Infinite Automata 2025/26

Lecture Notes 7

Henry Sinclair-Banks

Theorem 6.5. *Parikh's Theorem.* The Parikh image of any context free language is semilinear.

Proof of Theorem 6.5. Recall from Lecture 6, for a subset of nonterminals X, we defined $L_X \subseteq L$ to be the context free language that contains words in L for which there is a derivation derivation that uses *every* nonterminal in X and no nonterminals not in X. We also defined

$$F \coloneqq \{w \in L_X : |w| < N^k\}, \text{ and}$$
$$G \coloneqq \{x\,y : 1 \leq |x\,y| \leq N^k \text{ and there exists } A \in X : A \overset{*}{\underset{X}{\Rightarrow}} x\,A\,y\}.$$

We also proved that $\psi(L_X) \subseteq \psi(F \cdot G^*)$. It remains to prove that $\psi(F \cdot G^*) \subseteq \psi(L_X)$.

We will prove $\psi(F \cdot G^*) \subseteq \psi(L_X)$ by induction on the minimal number of factors from G that are required to describe an element of $\psi(F \cdot G^*)$. In the base case, if there are zero factors of G, then we know that the word $w \in \psi(F \cdot G^*)$ is actually in $\psi(F)$. Since $F \subseteq L_X$, we know that $\psi(w) \in \psi(L_X)$.

Now, for the inductive step, let us assume that that for all words w that can be described using using n factors in G, that $\psi(w) \in \psi(L_X)$. Consider a word w' that can be represented using $n+1$ factors in G. We know that $\psi(w') = \psi(w) + \psi(xy)$ such that w requires on less factor from G compared to w' and $xy \in G$. By induction, we know that there exists $v \in L_X$ such that $\psi(v) = \psi(w)$. By construction of G, there exists $A \in X$ such that $A \overset{*}{\underset{X}{\Rightarrow}} x\,A\,y$. We also know that because $v \in L_X$, there is a derivation of v that uses the nonterminal $A \in X$: $S \overset{*}{\underset{X}{\Rightarrow}} v_1\,A\,v_3 \overset{*}{\underset{X}{\Rightarrow}} v_1\,v_2\,v_3 = v$. We can therefore insert $A \overset{*}{\underset{X}{\Rightarrow}} x\,A\,y$ into this derivation to obtain the word $v' = v_1\,x\,v_2\,y\,v_3$ and $v' \in L_X$. Here $\psi(v') = \psi(v) + \psi(x\,y) = \psi(w) + \psi(x\,y) = \psi(w')$, which implies that $\psi(w') \in \psi(L_X)$. $\square$

In this lecture, we will proof Pottier's lemma (Lemma 7.2). First, we must first define some terms. A system of d integer linear equations over n variables can be represented as $A\mathbf{x} = \mathbf{b}$, which is the conjunction of equations:

$$a_{1,1}\,x_1 + a_{1,2}\,x_2 + \ldots + a_{1,n}\,x_n = b_1$$
$$\vdots$$
$$a_{d,1}\,x_1 + a_{d,2}\,x_2 + \ldots + a_{d,n}\,x_n = b_n$$

Here $x_1, \ldots, x_n$ are variables over the natural numbers and $a_{i,j}$ are (constant) coefficients over the integers and $b_1, \ldots, b_n$ are also integers. Such a system is *homogeneous* if $\mathbf{b} = \mathbf{0}$.

The following claim allows us to reduce from the the general (homogeneous or non-homogeneous) case to the homogeneous case.

Claim 7.1. Consider the non-homogeneous system of integer linear equations $A\mathbf{x} = \mathbf{b}$ over n variables. Define a new variable x_{n+1} and consider the homogeneous system of integer linear equations $A\mathbf{x} - x_{n+1}\mathbf{b} = \mathbf{0}$. The solution $\mathbf{x} \in \mathbb{N}^n$ is a minimal solution to $A\mathbf{x} = \mathbf{b}$ if and only if $(\mathbf{x}, 1) \in \mathbb{N}^{n+1}$ is a minimal solution to $A\mathbf{x} - x_{n+1}\mathbf{b} = \mathbf{0}$.

The following lemma (Pottier's lemma), lemma tells us that integer linear programs (ILPs) always have "small" solutions. Here "small" refers to the fact that the size of a minimal solution to a given ILP might be exponential in the number of equations. For example, it is possible have a system of equations such as $x_1 = 2x_2$, $x_2 = 2x_3$, $\ldots$, $x_{n-1} = 2x_n$. Here, assuming a non-zero (non-trivial) solution, we require $x_1 = 2^{n-1}x_n$. Nevertheless, we can prove that there all minimal solutions are relatively small.

