Bounding Stochastic Safety: Leveraging Freedman's Inequality with Discrete-Time Control Barrier Functions, Extended Proofs

Ryan K. Cosner, Preston Culbertson, and Aaron D. Ames

I. Proof for Lemma 1

A. Ville's Proof

Proof of Ville's inequality [1], Lemma **??**.

Proof. Fix $\lambda > 0$ and define the stopping time $\tau \triangleq \{\inf_{k\in\mathbb{N}} W_k > \lambda\}$ with $\tau = +\infty$ if $W_k <= \lambda$ for all time. Since W_k is a nonnegative supermartingale, the stopped process $W_{k\wedge\tau}$ is also a nonnegative supermartingale and

$$\mathbb{E}[W_{k\wedge\tau}] \leq \mathbb{E}[W_0] \text{ and } \liminf_{k\to\infty} \mathbb{E}[W_{k\wedge\tau}] \leq \mathbb{E}[W_0]. \quad (1)$$

We can further bound this in the case that τ is finite:

$$\begin{aligned}
\mathbb{E}[W_0] &\geq \liminf_{k\to\infty} \mathbb{E}[W_{k\wedge\tau}\mathbb{1}_{\{\tau<\infty\}}] && (2)\\
&\geq \mathbb{E}[\liminf_{k\to\infty} W_{k\wedge\tau}\mathbb{1}_{\{\tau<\infty\}}] && (3)\\
&> \mathbb{E}[\lambda\mathbb{1}_{\tau<\infty}] = \lambda\mathbb{P}\{\tau<\infty\} = \lambda\mathbb{P}\{\sup_{k\in\mathbb{N}} W_k > \lambda\}.
\end{aligned}$$

The first inequality is by the nonegativity of W_k and the second inequality is by Fatou's Lemma [2]. Rearranging terms completes the proof. □

II. Proof for Theorem 1 (RSS + c-martingales)

A. RSS Proof

Proof. Let $W_k = \alpha^{-k}(M - h(\mathbf{x}_k)) + M(\alpha^{-K} - \alpha^{-k})$. This is a nonnegative supermartingale for $k \leq K$:

$$\begin{aligned}
&\mathbb{E}[W_{k+1}|\mathscr{F}_k] && (4)\\
&= \alpha^{-(k+1)}(M - \mathbb{E}[h(\mathbf{x}_{k+1})|\mathscr{F}_k]) + M(\alpha^{-K} - \alpha^{-(k+1)})\\
&\leq \alpha^{-(k+1)}(M - \alpha h(\mathbf{x}_k)) + M(\alpha^{-K} - \alpha^{-(k+1)}) && (5)\\
&= \alpha^{-k}(M - h(\mathbf{x}_k)) + M(\alpha^{-K} - \alpha^{-k}) = W_k. && (6)
\end{aligned}$$

Apply Ville's inequality **??** to W_k to find:

$$\mathbb{P}\left\{\sup_{k\leq K} W_k \leq \lambda\right\} \leq \frac{\mathbb{E}[W_0]}{\lambda}. \quad (7)$$

Note that $\{\sup_{k\leq K} -h(\mathbf{x}_k) + \alpha^{-K}M > \lambda\} \subseteq \{\sup_{k\leq K} W_k > \lambda\}$. Choose $\lambda = \alpha M^{-K}$ to achieve:

$$P_u(K, \mathbf{x}_0) \leq \frac{M\alpha^{-K} - h(\mathbf{x}_0)}{M\alpha^{-K}} = 1 - \frac{h(\mathbf{x}_0)}{M}\alpha^K \quad (8)$$

□

B. Steinhardt Proof

Proof. Let $W_k \triangleq M - h(\mathbf{x_k}) + (K-k)c$. This is a non-negative supermartingale for $k \leq K$:

$$\begin{aligned}
W_k &= M - h(\mathbf{x}_k) + (K-k)c \geq 0 && (9)\\
\mathbb{E}[W_{k+1} \mid \mathscr{F}_k] &= M - \mathbb{E}[h(\mathbf{x}_{k+1}) \mid \mathscr{F}_k] + (K-k-1)c && (10)\\
&\leq M - h(\mathbf{x}_k) + c + (K-k-1)c && (11)\\
&= M - h(\mathbf{x}_k) + (K-k)c = W_k && (12)
\end{aligned}$$

