

КРМРА
Останин Андрей

№ 2.

Нукас $T(n)$ — спошве броеи

пайот на пасене греша n .

На вакоите ставе равноделото
бюджета съгласно иуб. Тога:

$$\begin{aligned} T(n) &= \frac{1}{n} \sum_{k=3}^n (T(k-s) + T(n-k)) + O(n) = \\ &= \frac{2}{n} \sum_{k=3}^n T(k-s) + O(n) \end{aligned}$$

Покалено, че $O(n \log n)$ — пълната
реализация:

$$\begin{aligned} T(n) &\geq \frac{2}{n} \sum_{k=1}^n O(k \log k) + O(n) \leq \\ &\leq \frac{2}{n} \sum_{k=1}^n O(k \log n) + O(n) = \end{aligned}$$

$$\Rightarrow \frac{2}{n} O(n^2 \log n) + O(n) = \underline{\underline{O(n \log n)}}$$

Още: $\underline{\underline{O(n \log n)}}$

№2.

(i) — пер. задача на к. балансиров.

(ii) нужно обновить изображение p -го в
 $\leq nd^{2r}$.

Dae-bo:

k_i — число балансов
не параллельных i
и не копий.

• • •

• k_1

•

$k_0 = s$

$$\frac{d \cdot (d-1) \cdot (d-2) \cdots (d-k_1+s)}{k_1!} \leftarrow \text{исходное} \\ \leftarrow \text{использовано}$$

$$\frac{dk_1 \cdot (dk_1-s) \cdots (dk_1-k_2+s)}{k_2!}$$

$$n \prod_{i=1}^{r-1} \left(\frac{dk_{i+1} \cdot (dk_{i+1}-1) \cdot (dk_{i+1}-2) \cdots (dk_{i+1}-k_i+s)}{k_i!} \right) =$$

$$= nd^{r-1} \prod_{i=1}^{r-1} \left(k_{i+1} \left(k_{i+1} - \frac{1}{d} \right) \left(k_{i+1} - \frac{2}{d} \right) \cdots \left(k_{i+1} - \frac{k_i}{d} + \frac{s}{d} \right) \right) =$$

$$= nd^{r-1} \prod_{i=0}^{r-2} \underbrace{\frac{k_i \left(k_i - \frac{1}{d} \right) \left(k_i - \frac{2}{d} \right) \cdots \left(k_i - \frac{k_{i+1}}{d} + \frac{s}{d} \right)}{k_i!}}_{k_i!} \cdot \frac{s}{k_{r-1}!} <$$

$$\left(k_i - \frac{b}{d} \right) d > k_i - s \Rightarrow < d^{k_i+s}$$

$$< n d \prod_{i=0}^{r-2} d^{k_{i+1}} = n d^{2(r-2)} < \underline{nd^{2r}}$$

$\sqrt{3}$.

$$P = \frac{1}{2d^2}, P = \frac{l}{2d^2}$$

$$(1) P(\text{не все } S \in V, |S| > \log n) = \frac{1}{n^2}$$

Dok-бд: Число деревьев не превышает $\log n$.
 $\log n \leq nd^{2\log n}$. Если более d в
 деревьях \rightarrow есть дерево с $\log n$ листьями.

$$P(\text{есть дерево с } \log n \text{ листьями}) = \sum P(\text{дерево с } \log n)$$

$$P(\text{дерево с } \log n) = \left(\frac{1}{2d^2}\right)^{\log n} = \frac{d^{-2\log n}}{2}$$

$$\Rightarrow \text{найденное дерево } \frac{nd^{2\log n} \cdot d^{-2\log n}}{2} = \frac{n}{2} \dots$$

NH.

Нука \leftarrow минимизировать количество генов. Тогда, если это количество генов нечетное, то вектора приобретут 0/1, то можно достичь приближения

$$\frac{2^k - 1}{2} \cdot E\left(\sum_{i=1}^n I(\text{chromosome}_i)\right)$$

$$= \sum_{i=1}^n P(I_i) \geq \sum_{i=1}^n \frac{2^k - 1}{2^k} = \frac{2^k - 1}{2^k} n$$

Нука cut-меню формируется след.

Тогда $E(\text{cut}) = E(\text{cut} | x_i = 1) + E(\text{cut} | x_i = 0)$

Хотя для I мы $\geq E(\text{cut}) \rightarrow$ бордюрах b_1 соответствующее. Как however E ? Нука I -меню
меню моногенов в среде. Тогда,
если b выше одноко в н

Задача. (Широнов, то $b_{\text{ep}} - b_0 = 0$)

рассмотрим $\frac{f}{2^n}$. Можно, например, подсчитывать
это же $\frac{f}{2^{n-k}}$ — бесконечный ряд чисел, где
на концах имеется бесконечное количество
значений с шагом b , то есть эти значения
будут иметь периодичность.

$$E(\text{ext} | b_1, \dots, b_{j-1}, \dots) = E(\text{ext} | \dots, b_j = 1) +$$

$$\frac{-E(\text{ext} | \dots, b_j = 0)}{2}$$

Т.е.

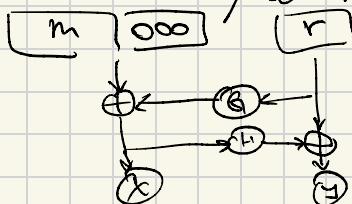
$m^e < n \Rightarrow m^e = m^e \bmod n$, можно брать вместо m :

$c := m^e$, $m = \sqrt[e]{c} \rightarrow$ удаляемость, можно

удалить коэффициент $\frac{1}{e}$ при переводе в двоичную систему заново (если e не делится на n).
Пример:

OAEF — Optimal Asymmetric Encryption Padding.

Несколько замечаний:



G, H — хеш-функции.
 P — случайное число.
Использование криптосистемы.

$X \cdot Y$ - замкнутое соединение (-conct)
Тогда $(X \cdot Y)^e$ над n - замкнутое
соединение.
Знач $X \sqcup Y, H \sqcup G$ можно рассмотреть
какое соединение.

Таким образом, можно включить достаточно
большого групп соединений в распределен-
ные ячейки.

№ 6.

3) Шифр-RSA, крипто-Энг-Гарант

Недостатки:

- Энг-Гарант требует много времени
на проверку подписи.

2) Шифр, крипто-RSA, но с различным назначением

Недостатки:

- В случае отказа на RSA все открытые
ключи становятся недействительными

3) Старт, миграция - бор
(стартует RSA-OAEP и RSA-PSS)

Начало:

- В случае если на RSA был введен соответствующий
- Максимум возможных ошибок уменьшается до OAEP

Таким образом, лучше всего использовать
рекомендованную, так как она является
(но не опровергнута и не доказана) более простой.
Максимальное количество ошибок