Supplementary material

The following proposition is needed for the proof of Theorem 3.

Proposition 2 (Formula of the Geometric Series) *Let $(s)_{i\in\mathbb{N}_0}$ be a sequence of real numbers satisfying $s_0 = 0$ and $s_{i+1} = qs_i + p$ [or $s_{i+1} \leq qs_i + p$] for some $p, q > 0$. Then it holds:*

$$s_i = p\frac{1-q^i}{1-q}\ , \ \ [\text{or } \ s_i \leq p\frac{1-q^i}{1-q}], \tag{14}$$

respectively.

Proof.

(a) We prove part (a) of the theorem by induction over $i \in \mathbb{N}_0$, the case of $i = 0$ being obvious.

In the inductive step we show that if Eq. (14) holds for an arbitrary fixed i it also holds for $i + 1$:

$$\begin{aligned} s_{i+1} &= qs_i + p = q\left(p\frac{1-q^i}{1-q}\right) + p = p\left(q\frac{1-q^i}{1-q} + 1\right) \\ &= p\left(\frac{q-q^{i+1}+1-q}{1-q}\right) = p\left(\frac{1-q^{i+1}}{1-q}\right)\ . \end{aligned}$$

(b) The proof of part (b) is analogous. □

Proof of Theorem 3.

Proof.

(a) Inserting the optimal attack strategy of Prop. 1 into Eq. (11) of Ax. 1, we have:

$$\mathbf{X}_{i+1} = \mathbf{X}_i + \frac{1}{n}\left(B_i\left(\mathbf{X}_i + \mathbf{a}\right) + (1-B_i)\boldsymbol{\epsilon}_i - \mathbf{X}_i\right)\ ,$$

which can be rewritten as:

$$\mathbf{X}_{i+1} = \left(1 - \frac{1-B_i}{n}\right)\mathbf{X}_i + \frac{B_i}{n}\mathbf{a} + \frac{(1-B_i)}{n}\boldsymbol{\epsilon}_i\ , \tag{15}$$

Taking the expectation on the latter equation, and noting that by Axiom 1 $E(\boldsymbol{\epsilon}) = 0$ and $E(B_i) = \nu$ holds, we have

$$\mathbf{E}\left(\mathbf{X}_{i+1}\right) = \left(1 - \frac{1-\nu}{n}\right)E(\mathbf{X}_i) + \frac{\nu}{n}\mathbf{a}\ .$$

Since by Eq. (12) we have $E(D_i) = E(\mathbf{X}_i)\cdot\mathbf{a}$ and $\|\mathbf{a}\| = R = 1$, we conclude

$$E(D_{i+1}) = \left(1 - \frac{1-\nu}{n}\right)E(D_i) + \frac{\nu}{n}\ .$$

Now statement (a) follows by the formula of the geometric series, i.e. by Prop. 2, from the latter recursive Equation.

(b) Multiplying both sides of Eq.(15) with $\mathbf{a}$ and substituting $D_i = \mathbf{X}_i\cdot\mathbf{a}$ results in

$$D_{i+1} = \left(1 - \frac{1-B_i}{n}\right)D_i + \frac{B_i}{n} + \frac{(1-B_i)}{n}\boldsymbol{\epsilon}_i\cdot\mathbf{a}\ .$$

Inserting $B_i^2 = B_i$ and $B_i(1-B_i) = 0$, which holds because B_i is Bernoulli, into the latter equation, we have:

$$\begin{aligned} D_{i+1}^2 &= \left(1 - 2\frac{1-B_i}{n} + \frac{1-B_i}{n^2}\right)D_i^2 + \frac{B_i}{n^2} + \frac{(1-B_i)}{n^2}\|\boldsymbol{\epsilon}_i\cdot\mathbf{a}\|^2 \\ &\quad + 2\frac{B_i}{n}D_i + 2(1-B_i)(1-\frac{1}{n})D_i\boldsymbol{\epsilon}_i\cdot\mathbf{a}\ . \end{aligned}$$

Taking the expectation on the latter equation, and noting that by Axiom 1 $\boldsymbol{\epsilon}_i$ and $\mathbf{D}_i$ are independent, we have:

$$\begin{aligned} E\left(D_{i+1}^2\right) &= \left(1 - \frac{1-\nu}{n}\left(2 - \frac{1}{n}\right)\right)E\left(D_i^2\right) + 2\frac{\nu}{n}E(D_i) + \frac{\nu}{n^2} \\ &\quad + \frac{1-\nu}{n^2}E(\|\boldsymbol{\epsilon}_i\cdot\mathbf{a}\|^2) \\ &\overset{(*)}{\leq} \left(1 - \frac{1-\nu}{n}\left(2 - \frac{1}{n}\right)\right)E\left(D_i^2\right)2\frac{\nu}{n}E(D_i) + \frac{1}{n^2} \end{aligned}$$

where (*) holds because by Axiom 1 we have $\|\boldsymbol{\epsilon}_i\|^2 \leq R$ and by definition $\|\mathbf{a}\| = R$, $R = 1$. Inserting the result of (a) in the latter equation results in the following recursive formula:

$$E\left(D_{i+1}^2\right) \leq \left(1 - \frac{1-\nu}{n}\left(2 - \frac{1}{n}\right)\right) E\left(D_i^2\right) + 2(1-c_i)\frac{\nu}{n}\frac{\nu}{1-\nu} + \frac{1}{n^2}\,.$$

By the formula of the geometric series, i.e. by Prop. 2, we have:

$$E\left(D_i^2\right) \leq \left(2(1-c_i)\frac{\nu}{n}\frac{\nu}{1-\nu} + \frac{1}{n^2}\right)\frac{1-d_i}{\frac{1-\nu}{n}\left(2-\frac{1}{n}\right)}\,,$$

denoting $d_i := \left(1 - \frac{1-\nu}{n}\left(2 - \frac{1}{n}\right)\right)^i$. Furthermore by some algebra

$$E\left(D_i^2\right) \leq \frac{(1-c_i)(1-d_i)}{1-\frac{1}{2n}}\frac{\nu^2}{(1-\nu)^2} + \frac{1-d_i}{(2n-1)(1-\nu)}. \tag{16}$$

We will need the auxiliary formula

$$\frac{(1-c_i)(1-d_i)}{1-\frac{1}{2n}} - (1-c_i)^2 \leq \frac{1}{2n-1} + c_i - d_i\,, \tag{17}$$

which can be verified by some more algebra and employing $d_i < c_i$. We finally conclude

$$\begin{aligned}
\mathrm{Var}(D_i) &= E(D_i^2) - (E(D_i))^2 \\
&\overset{\text{Th.3}(a);\ \text{Eq.(16)}}{\leq} \left(\frac{(1-c_i)(1-d_i)}{1-\frac{1}{2n}} - (1-c_i)^2\right)\left(\frac{\nu}{1-\nu}\right)^2 \\
&\quad + \frac{1-d_i}{(2n-1)(1-\nu)^2} \\
&\overset{\text{Eq.(17)}}{\leq} \gamma_i\left(\frac{\nu}{1-\nu}\right)^2 + \delta_n
\end{aligned}$$

where $\gamma_i := c_i - d_i$ and $\delta_n := \frac{\nu^2 + (1-d_i)}{(2n-1)(1-\nu)^2}$. This completes the proof the theorem. $\square$