Apply Ville's inequality **??** to W_k to find:

$$\mathbb{P}\left\{\sup_{k\leq K} W_k \leq \lambda\right\} \leq \frac{\mathbb{E}[W_0]}{\lambda} \quad (13)$$

Note that $\{\sup_{k\leq K} M - h(\mathbf{x}_k) \geq \lambda\} \subseteq \{\sup_{k\leq K} W_k \leq \lambda\}$. Choose $\lambda = M$ to achieve:

$$P_u(K, \mathbf{x}_0) \leq \frac{M - h(\mathbf{x}_0) + Kc}{M} = 1 - \frac{h(\mathbf{x}_0) - Kc}{M}.$$

□

III. Proof for Theorem 4

A. New c-martingale proof

Proof of Theorem **??**.

Proof. Define the candidate function $W_k = -h(\mathbf{x}_k) - kc + h(\mathbf{x}_0)$. This is satisfies $W_0 = 0$ and is a supermartingale:

$$\begin{aligned}
\mathbb{E}[W_{k+1} \mid \mathscr{F}_k] &= \mathbb{E}[-h(\mathbf{x}_{k+1})|\mathscr{F}_k] - (k+1)c + h(\mathbf{x}_0)\\
&\leq -h(\mathbf{x}_k) - kc + h(\mathbf{x}_0) = W_k. && (14)
\end{aligned}$$

Consider the Doob's decomposition of this supermartingale. The resulting martingale is:

$$M_k = W_k - \sum_{i=1}^{k}(\mathbb{E}[W_i \mid \mathscr{F}_{i-1}] - W_{i-1}) \quad (15)$$

The martingale difference is given by:

$$\begin{aligned}
M_k - M_{k-1} &= W_k - \mathbb{E}[W_k \mid \mathscr{F}_{k-1}] && (16)\\
&= -h(\mathbf{x}_k) + \mathbb{E}[h(\mathbf{x}_k) \mid \mathbf{F}_{k-1}] && (17)\\
&\leq 1 && (18)
\end{aligned}$$

Now we consider the inequalities:

$$\begin{aligned}
&\sup_{k\leq K} -h(\mathbf{x}_k) - Kc + h(\mathbf{x}_0) \leq \sup_{k\leq K} h(\mathbf{x}_k) - kc + h(\mathbf{x}_0)\\
&\leq \sup_{k\leq K} W_k + \sum_{i=1}^{k}(\mathbb{E}[h(\mathbf{x}_i) \mid \mathscr{F}_{i-1}] - h(\mathbf{x}_i) + c) && (19)\\
&= \sup_{k\leq K} W_k - \sum_{i=1}^{k}(\mathbb{E}[W_i \mid F_{i-1}] - W_{i-1}) = \sup_{k\leq K} M_k. && (20)
\end{aligned}$$

The authors are with the Department of Mechanical and Civil Engineering at the California Institute of Technology, Pasadena, CA 91125, USA. {rkcosner, pbulbert, ames}@caltech.edu
This work was supported by BP and NSF CPS Award #1932091.

Consider the case when $\lambda = -Kc + h(\mathbf{x}_0)$. Then the safety event satisfies the containment:

$$\left\{\inf_{k\leq K} h(\mathbf{x}_k) < 0\right\} \subseteq \left\{\sup_{k\leq K} M_k \geq -Kc + h(\mathbf{x}_0)\right\}.$$

Applying the probability bound from Theorem **??** results in the probability bound:

$$P_u(K, \mathbf{x}_0) \leq H(-Kc + h(\mathbf{x}_0), \sigma\sqrt{K}) \tag{21}$$

□

IV. Proof of proposition 6

Proof. By combining the bounds (**??**) and (**??**):

$$h(\mathbf{x}_{k+1}) \geq \mathbb{E}[h(\mathbf{x}_{k+1}) \mid \mathscr{F}_k] - \delta \geq \alpha h(\mathbf{x}_k) - \delta \tag{22}$$

Thus, for $K < \infty$, we can lower bound $h(\mathbf{x}_k) \geq \alpha^k h(\mathbf{x}_0) - \sum_{i=0}^{k-1} \alpha^i \delta$. Furthermore, for all time, $h(\mathbf{x}_k) \geq \frac{-\delta}{1-\alpha} \implies h(\mathbf{x}_{k+1}) \geq \frac{-\delta}{1-\alpha}$, so $\mathcal{C}_\delta$ is safe. □

