# Introduction to Finite Dynamical Systems

Adrien Richard

Lecture n° 4 and 5, M2 Informatique, October 2 and 4, 2019

## 1 Upper bound on $\max(G)$ via error correcting codes

Let $x, y \in \{0,1\}^n$. We set

$$\Delta(x,y) = \{i \in [n] | x_i \neq y_i\}, \qquad d(x,y) = |\Delta(x,y)|.$$

The quantity $d(x,y)$ is the **Hamming distance** between $x$ and $y$ (see Exercice 1). In particular, we have the triangular inequality $d(x,y) \leq d(x,z) + d(z,y)$ for all $z \in \{0,1\}^n$.

Here is a very useful lemma.

**Lemma 1.** *Let $f \in F(G)$ with distinct fixed points $x$ and $y$. Then $G[\Delta(x,y)]$ has a cycle.*

*Proof.* Let $I = \Delta(x,y)$ and $i \in I$, that is, $x_i \neq y_i$. If $x_{N(i)} = y_{N(i)}$ then $f_i(x) = f_i(y)$ and thus $x_i = y_i$ since $x$ and $y$ are fixed points, which is a contradiction. We deduce that $x_j \neq y_j$ for some $j \in N(i)$. Thus $N(i) \cap I \neq \emptyset$ for all $i \in I$. This is equivalent to say that $\delta^-(G[I]) \geq 1$, and this trivially implies that $G[I]$ has a cycle. □

The **girth** of $G$, denoted $g(G)$, is the minimum length of a cycle in $G$. If $G$ is acyclic, then $g(G) = n+1$ by convention, where $n$ is the number of vertices in $G$. Let $X \subseteq \{0,1\}^n$. The **minimum distance** of $X$ is the minimum of $d(x,y)$ for *distinct* $x, y \in X$. If $|X| \leq 1$, then the minimum distance of $X$ is $n+1$ by convention. As a simple consequence of the previous lemma, we have that the set of fixed points of a Boolean network on $G$ is at least the girth of $G$.

**Lemma 2.** *Let $f \in F(G)$ with distinct fixed points $x$ and $y$. Then $d(x,y) \geq g(G)$.*

*Proof.* Indeed, by the previous lemma, $G[\Delta(x,y)]$ has a cycle $C$. Since $V(G) \subseteq \Delta(x,y)$ we obtain

$$d(x,y) = |\Delta(x,y)| \geq |V(G)| \geq g(G).$$

□

Thus if the girth is large (with respect to the number of vertices), then fixed points are far from each other and we cannot have to many fixed points. To quantify this phenomena we need additional definitions from Information Theory.

For positive integers $n, d$, we denote by $A(n,d)$ the maximum size of a set $X \subseteq \{0,1\}^n$ with minimum distance at least $d$. Given $x \in \{0,1\}^n$ and $r \geq 0$, the **Hamming ball** of center $x$ and radius $r$ is the set of $y \in \{0,1\}^n$ such that $d(x,y) \leq r$. If $X$ has minimum distance at least $d$, then $B_t(x) \cap B_t(y) = \emptyset$ for all distinct $x, y \in X$, where $t = \lfloor \frac{d-1}{2} \rfloor$ (Exercise 3). Suppose now that the members of $X$, seen messages, are send through a communication channel, and suppose that at most $t$ bits can be changed during the transmission. If distinct $x, y \in X$ are send, the received messages belong to $B_t(x)$ and $B_t(y)$, and since these Hamming ball are disjoint, we can recover $x$ and $y$ without possible ambiguity. We then say that $X$ is a **Error Correcting Code** correcting $t$ bits, and $A(n,d)$ is the maximum size of such a code. This is a very well studied quantity in Information Theory.

An obvious consequence of the previous lemma is the following.

**Theorem 1** (Coding bound; Gadouleau, Riis, 2011)**.** *For every graph $G$ with $n$ vertices, we have*

$$\max(G) \leq A(n, g(G)).$$

*Proof.* Let $f \in F(G)$ and let $X \subseteq \{0,1\}^n$ be the set of fixed points of $f$. By the previous lemma, $X$ has minimum distance at least $g(G)$ and thus $|X| \leq A(n, g(G))$ by definition. □

We have now tow upper bounds on $\max(G)$, the feedback bound $2^{\tau(G)}$ and the coding bound given above. Each time we have two bound, a natural question is: do these bounds are comptitive? We think that the coding bound is never better than the feedback bound.

**Conjecture 1.** *For every graph $G$ with $n$ vertices, we have*

$$2^{\tau(G)} \leq A(n, g(G)).$$

## 2 Upper and lower bounds on $A(n,d)$

To show that there are few fixed points when the girth is large compare to the number of vertices, it is sufficient to show that $A(n,d)$ is small when $d$ is close to $n$. We do this is this section and we also show that, conversely, $A(n,d)$ is large when $d$ is far from $n$.

