

연습문제

1. 응용 프로그램 수준에서 알고리즘이 필요한 예와 이용된 알고리즘의 기능

웹 브라우저 URL에 쓰이는 HTTPS는 암호화 알고리즘을 사용한다.

기존에 쓰이던 HTTP는 보안상 문제가 많아서 클라이언트에서 서버로 리소스를 보낼 때 리소스를 암호화하게 된것이 HTTPS인데, 이 때 SSL(Secure Socket Layer) 알고리즘이 사용된다.

SSL 알고리즘은 대칭키 알고리즘, 디지털 서명 알고리즘, 해시함수 알고리즘, MAC 알고리즘 등이 절차에 따라 사용되며 통신한다.

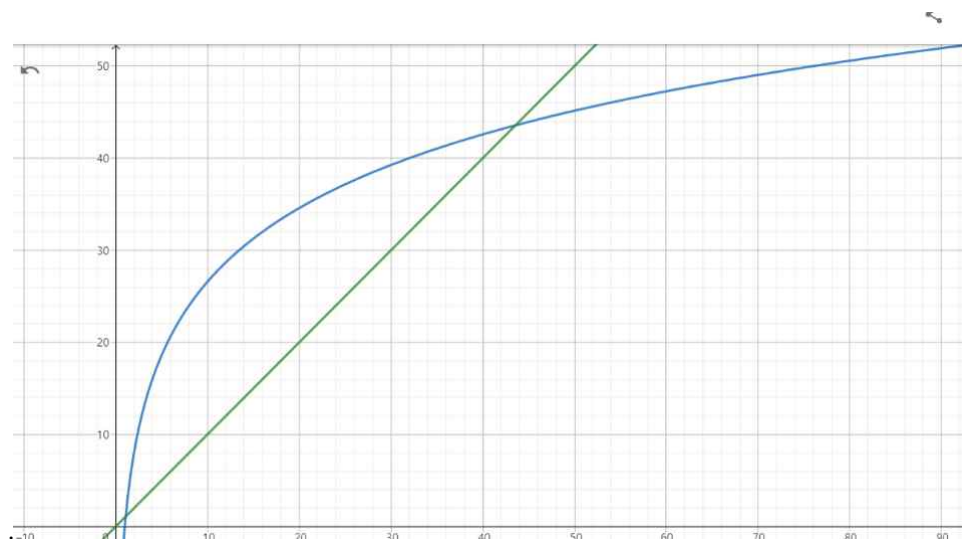
2. 동일한 기계에서 삽입 정렬과 병합 정렬의 구현 결과를 비교한다고 가정하자. n 개의 입력에 대해 삽입 정렬은 $8n^2$, 병합정렬은 $64n\log n$ 번을 계산하고 각각 종료한다. n 값이 얼마일 때 삽입 정렬이 병합정렬보다 빠를까?

우선 아마도 n 이 작을수록 삽입 정렬이 더 빠르고 n 이 클수록 병합 정렬이 빠를 것이다.

병합 정렬보다 삽입 정렬이 빠르게 되는 n 의 최댓값을 찾으려면

$8n^2 < 64n\log n$ 을 만족해야 하는데 양쪽을 $8n$ 으로 나눠주면

$n < 8\log n$ 이고 이 때 n 의 최댓값을 구하기 위해 <https://www.geogebra.org/graphing> 사이트를 써서 그래프를 그려보았다.



위 그래프에서 초록색 그래프가 삽입 정렬이고 파란 그래프가 병합 정렬인데, 두개의 교점의 x 좌표값은 약 1과 43정도이다. 따라서 1번에서 43번까지의 입력에서는 삽입 정렬이 병합 정렬보다 더 빠르고

44번 이후부터는 병합 정렬이 더 빠르다고 할 수 있다.

3. 동일한 기계에서 수행시간이 $100n^2$ 인 알고리즘이 수행시간이 2^n 인 알고리즘보다 빨라지는 n 의 최솟값은 얼마인가?

이것도 2번과 똑같은 방법으로 풀어보면

$100n^2 < 2^n$ 을 만족하면 되는데, 그래프로 그려보았는데 교점을 확인하기엔 교점의 y 좌표값이 너무 커져서 보기가 불편했다.

그래서 wolframalpha에 $100n^2 < 2^n$ 를 검색했더니 Solution은 무슨 뜻인지 잘 모르겠지만 그래프를 보면 n 이 15이상일때 부등식을 만족한다고 결과가 나왔다. 따라서 n 의 최솟값은 15이다.

종합 문제

1. 수행시간의 비교

$f(n)$ 함수가 t 시간에 풀 수 있는 문제의 최대 크기 n 을 구하라.

이 때 $f(n) = n$ 이면 하나당 100만분의 1초씩 걸린다고 가정한다. 즉 1초에 100만번 수행할 수 있다.

한시간이면 $3600 * 100$ 만번 수행할 수 있다.

	1초	1분	1시간	1일	1월	1년	1세기
$\lg n$	2^{10^6}	$2^{6 \times 10^7}$	$2^{3.6 \times 10^9}$	$2^{8.64 \times 10^{10}}$	$2^{2.59 \times 10^{12}}$	$2^{3.15 \times 10^{13}}$	$2^{3.15 \times 10^{15}}$
\sqrt{n}	10^{12}	3.6×10^{15}	1.3×10^{19}	7.46×10^{21}	6.72×10^{24}	9.95×10^{26}	9.95×10^{30}
n	10^6	6×10^7	3.6×10^9	8.64×10^{10}	2.59×10^{12}	3.15×10^{13}	3.15×10^{15}
$n \lg n$	6.24×10^4	2.8×10^6	1.33×10^8	2.76×10^9	7.19×10^{10}	7.98×10^{11}	6.86×10^{13}
n^2	1000	7745	60000	293938	1609968	5615692	56156922
n^3	100	391	1532	4420	13736	31593	146645
2^n	19	25	31	36	41	44	51
$n!$	9	11	12	13	15	16	17