The proof of Lemma 3.

Proof. We prove the statement by induction over k. The initial step $k=0$. Since α_0 is constant then

$$\mathbf{P}(\alpha_0 \geq t) = \begin{cases} 0 & \text{if } \alpha_0 < t, \\ 1 & \text{if } \alpha_0 \geq t. \end{cases}$$

On the other hand, in any case

$$\alpha_0^{0-\log\log(\frac{1}{t})+\log\log(\frac{1}{\alpha_0})} \geq 0$$

because $\alpha_0 > 0$ and if $t \geq \alpha_0$ then $-\log\log(\frac{1}{t}) + \log\log(\frac{1}{\alpha_0}) \leq 0$ and hence

$$\alpha_0^{0-\log\log(\frac{1}{t})+\log\log(\frac{1}{\alpha_0})} \geq 1.$$

Hence the statement is true.

Induction step. Let $k \geq 0$ be a natural number and assume that the statement holds for k and we prove it for $k+1$. For simplicity, let us denote $c = k - \log\log(\frac{1}{t})$. Then we have to prove

$$\mathbf{P}(\alpha_{k+1} \geq t) \leq \alpha_0^{c+1+\log\log(\frac{1}{\alpha_0})}.$$

If $c + 1 + \log\log(\frac{1}{\alpha_0}) \leq 0$ then the rigth side is at least 1 and the statement holds. Thus we can restrict ourselves on the case $c+1+\log\log(\frac{1}{\alpha_0}) > 0$. The idea of the proof is based on the following fact which enable us to fix a value α_1. For $a \in < 0, \alpha_0 >$ let us define $g(a) = \mathbf{P}(\alpha_{k+1} \geq t | \alpha_1 = a)$. Then

$$\mathbf{P}(\alpha_{k+1} \geq t) = \sum_{a \in <0,\alpha_0>} \mathbf{P}(\alpha_{k+1} \geq t | \alpha_1 = a)\mathbf{P}(\alpha_1 = a) = \mathbf{E}(g).$$

For $0 < x < 1$, let $f_0(x) = x^{c+\log\log(\frac{1}{x})}$ and $f(x) = \min\{1, f_0(x)\}$, $f(0) = 1$. Observe that if β_i for $i = 1, 2, \ldots, k$ are random variables and $\beta_0 = a \in < 0, \alpha_0 >$ is constant such that $0 \leq \beta_i \leq \beta_{i-1}$ and $\mathbf{E}(\beta_i | \beta_{i-1}, \beta_{i-2}, \ldots, \beta_0) = \beta_{i-1}^2$ for all $i = 1, 2, \ldots, k$ then $\mathbf{P}(\beta_k \geq t) = g(a)$ and, by induction hypothesis, $g(a) \leq f(a)$ for all $a \in < 0, \alpha_0 >$. Observe that $g(0) \leq f(0) = 1$ because $t \geq 0$.

Next we investigate a behaviour of the function $\frac{f_0(x)}{x}$ on the interval (0,1). The derivation of the function $\frac{f_0(x)}{x}$ on the interval (0,1) is

$$(\frac{f_0(x)}{x})' = (c - 1 + \log\log(\frac{1}{x}) + \log e)\frac{f_0(x)}{x^2}.$$

Hence if $x < 2^{-2^{-c+1-\log e}}$ then $\frac{f_0(x)}{x}$ is increasing in x and if $x > 2^{-2^{-c+1-\log e}}$ then $\frac{f_0(x)}{x}$ is decreasing in x. Let us define $x_1 = 2^{-2^{-c}}$. Since $-c > -c + 1 - \log e$ we conclude that $\frac{f_0(x)}{x}$ is increasing in x_1. For every $x \in < x_1, 1)$ we have $f(x) = 1$ because $f_0(x_1) = x_1^{c+\log\log(2^{2^{-c}})} = x_2^{c-c} = 1$ and f_0 is an increasing function.

The proof is divided into two cases. Set $x_2 = 2^{-2^{-c-1}}$ then $x_1 = x_2^2$. Since $-2 < -\log e$ we obtain that $-c-1 < -c+1-\log e$ and hence $x_2 = 2^{-2^{-c-1}} > 2^{-2^{-c+1-\log e}}$.

First assume that $\alpha_0 \leq x_2$. We prove

$$f(x) = \frac{f_0(\alpha_0)x}{\alpha_0}$$

for all $x \in (0, \alpha_0 >$. If $\alpha_0 \leq 2^{-2^{-c+1-\log e}}$ then $\frac{f_0(x)}{x} \leq \frac{f_0(\alpha_0)}{\alpha_0}$ for all $x \in (0, \alpha_0 >$ because $\frac{f_0(x)}{x}$ is an increasing in the interval $(0, \alpha_0 >$. Hence

$$f(x) = \frac{f(x)x}{x} \leq \frac{f_0(x)x}{x} \leq \frac{f_0(\alpha_0)x}{\alpha_0}$$

because $f(x) \leq f_0(x)$ for all $x \in (0,1)$.

