Chapter 1.2 Axiom of Probability

Randomized 알고리즘을 분석하기위해서, Probability space 정의가 필요하다.

Definition 1.1 Probability space 는 다음 3 가지 컴포넌트를 갖는다.

1. probability space 에서 랜덤 프로세스 모델에 의해 나올 수 있는 결과값의 집합을, sample space Ω 라고 한다.
2. family set $\mathrm{F} \in \Omega$ 는 발생 가능한 이벤트들을 의미한다. (둘 다 집합이지만, 기호를 찾지 못하여, 원소 기호를 사용)
3. a probability function $\Pr \mathrm{F} \rightarrow \mathrm{R}$ 은 Deifinition 1.2 를 만족한다.

Definition 1.2 어떤 확률함수 $\Pr \mathrm{F} \rightarrow \mathrm{R}$도 다음과 같은 조건을 만족한다.

1. 모든 이벤트 E 에 대해서, $0 \leq \Pr(E) \leq 1$
2. Pr (Ω) = 1
3. 서로 관련이 없는 (mutually disjoint) 각각의 원소들의 유한의 또는 셀 수 있는(countable) 무한한 수열에 대하여,

$$\Pr\left(\bigcup_{i \geq 1} E_i\right) = \sum_{i \geq 1} \Pr\left(E_i\right)$$

Verifying Polynomial Identities 문제에서 r 을 선택하는 것을 event 로 볼 수 있다.
r 은 숫자 {1...100d} 사이에서 uniformly 하게 선택하기 때문에 각각의 숫자가 선택될 확률은 $\frac{1}{100d}$ 이다.

이 전 장에서 H(x) = F(x) – G(x)로 정의하였고,
H(r) = 0 이지만, F(x) ≠ G(x)인 경우에 알고리즘이 실패한다고 하였다.

이 때, H(x)는 최고차항이 d 인 다항식이므로 H(x)의 해는 최대 d 개 있다.
그러므로, 이벤트 E 를 알고리즘이 실패할 경우라고 하면,

Pr(algorithm fail) $\leq \frac{d}{100d} = \frac{1}{100}$

즉, 알고리즘이 잘 못된 결과를 낼 확률은 1 / 100 보다 작다.

알고리즘의 성능을 개선하는 2 가지 방법이 있다.

1. 숫자의 범위를 넓힌다.

{1...100d}가 아닌 {1...1000d} 사이에서 숫자를 선택한다.

그러면 알고리즘이 잘 못된 결과를 낼 확률은 1/1000 보다 작다.

하지만, 숫자의 범위가 커지면서, F(r), G(r) 연산에 정확성이 떨어진다.

2. 여러 번 수행한다.

알고리즘 한 번 수행할 때 잘 못된 결과를 낼 확률이 1/100 이다.

따라서 r 을 k 번 선택했을 때, k 번 모두 잘 못된 결과를 낼 확률은 $(\frac{1}{100})^k$ 이다.