Subject:
Date

## الگوریتم توان رسانی

۱. expression = a  این الگوریتم برای محاسبه‌ی $x^K$ ~~6~~ K را به مبنای دودویی می‌برد. فرض کنیم $K=(abc)_2$ (این فرض تنها برای توضیح نحوه‌ی عملکرد الگوریتم گرفته شده است.) حال می‌دانیم:

$$x^K = x^{(abc)_2} = x^{c\times2^0+b\times2^1+a\times2^2} = x^{c\times2^0} x^{b\times2^1} \times x^{a\times2^2}$$

الگوریتم تبدیل مبنای K از دهدهی به دودویی را با تقسیم مکرر i بر ۲ (if i is odd) و سپس جایگزین کردن i با خارج قسمت تقسیم i بر ۲ ($i \leftarrow \lfloor i/2 \rfloor$) انجام می‌دهد. و هر بار در صورتی که رقم عدد مورد نظر در مبنای ۲، برابر با ۱ باشد، x به توان ۲ به توان جایگاه آن رقم را در a ضرب می‌کند ($a \leftarrow a \times y$). در صورتی که رقم عدد مورد نظر در مبنای ۲، برابر با ۰ باشد چون $\forall x, x \neq 0$ $x^0 = 1$ و $0 \times \alpha = 0$ نیازی به محاسبه‌ی x به توان ۲ به توان جایگاه آن رقم ضرب در ۰ نیست.

۲. $T(n) \in \theta(\log_2 n)$  با توجه به این که while i ... $i \leftarrow \lfloor i/2 \rfloor$ با تقسیم متوالی i بر ۲ (مفهوم وارون تابع نمایی با ضرب متوالی در ۲) به تعداد $\lg n$ بار اجرا می‌شود. و تمامی ضرب ها و تقسیم ها نیز $O(1)$ هستند.

۳. در P امین باری که حلقه اجرا می‌شود، x به توان P رقم سمت راست عدد دودویی معادل توان K محاسبه شده است. (فرض استقرا) پایه‌ی استقرا به ازای K=1 نیز با دنبال کردن کد بدیهی است. حال در P+1 امین بار که حلقه اجرا می‌شود i برابر با P+1 امین رقم عدد دودویی معادل توان K خواهد بود که اگر برابر با ۱ باشد، a برابر با $a\,x\,y$ (که y برابر با x به توان P+1 است) می‌شود و a برابر با x به توان P+1 رقم سمت راست عدد دودویی معادل توان K خواهد شد.