In a previous lecture, we have use (and prove) the *Projection Lemma*: If $X \subseteq \{0,1\}^n$, $I \subseteq [n]$ and $|X| > 2^{|I|}$ then $x_I = y_I$ for distinct $x, y \in X$, and thus $d(x,y) \leq n - |I|$. This indeed show that a large subset of $X$ contained at least to members close to each other. Actually, we easily get the following bound.

**Theorem 2** (Singleton bound)**.** *For all positive integers $n$ and $d \leq n+1$, we have*

$$A(n,d) \leq 2^{n-d+1}.$$

*Proof.* Let $X \subseteq \{0,1\}^n$ with minimal distance at least $d$ and $|X| = A(n,d)$. Let $I \subseteq [n]$ of size $n-d+1$. If $|X| > 2^{n-d+1}$ then $x_I = y_I$ for distinct $x, y \in X$. But then $d(x,y) \leq n - |I| = d-1$, a contradiction. Thus $A(n,d) = |X| \leq 2^{n-d+1}$. □

As a consequence, $\max(G) \leq 2^{n-g(G)+1}$ but this bound is not interesting since for all graph $G$ with $n$ vertices we have

$$\tau(G) \leq n - g(G) + 1$$

(see Exercice 4). It is a nice exercise to characterize the graphs $G$ such that the previous inequality is an equality (Exercice 6), and the graphs $G$ such that $\max(G) = 2^{n-g(G)+1}$ (Exercice 8). The following bound improve the singleton bound, excepted for very particular cases (Exercice 9).

**Theorem 3** (Sphere packing bound)**.** *For all positive integers $n$ and $d \leq n+1$, we have*

$$A(n,d) \leq \frac{2^n}{\sum_{k=0}^{t} \binom{k}{n}} \qquad \textit{where} \qquad t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

*Proof.* Let $X \subseteq \{0,1\}^n$ with minimum distance at least $d$. It is sufficient to prove that $|X| \leq 2^n/b_t(n)$, where $b_t(n) = \sum_{k=0}^{t} \binom{k}{n}$. Note that $|B_t(x)| = b_t(n)$ for all $x \in \{0,1\}^n$ (Exercice 2). Furthermore, $B_t(x) \cap B_t(y) = \emptyset$ for all distinct $x, y \in X$ (Exercice 3). We deduce that

$$2^n \geq \left| \bigcup_{x \in X} B_t(x) \right| = \sum_{x \in X} |B_t(x)| = \sum_{x \in X} b_t(n) = |X| \cdot b_t(n).$$

Thus $|X| \leq 2^n/b_t(n)$. □

**Theorem 4** (Gilbert bound)**.** *For all positive integers $n$ and $d \leq n+1$, we have*

$$A(n,d) \leq \frac{2^n}{\sum_{k=0}^{d-1} \binom{k}{n}}.$$

*Proof.* Let $X \subseteq \{0,1\}^n$ with minimum distance at least $d$ and of maximal size of this property, that is, of size $A(n,d)$. We have

$$\text{for all } y \in \{0,1\}^n \text{, there is } x \in X \text{ such that } d(y,x) \leq d-1. \qquad (*)$$

Suppose, for a contradiction, that there is $y \in \{0,1\}^n$ such that $d(y,x) \geq d$ for all $x \in X$. Then $X \cup \{y\}$ is of size $|X|+1$ and has minimum distance at least $d$. This is a contradiction since $X$ is of maximal size for this property. This proves $(*)$, which is equivalent to

$$\bigcup_{x \in X} B_{d-1}(x) = \{0,1\}^n.$$

We obtain

$$2^n = \left| \bigcup_{x \in X} B_{d-1}(x) \right| \leq \sum_{x \in X} |B_{d-1}(x)| = \sum_{x \in X} \sum_{k=0}^{d-1} \binom{k}{n} = |X| \cdot \sum_{k=0}^{d-1} \binom{k}{n}.$$

□

## 3 Exercises

1. *Prove that the Hamming distance is indeed a distance.*

   *Answer.* Let $x, y \in \{0,1\}^n$. We trivially have $d(x,y) \geq 0$ (non-negativity), $d(x,y) = 0 \iff x = y$ (identity), and $d(x,y) = d(y,x)$ (symmetry). It only remains to prove the triangular inequality: for any $z \in \{0,1\}^n$, $d(x,y) \leq d(x,z) + d(z,y)$. Suppose that $i \in \Delta(x,y)$, that is, $x_i \neq y_i$. Then, either $x_i \neq z_i$ or $y_i \neq z_i$, and thus either $i \in \Delta(x,z)$ or $i \in \Delta(z,y)$. We have prove that $\Delta(x,y) \subseteq \Delta(x,z) \cup \Delta(z,y)$. We deduce

   $$d(x,y) = |\Delta(x,y)| \leq |\Delta(x,z) \cup \Delta(z,y)| \leq |\Delta(x,z)| + |\Delta(z,y)| = d(x,z) + d(z,y).$$

