number of binary relations on a set A, where $|A| = n$, is 2^{n^2}.

Proof: If $|A| = n$, then the cardinality of the Cartesian product $|A \times A| = n^2$.

R is a binary relation on A if $R \subseteq A \times A$ (R is subset).

The number of subsets of a set with k elements is 2^k.

Reflexive Relation

Reflexive Relation: A relation R on a set A is called reflexive if $(a,a) \in R$ for every element $a \in A$.

$$MR_{div} = \begin{matrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}$$

Irreflexive Relation

Irreflexive Relation: A relation R on a set A is called irreflexive if $(a,a) \notin R$ for every element $a \in A$.

Symmetric Relation

$$MR = \begin{matrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{matrix}$$

Symmetric Relation: A relation R on a set A is called symmetric if $(b,a) \in R$ whenever $(a,b) \in R$ for all $a,b \in A$.

$$MR = \begin{matrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{matrix}$$

Antisymmetric Relation

Antisymmetric Relation: A relation R on a set A is called antisymmetric if $(b,a) \in R$ and $(a,b) \in R$ implies $a = b$ for all $a,b \in A$.

$$MR = \begin{matrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{matrix}$$

Transitive Relation

Transitive Relation: A relation R on a set A is called transitive if $(a,b) \in R$ and $(b,c) \in R$ implies $(a,c) \in R$ for all $a,b,c \in A$.

Combining Relations

Example: $R_1 = \{(x,y)|x < y\}$ and $R_2 = \{(x,y)|x > y\}$. What are $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 - R_2$, $R_2 - R_1$, and $R1 \oplus R_2$?

$R_1 \cup R_2 = \{(x,y)|x \neq y\}$
$R_1 \cap R_2 = \emptyset$
$R_1 - R_2 = R_1$
$R_2 - R_1 = R_2$
$R_1 \oplus R_2 = \{(x,y)|x \neq y\}$

Composite of Relations

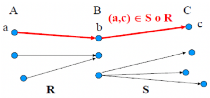
$$M_R = \begin{matrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{matrix}$$

$$M_R \odot M_S = \begin{matrix} 1 & 1 \\ 1 & 0 \end{matrix}$$

Example: Let $A = \{1,2,3\}$, $B = \{0,1,2\}$, and $C = \{a,b\}$:

- $R = \{(1,0), (1,2), (3,1), (3,2)\}$
- $S = \{(0,b), (1,a), (2,b)\}$
- $S \circ R = \{(1,b), (3,a), (3,b)\}$

$$M_S = \begin{matrix} 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{matrix}$$



Power of a Relation

Definition: Let R be a relation on A. The powers R^n, for $n = 1,2,3,\dots$, is defined inductively by

$$R^1 = R \text{ and } R^{n+1} = R^n \circ R$$

Example: Let $A = \{1,2,3,4\}$, and $R = \{(1,2), (2,3), (2,4), (3,3)\}$

- $R^1 = R$
- $R^2 = R \circ R = \{(1,3), (1,4), (2,3), (3,3)\}$
- $R^3 = R^2 \circ R = \{(1,3), (2,3), (3,3)\}$
- $R^4 = R^3 \circ R = \{(1,3), (2,3), (3,3)\}$
- $R^k =?$ for $k > 3$

Theorem: The relation R on a set A is transitive if and only if $R^n \subseteq R$ for $n = 1,2,3,\dots$

Theorem: The number of binary relations on a set A, where $|A| = n$, is 2^{n^2}.

Number of Reflexive Relations

Theorem: The number of reflexive relations on a set A with $|A| = n$ is $2^{n(n-1)}$.

Proof: A reflexive relation R on A must contain all pairs (a,a) for every $a \in A$.

All other pairs in R are of the form (a,b) with $a \neq b$, s.t. $a,b \in A$.

How many of these pairs are there?

How many subsets on $n(n-1)$ elements are there?

Reflexive Relation: A relation R on a set A is called reflexive if $(a,a) \in R$ for every element $a \in A$.

