

# Adversarial Reinforcement Learning: Neural Cryptography

Faris Sbahi<sup>1</sup> and Barrett Ames<sup>2</sup>

<sup>1</sup> Primary

`faris.sbahi@duke.edu`

<sup>2</sup> Consultant

`barrett.ames@duke.edu`

**Abstract.** The abstract should summarize the contents of the paper using at least 70 and at most 150 words. It will be set in 9-point font size and be inset 1.0 cm from the right and left margins. There will be two blank lines before and after the Abstract. ...

**Keywords:** computational geometry, graph theory, Hamilton cycles

## 1 Fixed-Period Problems: The Sublinear Case

With this chapter, the preliminaries are over, and we begin the search for periodic solutions to Hamiltonian systems. All this will be done in the convex case; that is, we shall study the boundary-value problem

$$\begin{aligned}\dot{x} &= JH'(t, x) \\ x(0) &= x(T)\end{aligned}$$

with  $H(t, \cdot)$  a convex function of  $x$ , going to  $+\infty$  when  $\|x\| \rightarrow \infty$ .

## 1.1 Autonomous Systems

In this section, we will consider the case when the Hamiltonian  $H(x)$  is autonomous. For the sake of simplicity, we shall also assume that it is  $C^1$ .

We shall first consider the question of nontriviality, within the general framework of  $(A_\infty, B_\infty)$ -subquadratic Hamiltonians. In the second subsection, we shall look into the special case when  $H$  is  $(0, b_\infty)$ -subquadratic, and we shall try to derive additional information.

**The General Case: Nontriviality.** We assume that  $H$  is  $(A_\infty, B_\infty)$ -subquadratic at infinity, for some constant symmetric matrices  $A_\infty$  and  $B_\infty$ , with  $B_\infty - A_\infty$  positive definite. Set:

$$\gamma := \text{smallest eigenvalue of } B_\infty - A_\infty \quad (1)$$

$$\lambda := \text{largest negative eigenvalue of } J \frac{d}{dt} + A_\infty . \quad (2)$$

Theorem 1 tells us that if  $\lambda + \gamma < 0$ , the boundary-value problem:

$$\begin{aligned} \dot{x} &= JH'(x) \\ x(0) &= x(T) \end{aligned} \quad (3)$$

has at least one solution  $\bar{x}$ , which is found by minimizing the dual action functional:

$$\psi(u) = \int_0^T \left[ \frac{1}{2} (\Lambda_o^{-1} u, u) + N^*(-u) \right] dt \quad (4)$$

on the range of  $\Lambda$ , which is a subspace  $R(\Lambda)_L^2$  with finite codimension. Here

$$N(x) := H(x) - \frac{1}{2} (A_\infty x, x) \quad (5)$$

is a convex function, and

$$N(x) \leq \frac{1}{2} ((B_\infty - A_\infty) x, x) + c \quad \forall x . \quad (6)$$

**Proposition 1.** *Assume  $H'(0) = 0$  and  $H(0) = 0$ . Set:*

$$\delta := \liminf_{x \rightarrow 0} 2N(x) \|x\|^{-2} . \quad (7)$$

*If  $\gamma < -\lambda < \delta$ , the solution  $\bar{u}$  is non-zero:*

$$\bar{x}(t) \neq 0 \quad \forall t . \quad (8)$$

*Proof.* Condition (7) means that, for every  $\delta' > \delta$ , there is some  $\varepsilon > 0$  such that

$$\|x\| \leq \varepsilon \Rightarrow N(x) \leq \frac{\delta'}{2} \|x\|^2 . \quad (9)$$

It is an exercise in convex analysis, into which we shall not go, to show that this implies that there is an  $\eta > 0$  such that

$$f \|x\| \leq \eta \Rightarrow N^*(y) \leq \frac{1}{2\delta'} \|y\|^2 . \quad (10)$$

