프로그래머, 수학으로 생각하라

유키히로시 지음 | 안동현 옮김 | 프리렉

기수법

- 2진법 → 8진법 → 16진법
- 위치값 기수법 Positional Notation

$a_{3} \times N^3 + a_{2} \times N^2 + a_{1} \times N^1 + a_{0} \times N^0$

- 지수법칙

$10^0 ?$
$10^-1 ?$
$N^a \times N^b = N^{a+b}$

- 0의 역할; 자리확보, 패턴을 만들어 규칙을 간단하게 하기

$a_{n} \times \ m^n + a_{n-1} \times m^{n-1} + a_{n-2} \times m^{n-2} + \ldots + a_{2} \times m^2 + a_{1} \times m^1 + a_{0} \times m^0$

논리

애매함을 없애는 도구; **망라(網羅)** 적이고 **배타적**인 분할

명제; 참, 거짓

누락은 없는가, 중복은 없는가

부정; A가 아님

~A (Not A), ~~A == A

Venn Diagram, 진리표

논리곱; A 이고 B

$A \wedge B (A and B)$

논리합; A 또는 B

$A \vee B (A or B)$

배타적 논리합; A 또는 B (그러나 둘 다는 아님)

$A \oplus B$

등치; A와 B는 같다

A = B

배타적 논리합의 부정 ; $(\sim(A \oplus B)) = (A = B)$

조건 명제; A라면 B A⇒B

- 드 모르간의 법칙 de Morgan's Law;

$(\sim{A})\vee(\sim{B})=\sim(A\wedge{B})$
$(\sim{A})\wedge(\sim{B})=\sim(A\vee{B})$

쌍대성

true↔false
A↔~A
$\wedge \leftrightarrow \vee$

- 카르노 맵 Karnaugh Map); 모든 명제의 참, 거짓 조합을 2차원으로 나타낸 그림

- 정의되지 않음을 포함한 논리; true, false, undefined
- 조건 논리곱(&&) Conditional And, Short-circuit Logical And; A라는 조건에 따라 B를 조사할 것인지 안 할 것인지를 판단하는 것
- 조건 논리합(||)
- 3값 논리의 부정(!)
- 3값 논리에서 드 모르간 법칙

(!A) || (!B) = ! (A && B)
(!A) && (!B) = ! (A || B)

주기성과 그룹 나누기

나머지는 그룹 나누기. 패리티Parity; 통신에서 에러를 확인할 때 사용하는 중요한 개념
나머지의 주기성

- 한붓그리기; 오일러 (Leonard Euler, 1707~1783)는 쾨니히스베르크의 다리 건너기 문제 → 그래프 이론

'한붓 그리기 성공' ⇒ '모든 정점은 짝수점 또는 홀수점이 2개'

수학적 귀납법

Mathematical Induction, 정수에 관한 주장을 0 이상의 모든 정수(0,1,2,3,…)에 대해 증명할 때 이용하는 방법, 2단계로 증명을 수행

단계1(기저Base), 'P(0)이 성립함'을 증명한다.
단계2(귀납Induction), 0 이상의 어떤 정수 k를 선택해도 'P(k)가 성립한다면 P(k+1)도 성립함'을 증명한다.

- 가우스

$0 + 1 + 2 + 3 + \dots + n = \frac{(n + 1)\times{n}}{2}$

순열과 조합

- 덧셈법칙

$|A\cup{B}|=|A|+|B|$

포함과 배제의 원리; The Principle of Inclusion and Exclusion

$|A\cup{B}|=|A|+|B|-|A\cap{B}|$

- 곱셈법칙

$|A\times{B}|=|A|\times|B|$

- 치환Substitution; n개의 무엇가를 순서를 생각하며 나열하는 것, 계승Factorial
- 순열Permutation; n개의 무언가 중 일부만을 선택하여 나열

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

수형도Tree Diagram

- 조합Combination; 순서를 생각하지 않는 것

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

$_{n}C_{k}=\frac{_{n}P_{k}}{_{k}P_{k}}=\frac{(n-0)\times(n-1)\times(n-2)\times\dots\times(n-(k-1))}{(k-0)\times(k-1)\times(k-2)\times\dots\times(k-(k-1))}$

재귀

- 하노이의 탑; 1883년 뤼카(Edouard Lucas, 1842~1891)

닫힌식Closed-form Expression 또는 일반항 $H(n)=2^n-1$

[재귀를 사용한 표현] 'n 하노이'를 'n-1 하노이'를 이용하여 푸는 순서를 발견해낸다. [점화식] 'n 하노이'의 횟수를 'n-1 하노이'의 횟수를 이용하여 표현한다.

재귀Recursion와 귀납Induction은 모두 “큰 문제를 같은 형태의 작은 문제로 만든다.”

재귀적Recursive, 귀납적Inductive

- 피보나치 수열; Leonardo Fibonacci, 1170~1250

0,1,1,2,3,5,8,13,21,34,55,89,…

- 파스칼의 삼각형

시어핀스키 개스킨(Sierpinski Gasket, Sierpinski Triangle)

프랙털 도형

지수적 폭발

Exponential Explosion; 수가 급격하게 증가하는 것. 지수적 증가, 지수함수적 증가, 조합론적 폭발

- 이진검색; 지수적 폭발을 이용한 검색
- 로그; 지수적 폭발을 다루는 도구 Logarithm, 1614년 스코틀랜드의 수학자 네이피어(John Napier, 1550~1617)
- 암호; 지수적 폭발로 비밀을 지킴

무작위 공격(Brute-force Attack)

계산할 수 없는 문제

- 귀류법; 증명하고자 하는 것의 부정을 가정하면 모순이 생긴다. 배리법
  1. 우선 '증명하고자 하는 명제의 부정'이 성립한다고 가정
  2. 그 가정을 기본으로 증명을 진행하여 모순을 유도

소수Prime Number; 1과 자기 자신의 수만으로 나누어떨어지는 2 이상의 수

- countable; 집합의 요수 개수가 한정되거나 집합의 모든 요소를 1 이상의 정수와 1대 1로 대응할 수 있다.
- 대각선 논법
- 계산할 수 없는 문제; 프로그램으로 푸는 것이 원리적으로 불가능한 문제

페르마의 마지막정리; $x^n+y^n=z^n$
골드바흐의 추측Goldbach's conjecture; 4 이상의 모든 짝수는 소수2개의 합으로 나타낼 수 있다

정리

- '0'은 규칙을 간단하게 만든다
- '논리'는 둘로 나누기
- '나머지'로 그룹화
- '수학적 귀납법'은 2단계로 무한에 도전한다
- '순열과 조합'에서는 대상의 성질을 파악하는 것이 중요하다
- '재귀'는 자신 안에서 자신을 발견하는 것
- '지수적 폭발'이란
- '계산할 수 없는 문제'는 원리적인 제한을 나타낸다