Irreflexive Relation: A relation R on a set A is called irreflexive if $(a,a) \notin R$ for every element $a \in A$.

Symmetric Relation: A relation R on a set A is called symmetric if $(b,a) \in R$ whenever $(a,b) \in R$ for all $a,b \in A$.

Antisymmetric Relation: A relation R on a set A is called antisymmetric if $(b,a) \in R$ and $(a,b) \in R$ implies $a = b$ for all $a,b \in A$. Is $R_{\neq}$ transitive? No. $(1,2),(2,1) \in R_{\neq}$ but $(1,1) \notin R_{\neq}$.

Transitive Relation: A relation R on a set A is called transitive if $(a,b) \in R$ and $(b,c) \in R$ implies $(a,c) \in R$ for all $a,b,c \in A$.

Lecture 15

n-ary Relations

Definition: An n-ary relation R on sets $A_1, \dots, A_n$, written as $R : A_1, \dots, A_n$, is a subset $R \subseteq A_1 \times \dots \times A_n$.

- The sets $A_1, \dots, A_n$ are called the domains of R.
- The degree of R is n.
- R is functional in domain A_i if it contains at most one n-tuple $(\cdots, a_i, \cdots)$ for any value a_i within domain A_i.

Relational Databases

A relational database is essentially an n-ary relation R.

A domain A_i is a primary key for the database if the relation R is functional in A_i. Student name, student ID.

Student_name	*ID_number*	*Major*	*GPA*
Ackermann	231455	Computer Science	3.88
Adams	888323	Physics	3.45
Chou	102147	Computer Science	3.49
Goodfriend	453876	Mathematics	3.45
Rao	678543	Mathematics	3.90
Stevens	786576	Psychology	2.99

the domain of major fields of study and the domain of GPAs

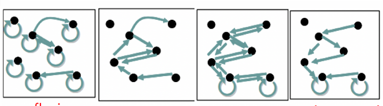
a composite key for the n-ary relation, assuming that no n-tuples are ever

Selection Operator

Let A be any n-ary domain $A = A_1 \times \dots \times A_n$, and let $C : A \to \{T,F\}$ be any condition (predicate) on elements (n-tuples) of A.

The selection operator s_C is the operator that maps any (n-ary) relation R on A to the n-ary relation of all n-tuples from R that satisfy C.

$$\forall R \subseteq A, s_C(R) = R \cap \{a \in A | s_C(a) = T\} = \{a \in R | s_C(a) = T\}$$



reflexive   irreflexive   symmetric   antisymmetric

***47.** How many relations are there on a set with n elements that are

a) symmetric? **b)** antisymmetric?
c) asymmetric? **d)** irreflexive?
e) reflexive and symmetric?
f) neither reflexive nor irreflexive?

a) $2^{n(n+1)/2}$ **b)** $2^n3^{n(n-1)/2}$
c) $3^{n(n-1)/2}$ **d)** $2^{n(n-1)}$ **e)** $2^{n(n-1)/2}$ **f)** $2^{n^2} - 2 \cdot 2^{n(n-1)}$

a) **Symmetric Relations**: For a symmetric relation on a set with n elements, each element can be related to itself and every pair (a,b) where $a \neq b$, can be included in the relation. Since (a,b) and (b,a) are considered the same in a symmetric relation, we only need to consider each pair once. Therefore, there are $n(n-1)/2$ unique pairs where $a \neq b$, plus the n possible pairs where $a = b$, giving us a total of $n(n+1)/2$ pairs. Each pair can either be in the relation or not, which gives us two choices (yes or no) for each pair. Thus, the total number of symmetric relations is $2^{n(n+1)/2}$.

b) **Antisymmetric Relations**: A relation is antisymmetric if for every (a,b) in R, (b,a) is not in R unless $a = b$. For each of the $n(n-1)/2$ pairs where $a \neq b$, you can choose to include either (a,b), (b,a), or neither, resulting in $3^{n(n-1)/2}$ possibilities.