Lemma 7.2. *Pottier's Lemma.* Let $\mathbf{x} \in \mathbb{N}^n$ be a solution to a n-variable homogeneous system of d integer linear equations with integer coefficients whose absolute values are bounded above by M. If $\mathbf{x}$ is a non-trivial minimal solution, then $\|\mathbf{x}\|_1 \leq (1 + 2Mn)^d$.

Proof. Let $\mathbf{x} \in \mathbb{N}^n$ be a minimal solution to the homogeneous system of integer linear equations. For sake of contradiction, let's assume that $\|\mathbf{x}\|_1 > (1 + 2Mn)^d$. Let $s = \|\mathbf{x}\|_1$.

For the main part of this proof, we will construct a sequence of vectors in $\mathbb{N}^n$: $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_s$. The first vector in this sequence is the zero-vector, so $\mathbf{y}_0 = \mathbf{0} \in \mathbb{N}^n$. The last vector in this sequence is the minimal solution vector $\mathbf{x}$, so $\mathbf{y}_s = \mathbf{x}$. We would also like the sequence of vectors to differ by standard basis vectors; recall $\mathbf{e}_j \in \mathbb{N}^n$ is 1 in the j-th component and 0 on every other component. In other words, for every $k \in \{1, \ldots, s\}$, there exists $j \in \{1, \ldots, n\}$ such that $\mathbf{y}_k - \mathbf{y}_{k-1} = \mathbf{e}_j$. In yet further words, the difference between two consecutive vectors in the sequence is just one on one component and zero on all other components. Notice that it is for this reason why we have $s + 1 = \|\mathbf{x}\|_1 + 1$ many vectors in the sequence.

We would also like to construct a sequence of vectors with the following property. For every $k \in \{1, \ldots, s\}$, there exists $\mathbf{z}_k \in \mathbb{R}^n$ such that $\mathbf{z}_k$ is a *real* solution to the system of d linear equations and such that $\|\mathbf{y}_k - \mathbf{z}_k\|_\infty \leq 1$.

First, consider the closed unit-ball around $\mathbf{y}_0$, that is

$$B_0 \coloneqq \{\mathbf{v} \in \mathbb{R}^n : \|\mathbf{y}_0 - \mathbf{v}\|_\infty \leq 1\}.$$

Observe that the set $B_0 \cap \{\alpha\, \mathbf{x} : \alpha \in [0, 1]\}$ is non-empty. Let $\alpha_0\, \mathbf{x}$ be the point in the intersection of B_0 and the line such that α_0 is maximised. In other words, $\alpha_0\, \mathbf{x}$ is the point on the boundary of the closed unit-ball around $\mathbf{y}_0$ that is on the line of the vector $\mathbf{x}$. Since $\alpha_0\, \mathbf{x}$ is on the boundary of the ball, we know that $\|\mathbf{y}_0 - \alpha_0\, \mathbf{x}\|_\infty = 1$. Also, given that $\mathbf{x} > \mathbf{0}$, we know that there exists at least one component $j \in \{1, \ldots, n\}$ such that $\alpha_0\, \mathbf{x}[j] - \mathbf{y}_0[j] = 1$. We will accordingly define $\mathbf{y}_1 = \mathbf{y}_0 + \mathbf{e}_j$.

Now, consider the closed unit-ball around $\mathbf{y}_1$, that is

$$B_1 \coloneqq \{\mathbf{v} \in \mathbb{R}^n : \|\mathbf{y}_1 - \mathbf{v}\|_\infty \leq 1\}.$$

First, we will argue that $B_1 \cap \{\alpha\, \mathbf{x} : \alpha \in [0, 1]\}$ is non-empty. For this, we will prove that $\alpha_0\, \mathbf{x} \in B_1$. Recall that $\|\mathbf{y}_0 - \alpha_0\, \mathbf{x}\|_\infty \leq 1$ and that $\mathbf{y}_1$ and $\mathbf{y}_0$ only differ on the j-th component. This means that for all $j' \in \{1, \ldots, n\} \setminus \{j\}$, it is true that $\mathbf{y}_1[j'] = \mathbf{y}_0[j']$, so it still holds that $|\mathbf{y}_1[j'] - \alpha_0\, \mathbf{x}[j']| \leq 1$. Furthermore, $j \in \{1, \ldots, n\}$ was selected to be the component such that $\alpha_0\, \mathbf{x}[j] - \mathbf{y}_0[j] = 1$. This implies that $\alpha_0\, \mathbf{x}[j] - \mathbf{y}_1[j] = 0$. Hence $\|\mathbf{y}_1 - \alpha_0\, \mathbf{x}\|_\infty \leq 1$ so $\alpha_0\, \mathbf{x} \in B_1$. Now that we know that the line $\{\alpha\, \mathbf{x} : \alpha \in [0, 1]\}$ intersects B_1, we shall look at the points on the the boundary of the ball that intersect with the line. Let $\beta_1\, \mathbf{x}$ and $\alpha_1\, \mathbf{x}$ be the points in the intersection of B_1 and the line such that β_1 is minimised and α_1 is maximised, respectively. It is true that $\|\mathbf{y}_1 - \beta_1\, \mathbf{x}\|_\infty, \|\mathbf{y}_1 - \alpha_1\, \mathbf{x}\|_\infty = 1$. Since $\mathbf{x} > 0$ (is non-trivial), we know that there exists $j \in \{1, \ldots, n\}$ such that $\alpha_1\, \mathbf{x}[j] - \mathbf{y}_1[j] = 1$. We will accordingly define $\mathbf{y}_2 = \mathbf{y}_1 + \mathbf{e}_j$.