**Fig. 1.** This is the caption of the figure displaying a white eagle and a white horse on a snow field

Since  $u_1$  is a smooth function, we will have  $\|hu_1\|_\infty \leq \eta$  for  $h$  small enough, and inequality (10) will hold, yielding thereby:

$$\psi(hu_1) \leq \frac{h^2}{2} \frac{1}{\lambda} \|u_1\|_2^2 + \frac{h^2}{2} \frac{1}{\delta'} \|u_1\|^2 . \quad (11)$$

If we choose  $\delta'$  close enough to  $\delta$ , the quantity  $(\frac{1}{\lambda} + \frac{1}{\delta'})$  will be negative, and we end up with

$$\psi(hu_1) < 0 \quad \text{for } h \neq 0 \text{ small} . \quad (12)$$

On the other hand, we check directly that  $\psi(0) = 0$ . This shows that 0 cannot be a minimizer of  $\psi$ , not even a local one. So  $\bar{u} \neq 0$  and  $\bar{u} \neq \Lambda_o^{-1}(0) = 0$ .  $\square$

**Corollary 1.** *Assume  $H$  is  $C^2$  and  $(a_\infty, b_\infty)$ -subquadratic at infinity. Let  $\xi_1, \dots, \xi_N$  be the equilibria, that is, the solutions of  $H'(\xi) = 0$ . Denote by  $\omega_k$  the smallest eigenvalue of  $H''(\xi_k)$ , and set:*

$$\omega := \text{Min} \{ \omega_1, \dots, \omega_k \} . \quad (13)$$

If:

$$\frac{T}{2\pi} b_\infty < -E \left[ -\frac{T}{2\pi} a_\infty \right] < \frac{T}{2\pi} \omega \quad (14)$$

then minimization of  $\psi$  yields a non-constant  $T$ -periodic solution  $\bar{x}$ .

We recall once more that by the integer part  $E[\alpha]$  of  $\alpha \in \mathbb{R}$ , we mean the  $a \in \mathbb{Z}$  such that  $a < \alpha \leq a + 1$ . For instance, if we take  $a_\infty = 0$ , Corollary 2 tells us that  $\bar{x}$  exists and is non-constant provided that:

$$\frac{T}{2\pi} b_\infty < 1 < \frac{T}{2\pi} \quad (15)$$

or

$$T \in \left( \frac{2\pi}{\omega}, \frac{2\pi}{b_\infty} \right) . \quad (16)$$

*Proof.* The spectrum of  $\Lambda$  is  $\frac{2\pi}{T}\mathbb{Z} + a_\infty$ . The largest negative eigenvalue  $\lambda$  is given by  $\frac{2\pi}{T}k_o + a_\infty$ , where

$$\frac{2\pi}{T}k_o + a_\infty < 0 \leq \frac{2\pi}{T}(k_o + 1) + a_\infty . \quad (17)$$

Hence:

$$k_o = E \left[ -\frac{T}{2\pi} a_\infty \right] . \quad (18)$$

The condition  $\gamma < -\lambda < \delta$  now becomes:

$$b_\infty - a_\infty < -\frac{2\pi}{T}k_o - a_\infty < \omega - a_\infty \quad (19)$$

which is precisely condition (14).  $\square$

**Lemma 1.** *Assume that  $H$  is  $C^2$  on  $\mathbb{R}^{2n} \setminus \{0\}$  and that  $H''(x)$  is non-degenerate for any  $x \neq 0$ . Then any local minimizer  $\tilde{x}$  of  $\psi$  has minimal period  $T$ .*

*Proof.* We know that  $\tilde{x}$ , or  $\tilde{x} + \xi$  for some constant  $\xi \in \mathbb{R}^{2n}$ , is a  $T$ -periodic solution of the Hamiltonian system:

$$\dot{x} = JH'(x) . \quad (20)$$

There is no loss of generality in taking  $\xi = 0$ . So  $\psi(x) \geq \psi(\tilde{x})$  for all  $\tilde{x}$  in some neighbourhood of  $x$  in  $W^{1,2}(\mathbb{R}/T\mathbb{Z}; \mathbb{R}^{2n})$ .