If $2^{-2^{-c+1-\log e}} < \alpha_0 < x_2$ then for $x \in (0, x_1 >$ we have

$$\frac{f(x)}{x} \leq \frac{f(x_1)}{x_1} = \frac{1}{x_1}$$

and thus $f(x) = \frac{f(x)}{x}x \leq \frac{x}{x_1}$. If $x \in < x_1, \alpha_0 >$ then $f(x) = 1 = \frac{x}{x} \leq \frac{x}{x_1}$. Since

$$\begin{aligned}\frac{f_0(x_2)}{x_2} =& \frac{(2^{-2^{-c-1}})^{c+\log(-\log(2^{-2^{-c-1}}))}}{2^{-2^{-c-1}}} = \\ & \frac{(2^{-2^{-c-1}})^{c+\log(2^{-c-1})}}{2^{-2^{-c-1}}} = \\ & \frac{(2^{-2^{-c-1}})^{-1}}{2^{-2^{-c-1}}} = \frac{1}{x_2^2} = \frac{1}{x_1}\end{aligned}$$

we infer that $f(x) \leq \frac{x}{x_1} = \frac{f_0(x_2)x}{x_2} \leq \frac{f_0(\alpha_0)x}{\alpha_0}$, because $\frac{f_0(x)}{x}$ is decreasing on the interval $< 2^{-2^{-c+1-\log e}}, 1)$.

Hence we obtain that

$$\begin{aligned}\mathbf{P}(\alpha_{k+1} \geq t) \leq& \mathbf{E}(g) \leq \mathbf{E}(f|x \leq \alpha_0) \leq \mathbf{E}(\frac{f_0(\alpha_0)}{\alpha_0}x|x \leq \alpha_0) = \\ & \frac{f_0(\alpha_0)}{\alpha_0}\mathbf{E}(\alpha_1|\alpha_0) = \alpha_0 f_0(\alpha_0) = \alpha_0^{c+1+\log\log(\frac{1}{\alpha_0})}\end{aligned}$$

here the expected value of g and of f are computed through α_1 and, by the the assumption, $\mathbf{E}(\alpha_1|\alpha_0) = \alpha_0^2$. Thus the statement is proved.

Secondly assume that $\alpha_0 > x_2$. We prove that then $c+1+\log\log(\frac{1}{\alpha_0}) < 0$ and the proof follows. Indeed $c+1+\log\log(\frac{1}{\alpha_0}) < c+1+\log\log(\frac{1}{x_2}) = c+1+\log(-\log(2^{-2^{-c-1}})) = c+1+\log(2^{-c-1}) = c+1-c-1 = 0$. $\square$

Let $u \geq t$. We describe as we can random uniformly choose a surjective linear mapping $T : Z_2^u \longrightarrow Z_2^t$. Choose a base $\{v_1, v_2, \ldots, v_t\}$ of Z_2^t. Observe that if $T : Z_2^u \longrightarrow Z_2^t$ is a surjective linear mapping then there exist a base $\{w_1, w_2, \ldots, w_u\}$ of Z_2^u and a set $A \subseteq \{w_1, w_2, \ldots, w_u\}$ with $|A| = u - t$ such that $T(A) = \vec{0}$ and $T(\{w_1, w_2, \ldots, w_u\} \setminus A) = \{v_1, v_2, \ldots, v_t\}$. Conversely if $T : Z_2^u \longrightarrow Z_2^t$ is a linear mapping such that there exist a base $\{w_1, w_2, \ldots, w_u\}$ of Z_2^u and a set $A \subseteq \{w_1, w_2, \ldots, w_u\}$ with $|A| = u - t$, $T(A) = \vec{0}$ and $T(\{w_1, w_2, \ldots, w_u\} \setminus A) = \{v_1, v_2, \ldots, v_t\}$ then T is surjective. Because a linear mapping is uniquelly determined by the image of a base we can proceed as follows: we fix a base $\{v_1, v_2, \ldots, v_t\}$ of Z_2^t, then uniformly choose a random base $\{w_1, w_2, \ldots, w_u\}$ of Z_2^u and a set $A \subseteq \{w_1, w_2, \ldots, w_u\}$ with $|A| = u - t$ and finally we uniformly choose a random permutation $\tau : \{w_1, w_2, \ldots, w_u\} \longrightarrow \{v_1, v_2, \ldots, v_t\}$. Then define

$$T(w_i) = \begin{cases} \vec{0} & \text{if } w_i \in A, \\ \tau(w_i) & \text{if } w_i \notin A. \end{cases}$$

Then a linear extension of T is a random uniformly choosen surjective linear mapping.