c) **Asymmetric Relations**: A relation is asymmetric if for every (a,b) in R, (b,a) is not in R. This is a stricter form of antisymmetry because it applies even when $a = b$. The number of asymmetric relations is the same as the number of antisymmetric relations minus the number of diagonal elements, which is $3^{n(n-1)/2}$

d) **Irreflexive Relations**: A relation is irreflexive if no element is related to itself, meaning (a,a) is not in R for all elements a. For each of the n pairs (a,a), there is only one option: not to include it. For the remaining $n(n-1)$ pairs, each can either be included or not, resulting in $2^{n(n-1)}$ possibilities.

e) **Reflexive and Symmetric Relations**: A relation is both reflexive and symmetric if every element is related to itself, and for every (a,b) in R, (b,a) is also in R. Since all n reflexive pairs (a,a) must be included, there are $2^{n(n-1)/2}$ ways to include the remaining pairs.

1. 2^{n^2} represents the total number of relations on a set with n elements without any restrictions. Since a relation on a set can be represented as a matrix with $n \times n$ entries (where each entry can either be 0 or 1 representing the absence or presence of a relation), there are n^2 entries, and each entry has 2 options. Hence, 2^{n^2}.
2. $2^{n(n-1)}$ represents the number of irreflexive relations on a set with n elements. An irreflexive relation is one where no element is related to itself, hence the diagonal of the relation matrix (which has n entries) must be all zeros. The remaining $n(n-1)$ entries (off-diagonal) can be either 0 or 1, leading to $2^{n(n-1)}$ irreflexive relations.
3. $2 \cdot 2^{n(n-1)}$ is subtracted from the total number of relations to exclude both the completely reflexive and completely irreflexive relations. The completely reflexive relations, where each element is related to itself, would also count as $2^{n(n-1)}$ since we only consider the off-diagonal elements (which can be either 0 or 1). We multiply by 2 because we need to exclude both the completely reflexive and completely irreflexive sets of relations from our total.

$$A(x) = (1+x)^{m+n} = \sum_{r=0}^{m+n} a_rx^r = \sum_{r=0}^{m+n} C(m+n,r)x^r,$$
$$B(x) = (1+x)^n = \sum_{r=0}^{n} b_rx^r = \sum_{r=0}^{n} C(n,r)x^r,$$
$$C(x) = (1+x)^m = \sum_{r=0}^{m} c_rx^r = \sum_{r=0}^{m} C(m,r)x^r.$$

$$A(x) = B(x)C(x) = \sum_{r=0}^{m+n}\left(\sum_{k=0}^{r} b_kc_{r-k}\right)x^r = \sum_{r=0}^{m+n}\sum_{k=0}^{r} C(m,r-k)C(n,k)x^r.$$

Therefore, we must have $C(m+n,r) = \sum_{k=0}^{r} C(m,r-k)C(n,k)$ for all $r = 0, 1, \dots, m+n$.

Polynomial Multiplication

$A(x) = 1 + x + 2x^2$
$B(x) = 2 + x - x^2$
$C(x) = A(x)B(x) = (1 + x + 2x^2)(2 + x - x^2) = 2 + 3x + 4x^2 + x^3 - 2x^4$

$$C(x) = A(x)B(x) = \left(\sum_{p=0}^{n-1} a_px^p\right)\left(\sum_{q=0}^{m-1} b_qx^q\right) = \sum_{k=0}^{n+m-2}\left(\sum_{p=0}^{n} a_pb_{k-p}\right)x^k = \sum_{k=0}^{n+m-2} c_kx^k$$

Convolution

$$\Longrightarrow \quad c_k = \sum_{p=0}^{n} a_pb_{k-p} = \sum_{p=0}^{n-1}\sum_{q=0}^{m-1}[p+q=k] \cdot a_pb_q$$

$$[P] = \begin{cases} 1 & P \text{ is true} \\ 0 & P \text{ is false} \end{cases}$$