But this index is precisely the index  $i_T(\tilde{x})$  of the  $T$ -periodic solution  $\tilde{x}$  over the interval  $(0, T)$ , as defined in Sect. 2.6. So

$$i_T(\tilde{x}) = 0 . \quad (21)$$

Now if  $\widetilde{x}$  has a lower period,  $T/k$  say, we would have, by Corollary 31:

$$i_T(\widetilde{x}) = i_{kT/k}(\widetilde{x}) \geq ki_{T/k}(\widetilde{x}) + k - 1 \geq k - 1 \geq 1 \; . \tag{22}$$

This would contradict (21), and thus cannot happen.  $\square$

*Notes and Comments.* The results in this section are a refined version of [?]; the minimality result of Proposition 14 was the first of its kind.

To understand the nontriviality conditions, such as the one in formula (16), one may think of a one-parameter family  $x_T$ ,  $T \in (2\pi\omega^{-1}, 2\pi b_\infty^{-1})$  of periodic solutions,  $x_T(0) = x_T(T)$ , with  $x_T$  going away to infinity when  $T \rightarrow 2\pi\omega^{-1}$ , which is the period of the linearized system at 0.

**Table 1.** This is the example table taken out of *The T<sub>E</sub>Xbook*, p. 246

Year	World population
8000 B.C.	5,000,000
50 A.D.	200,000,000
1650 A.D.	500,000,000
1945 A.D.	2,300,000,000
1980 A.D.	4,400,000,000

**Theorem 1 (Ghoussoub-Preiss).** *Assume  $H(t, x)$  is  $(0, \varepsilon)$ -subquadratic at infinity for all  $\varepsilon > 0$ , and  $T$ -periodic in  $t$*

$$H(t, \cdot) \quad \text{is convex} \quad \forall t \tag{23}$$

$$H(\cdot, x) \quad \text{is } T\text{--periodic} \quad \forall x \tag{24}$$

$$H(t, x) \geq n(\|x\|) \quad \text{with } n(s)s^{-1} \rightarrow \infty \text{ as } s \rightarrow \infty \tag{25}$$

$$\forall \varepsilon > 0 \; , \quad \exists c \; : \; H(t, x) \leq \frac{\varepsilon}{2} \|x\|^2 + c \; . \tag{26}$$

Assume also that  $H$  is  $C^2$ , and  $H''(t, x)$  is positive definite everywhere. Then there is a sequence  $x_k$ ,  $k \in \mathbb{N}$ , of  $kT$ -periodic solutions of the system

$$\dot{x} = JH'(t, x) \quad (27)$$

such that, for every  $k \in \mathbb{N}$ , there is some  $p_o \in \mathbb{N}$  with:

$$p \geq p_o \Rightarrow x_{pk} \neq x_k . \quad (28)$$

□

*Example 1* (External forcing). Consider the system:

$$\dot{x} = JH'(x) + f(t) \quad (29)$$

where the Hamiltonian  $H$  is  $(0, b_\infty)$ -subquadratic, and the forcing term is a distribution on the circle:

$$f = \frac{d}{dt}F + f_o \quad \text{with } F \in L^2(\mathbb{R}/T\mathbb{Z}; \mathbb{R}^{2n}) , \quad (30)$$

where  $f_o := T^{-1} \int_0^T f(t)dt$ . For instance,

$$f(t) = \sum_{k \in \mathbb{N}} \delta_k \xi , \quad (31)$$

where  $\delta_k$  is the Dirac mass at  $t = k$  and  $\xi \in \mathbb{R}^{2n}$  is a constant, fits the prescription. This means that the system  $\dot{x} = JH'(x)$  is being excited by a series of identical shocks at interval  $T$ .