V. Proof of Corollary 1

A. Proof of Corrolary ??

Proof. First define $\eta(\mathbf{x}) = \frac{h(\mathbf{x})+\epsilon}{\delta}$ and $W_k = -\alpha^{K-k}\eta(\mathbf{x}_k) + \alpha^K \eta(\mathbf{x}_0) + \sum_{i=1}^{k} \alpha^{K-i} \frac{\epsilon}{\delta}(1-\alpha)$. First note that h_k satisfies:

$$E[\eta(\mathbf{x}_k)|\mathscr{F}_{k-1}] \geq \alpha(\eta_{k-1}) + \frac{\epsilon}{\delta}(1-\alpha) \tag{23}$$

Note that W_k is a supermartingale:

$$\mathbb{E}[W_{k+1}|\mathscr{F}_k] \tag{24}$$

$$= -\alpha^{K-(k+1)}\mathbb{E}[\eta_{k+1}|\mathscr{F}_k] + \alpha^K \eta_0 + \sum_{i=1}^{k+1} \alpha^{K-i}\epsilon(1-\alpha)/\delta$$

$$\leq -\alpha^{K-k}\eta_k + \alpha^K\eta_0 + \sum_{i=1}^{k}\alpha^{K-i}\epsilon(1-\alpha)/\delta = W_k \tag{25}$$

and $W_0 = 0$.

Take the Doob's decomposition. Then consider the martingale: $M_k = W_0 + \sum_{i=1}^{k}(W_i - \mathbb{E}[W_i|\mathscr{F}_{i-1}])$. Since the predictable quadratic variation $\langle h(\mathbf{x})\rangle_k$ is bounded, so is $\langle M\rangle_k$:

$$\langle M\rangle_k = \sum_{i=1}^{k} \mathbb{E}[(W_i - \mathbb{E}[W_i|\mathscr{F}_{i-1}])^2|\mathscr{F}_{i-1}] \tag{26}$$

$$= \sum_{i=1}^{k} \alpha^{2(K-i)}\mathbb{E}[(\eta(\mathbf{x}_k) - \mathbb{E}[\eta(\mathbf{x}_i)|\mathscr{F}_{i-1}])^2|\mathscr{F}_{i-1}] \tag{27}$$

$$= \sum_{i=1}^{k} \frac{\alpha^{2(K-i)}}{\delta^2}\mathbb{E}[(h(\mathbf{x}_k) - \mathbb{E}[h(\mathbf{x}_i)|\mathscr{F}_{i-1}])^2|\mathscr{F}_{i-1}] \tag{28}$$

$$\leq \sum_{i=1}^{k} \frac{\alpha^{2(K-i)}}{\delta^2}\sigma^2 \leq \frac{K\sigma^2}{\delta^2} \tag{29}$$

Next we'll bound some stuff:

$$\min_{k\leq K} \eta(\mathbf{x}_k) < 0 \iff \min_{1\leq k\leq K} \eta(\mathbf{x}_k) \leq 0 \tag{30}$$

$$\implies \max_{1\leq k\leq K} W_k \geq \alpha^K \eta(\mathbf{x}_0) + \sum_{i=1}^{k} \alpha^{K-i}\frac{\epsilon}{\delta}(1-\alpha) \tag{31}$$

$$\implies \max_{1\leq k\leq K} W_k \geq \alpha^K \eta(\mathbf{x}_0) + \alpha^{K-1}\frac{\epsilon}{\delta}(1-\alpha) \tag{32}$$

$$\implies \max_{1\leq k\leq K} M_k \geq \alpha^K \eta(\mathbf{x}_0) + \alpha^{K-1}\frac{\epsilon}{\delta}(1-\alpha) \tag{33}$$

Lower bound h as in Theorem **??**, $h(\mathbf{x}_k) \geq \alpha^K h(\mathbf{x}_0) + \sum_{i=0}^{K-1} \alpha^i \delta$ to achieve the indicator probability and then choose $\lambda = \alpha^K \eta(\mathbf{x}_0) + \alpha^{K-1}\frac{\epsilon}{\delta}(1-\alpha)$ and apply Theorem **??** to M_k to finalize the bound. □

References

[1] J. Ville, "Etude critique de la notion de collectif," 1939.

[2] G. Grimmett and D. Stirzaker, *Probability and Random Processes*. Oxford University Press, July 2020.