2. *Let $x \in \{0,1\}^n$ and $r \geq 0$. Give the size $B_r(x)$ as a function of $n$ and $r$.*

   *Answer.* We have

   $$|B_r(x)| = \sum_{k=0}^{r} \binom{k}{n}.$$

3. *Let* $X \subseteq \{0,1\}^n$ *with minimum distance at least* $d \geq 1$. *Let* $t = \lfloor d - 1/2 \rfloor$. *Prove that* $B_t(x) \cap B_t(y) = \emptyset$ *for all distinct* $x, y \in X$.

   *Answer.* Let $x, y \in X$, $x \neq y$. Suppose for a contradiction that $z \in B_t(x) \cap B_t(y)$. This is equivalent to say that $d(x,z) \leq t$ and $d(y,z) \leq t$. Using the triangular inequality, we get

   $$d(x,y) \leq d(x,z) + d(z,y) \leq 2t = 2\lfloor d - 1/2 \rfloor \leq d - 1.$$

   This is a contradiction since $X$ has minimum distance at least $d$.

4. *Let* $G$ *be a graph with* $n$ *vertices. Prove that*

   $$g(G) \geq 2 \quad \text{and} \quad \tau(G) = n - 1 \qquad \Longleftrightarrow \qquad G \sim K_n.$$

   *Answer.* The direction $\Leftarrow$ is obvious. To prove $\Rightarrow$, suppose that $g(G) \geq 2$ and $\tau(G) = n - 1$. Then $G$ has no loop. Let $i, j$ be distinct vertices. Let $I = V(G) \setminus \{i, j\}$. Since $|I| < \tau(G)$, $G \setminus I$ has a cycle, that is, the is an arc form $i$ to $j$ and from $j$ to $i$. This proves that $G \sim K_n$.

5. *Prove that* $\tau(G) \leq n - g(G) + 1$ *for every graph* $G$ *with* $n$ *vertices.*

   *Answer.* Let $I$ be a FVS of $G$ os size $\tau(G)$. In a previous lecture, we have seen that, given $i \in I$, there exists a cycle $C$ with $V(C) \cap I = \{i\}$. Thus

   $$n \geq |V(C) \cup I| = |V(C)| + |I| - 1 = |V(C)| + \tau(G) - 1 \geq g(G) + \tau(G) - 1.$$

6. *Let* $G$ *be a graph with* $n$ *vertices. Prove that* $\tau(G) = n - g(G) + 1$ *if and only is one of the following holds:*

   (a) $G \sim C_n$.

   (b) $G \sim K_n$.

   (c) *each vertex of* $G$ *has a loop.*

   *Answer.* Let $\tau = \tau(G)$ and $g = g(G)$. It is clear that if one of (a),(b),(c) is true then $\tau = n - g + 1$. For the other direction, suppose that $\tau = n - g + 1$. Suppose first that $g = 1$. Then $\tau = n$ and we deduce that (c) is true. So suppose that $g \geq 2$. Let $I$ be a FVS of $G$ of size $\tau$ and let $J = V(G) \setminus I$ (the acyclic part). Let $i \in I$ and let $C$ be a cycle with $V(C) \cap I = \{i\}$. Then

   $$n \geq |V(C) \cup I| = |V(C)| + |I| - 1 = V(C) + \tau - 1 \geq g + \tau - 1 = n.$$

   Thus $C$ is of length $g$. Let $j_1 j_2 \dots j_g$ the vertices of $C$ in the order, starting from $j_1 = i$. Then $\{j_2, \dots, j_g\}$ is disjoint from $I$ and of size $g - 1 = n - \tau$, thus $J = \{j_2, \dots, j_g\}$ and $G[J]$ is the path $j_2 \dots j_g$. We deduce that if $I = \{i\}$ then $G = C_n$. So suppose that $|I| = \tau > 1$. Let $i' \in I$ distinct from $i$ and let $C'$ be a cycle with $V(C') \cap I = \{i'\}$. We prove similarly that $C'$ is of length $g$, and thus the vertices of $C'$ in the order are $i' j_2 \dots j_g$. We deduce that all the cycles of $G \setminus \{j_2\}$ are in $G[I]$. Let $I'$ be a FVS of size $G[I]$; it is not empty since $\tau > 1$. Then $I' \cup \{i\}$ is a FVS of $G$, and thus $|I| \leq |I'| + 1$. On the other hand, we have $|I'| < |I|$ since if $|I'| = |I|$ then it means that each vertex of $G[I]$ has a loop, and thus $g = 1$, a contradiction. Hence, $|I'| = |I| - 1$ and since $g(G[I]) \geq g(G) \geq 2$, we deduce from a previous exercise that $G[I] \sim K_\tau$. Thus $g = 2$ and we again deduce from the previous exercise that $G \sim K_n$.