**Definition 1.** Let  $A_\infty(t)$  and  $B_\infty(t)$  be symmetric operators in  $\mathbb{R}^{2n}$ , depending continuously on  $t \in [0, T]$ , such that  $A_\infty(t) \leq B_\infty(t)$  for all  $t$ .

A Borelian function  $H : [0, T] \times \mathbb{R}^{2n} \rightarrow \mathbb{R}$  is called  $(A_\infty, B_\infty)$ -subquadratic at infinity if there exists a function  $N(t, x)$  such that:

$$H(t, x) = \frac{1}{2} (A_\infty(t)x, x) + N(t, x) \quad (32)$$

$$\forall t, \quad N(t, x) \quad \text{is convex with respect to } x \quad (33)$$

$$N(t, x) \geq n(\|x\|) \quad \text{with } n(s)s^{-1} \rightarrow +\infty \text{ as } s \rightarrow +\infty \quad (34)$$

$$\exists c \in \mathbb{R} : \quad H(t, x) \leq \frac{1}{2} (B_\infty(t)x, x) + c \quad \forall x. \quad (35)$$

If  $A_\infty(t) = a_\infty I$  and  $B_\infty(t) = b_\infty I$ , with  $a_\infty \leq b_\infty \in \mathbb{R}$ , we shall say that  $H$  is  $(a_\infty, b_\infty)$ -subquadratic at infinity. As an example, the function  $\|x\|^\alpha$ , with  $1 \leq \alpha < 2$ , is  $(0, \varepsilon)$ -subquadratic at infinity for every  $\varepsilon > 0$ . Similarly, the Hamiltonian

$$H(t, x) = \frac{1}{2}k \|k\|^2 + \|x\|^\alpha \quad (36)$$

is  $(k, k + \varepsilon)$ -subquadratic for every  $\varepsilon > 0$ . Note that, if  $k < 0$ , it is not convex.

*Notes and Comments.* The first results on subharmonics were obtained by Rabinowitz in [?], who showed the existence of infinitely many subharmonics both in the subquadratic and superquadratic case, with suitable growth conditions on  $H'$ . Again the duality approach enabled Clarke and Ekeland in [?] to treat the same problem in the convex-subquadratic case, with growth conditions on  $H$  only.

Recently, Michalek and Tarantello (see [?] and [?]) have obtained lower bound on the number of subharmonics of period  $kT$ , based on symmetry considerations and on pinching estimates, as in Sect. 5.2 of this article.



## References

1. R. Elderman, L. J. Pater, A. S. Thie, M. M. Drugan, and M. Wiering, “Adversarial reinforcement learning in a cyber security simulation.,” in *ICAART (2)*, pp. 559–566, 2017.
2. M. Abadi and D. G. Andersen, “Learning to protect communications with adversarial neural cryptography,” *arXiv preprint arXiv:1610.06918*, 2016.
3. S. Shiva, S. Roy, and D. Dasgupta, “Game theory for cyber security,” in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, p. 34, ACM, 2010.
4. C. Finn, P. Christiano, P. Abbeel, and S. Levine, “A connection between generative adversarial networks, inverse reinforcement learning, and energy-based models,” *arXiv preprint arXiv:1611.03852*, 2016.
5. D. Pfau and O. Vinyals, “Connecting generative adversarial networks and actor-critic methods,” *arXiv preprint arXiv:1610.01945*, 2016.
6. L. Pinto, J. Davidson, R. Sukthankar, and A. Gupta, “Robust adversarial reinforcement learning,” *arXiv preprint arXiv:1703.02702*, 2017.
7. X. Lin, P. A. Beling, and R. Cogill, “Multi-agent inverse reinforcement learning for zero-sum games,” *arXiv preprint arXiv:1403.6508*, 2014.
8. R. Sutton and A. Barto, “Reinforcement learning: an introduction.[internet],” 2016.