This process repeats and we obtain $\mathbf{y}_3, \mathbf{y}_4, \ldots, \mathbf{y}_s$. Observe that, for every $k \in \{1, \ldots, s\}$, there exists $\mathbf{z}_k \in \mathbb{R}^n$ such that such that $\mathbf{z}_k$ is a solution to the system of d linear equations and $\|\mathbf{y}_k - \mathbf{z}_k\|_\infty \leq 1$. This is because we can choose $\mathbf{z}_k = \alpha_k\, \mathbf{x}$. We get $\|\mathbf{y}_k - \alpha_k\, \mathbf{x}\|_\infty \leq 1$ because $\alpha_k\, \mathbf{x} \in B_k$ and we know that $\alpha_k\, \mathbf{x}$ is a solution because $\mathbf{x}$ is a solution and the system is homogeneous.

Now, we shall consider the differences between "near solutions" $\mathbf{y}_k$ and the solutions in the reals $\mathbf{z}_k$. Since $\|\mathbf{y}_k - \mathbf{z}_k\|_\infty \leq 1$, we know that $|\mathbf{y}_k[j] - \mathbf{z}_k[j]| \leq 1$ for all $j \in \{1, \ldots, n\}$. This means that for all $i \in \{1, \ldots, d\}$ and all $j \in \{1, \ldots, n\}$, $a_{i,j}(\mathbf{y}_k[j] - \mathbf{z}_k[j]) \in [-M, M]$. Thus,

$$-nM \leq a_{1,1}(\mathbf{y}_k[1] - \mathbf{z}_k[1]) + a_{1,2}(\mathbf{y}_k[2] - \mathbf{z}_k[2]) + \ldots + a_{1,n}(\mathbf{y}_k[n] - \mathbf{z}_k[n]) \leq nM,$$

$$\vdots$$

$$-nM \leq a_{d,1}(\mathbf{y}_k[1] - \mathbf{z}_k[1]) + a_{d,2}(\mathbf{y}_k[2] - \mathbf{z}_k[2]) + \ldots + a_{d,n}(\mathbf{y}_k[n] - \mathbf{z}_k[n]) \leq nM.$$

This means that $A\mathbf{y}_k - A\mathbf{z}_k \in [-nM, nM]^d$. Recall that $A\mathbf{z}_k = A(\alpha_k\, \mathbf{x}) = \mathbf{0}$. This means that $A\mathbf{y}_k - A\mathbf{z}_k = A\mathbf{y}_k$, so $A\mathbf{y}_k \in [-nM, nM]^d$.

There are at most $(1+2Mn)^d - 1$ many possible difference choices for $A\mathbf{y}_k$. The -1 is here because we know that for all $k \in \{1, \ldots, s-1\}$, that $\mathbf{y}_k < \mathbf{x}$ and if $A\mathbf{y}_k = \mathbf{0}$, then $\mathbf{y}_k$ would be a non-trivial solution that was smaller than $\mathbf{x}$ (which would contradict the minimality of $\mathbf{x}$). Since we have assumed that $s > (1+2Mn)^d$, we know that (by pigeonhole principle) there exist $k, \ell \in \{1, \ldots, (1+2Mn)^d\}$ such that $k < \ell$ and $A\mathbf{y}_k = A\mathbf{y}_\ell$. This means that $A(\mathbf{y}_\ell - \mathbf{y}_k) = \mathbf{0}$ and $\mathbf{y}_\ell > \mathbf{y}_k$ so $\mathbf{y}_\ell - \mathbf{y}_k > \mathbf{0}$ is a non-trivial solution. Lastly, since $\mathbf{y}_\ell < \mathbf{x}$, we know that $\mathbf{y}_\ell - \mathbf{y}_k < \mathbf{x}$ which means $\mathbf{x}$ is not a minimal solution. With this final contradiction, we conclude that any non-trivial solution $\mathbf{x} \in \mathbb{N}^n$ to this homogeneous system of d integer linear equations must have $\|\mathbf{x}\|_1 \leq (1+2Mn)^d$. □