7. *Prove that* $\max(C_n) = 2$ *and* $\max(K_n) = 2^{n-1}$.

   *Answer.* Since $\tau(C_n) = 1$ we have $\max(C_n) \leq 2$ and since $\nu(C_n) = 1$ we have $\max(C_n) \geq 2$. Since $\tau(K_n) = n-1$, it is sufficient to prove that there is $f \in F(K_n)$ with $2^{n-1}$ fixed points. Let $f \in F(K_n)$ be defined by $f_i(x) = \sum_{j \neq i} x_j$ for all $i \in [n]$. Let $x \in \{0,1\}^n$ with an even number of ones. If $x_i = 0$ then $f_i(x) = 0$ and if $x_i = 1$ then $f_i(x) = 1$. Thus $f(x) = x$. We deduce that $f$ has $2^{n-1}$ fixed points.

8. *Let* $G$ *be a graph with* $n$ *vertices, and let* $nC_1$ *be the disjoint union of* $n$ *copies of* $C_1$. *Prove that*

$$\max(G) = 2^{n-g(G)+1} \qquad \iff \qquad G \sim nC_1 \quad \text{or} \quad G \sim C_n \quad \text{or} \quad G \sim K_n.$$

   *Answer.* The direction $\Leftarrow$ is obvious for $nC_1$ and easy for $C_n$ and $K_n$ (Exercise 7). To prove $\Rightarrow$, let $\tau = \tau(G)$, $g = g(G)$ and suppose that $\max(G) = 2^{n-g+1}$. Since $\tau \leq n-g+1$ (Exercice 5), we deduce from the feedback bound that $\tau = n-g+1$, that is $n = \tau + g - 1$. Thus either $G \sim C_n$ or $G \sim K_n$ or each vertex of $G$ has a loop (Exercice 6). Suppose that each of $G$ vertex has a loop. Then $g = 1$ thus $\tau = n$ thus $\max(G) = 2^n$ and it is then obvious that $G \sim nC_1$.

9. *Prove that the sphere packing bound is better than the singleton bound for* $5 \leq d < n-1$.

   *Answer.* Let $3 \leq d < n$ be positive integers, and $t = \lfloor (d-1)/2 \rfloor \geq 1$. It is sufficient to prove that $b_t(n) = \sum_{k=0}^{t} \binom{n}{k} > 2^{d-1}$. We essentially use the fact that if $d$ is odd, then $b_t(d) = 2^{d-1}$. Suppose that $d$ is odd. Then

$$\sum_{k=0}^{t}\binom{n}{k} \geq \sum_{k=0}^{t}\binom{d+1}{k} = \sum_{k=0}^{t}\binom{d}{k} + \binom{d}{k-1} = \sum_{k=0}^{t}\binom{d}{k} + \sum_{k=0}^{t-1}\binom{d}{k} \geq 2^{d-1} + 1 > 2^{d-1}.$$

Suppose now that $d$ is even. Since $t \geq 2$ we have

$$\begin{aligned}
\sum_{k=0}^{t}\binom{n}{k} &\geq \sum_{k=0}^{t}\binom{d+2}{k} \\
&= \sum_{k=0}^{t}\binom{d-1}{k} + 3\binom{d-1}{k-1} + 3\binom{d-1}{k-2} + 3\binom{d-1}{k-3} \\
&\geq 2^{d-2} + 3\left(\sum_{k=0}^{t}\binom{d-1}{k-1}\right) + 1 \\
&> 2^{d-2} + 3 \cdot 2^{d-2} - 3\binom{d-1}{t}.
\end{aligned}$$

Thus we only have to prove that

$$3 \cdot 2^{d-2} - 3\binom{d-1}{t} \geq 2^{d-2}$$

which is equivalent to

$$3\binom{d-1}{t} \leq 2^{d-1}.$$

Since

$$2\binom{d-1}{t} + 2\binom{d-1}{t-1} \leq 2^{d-1}$$

it is sufficient to prove that

$$\binom{d-1}{t} \leq 2\binom{d-1}{t-1}$$

and an easy computation shows that this is true if $d \geq 6$.