One-dimensional Integer Sets
**p-ary Expansions**

Given $n \in \mathbb{N}$, its *p-ary expansion* is the word $w \in \{0, 1, \ldots, p-1\}^*$ such that:

$$n = w(0)p^0 + w(1)p^1 + \ldots + w(k)p^k$$

$w$ is denoted also as $(n)_p$. Note that the most significant digit is $w(k)$.

Conversely, to any word $w \in \{0, 1, \ldots, p-1\}^*$ corresponds its value

$$[w]_p = w(0)p^0 + w(1)p^1 + \ldots + w(k)p^k.$$

Notice that $[w]_p = [w0]_p = [w00]_p = \ldots$, i.e. the trailing zeros don’t change the value of a word.
One-dimensional Sets

We consider one-dimensional sets $S \subseteq \mathbb{N}$ coded in base $p$.

*Example 1* Powers of 2 coded in base 2:

<table>
<thead>
<tr>
<th>$n$</th>
<th>$(n)_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100000…</td>
</tr>
<tr>
<td>2</td>
<td>010000…</td>
</tr>
<tr>
<td>4</td>
<td>001000…</td>
</tr>
<tr>
<td>8</td>
<td>000100…</td>
</tr>
<tr>
<td>16</td>
<td>000010…</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
</tr>
</tbody>
</table>
One-dimensional $p$-Automata

A $p$-automaton is a finite automaton over the alphabet $\{0, 1, \ldots, p - 1\}$.

A set $S \subseteq \mathbb{N}$ is said to be $p$-recognizable iff there exists a $p$-automaton $A = (S, q_0, T, F)$ such that $\mathcal{L}(A) = \{w \mid [w]_p \in S\}$.

We assume that any $p$-automaton has a loop $q \xrightarrow{0} q$ for all $q \in F$.

**Example 2** The $2$-automaton recognizing the powers of $2$ is $A = (\{q_0, q_1\}, q_0, \rightarrow, \{q_1\})$ where:

- $q_0 \xrightarrow{0} q_0$
- $q_0 \xrightarrow{1} q_1$
- $q_1 \xrightarrow{0} q_1$
\textit{p-Definability}

Consider the theory \langle \mathbb{N}, +, V_p \rangle, where \( p \in \mathbb{N} \), and \( V_p : \mathbb{N} \to \mathbb{N} \) is:

- \( V_p(0) = 1 \),
- \( V_p(x) \) is the greatest power of \( p \) dividing \( x \).

\langle \mathbb{N}, +, V_p \rangle \) is strictly more expressive than Presburger Arithmetic (why?)

\( P_p(x) \) is true iff \( x \) is a power of \( p \), i.e. \( P_p(x) : V_p(x) = x \).

\( x \in_p y \) is true iff \( x \) is a power of \( p \) and \( x \) occurs in the \( p \)-expansion of \( y \) with coefficient \( 0 \leq j < p \):

\( x \in_{j,p} y : P_p(x) \land [\exists z \exists t . y = z + j \cdot x + t \land z < x \land (t = 0 \lor x < V_p(t))] \)
**p-Definability**

A set $S \subseteq \mathbb{N}$ is *p-definable* iff there exists a first-order formula $\varphi_S(x)$ of $\langle \mathbb{N}, +, V_p \rangle$ such that:

$$x \in S \iff \varphi_S(x) \text{ holds}$$

**Example 3** The set $S$ of powers of 2 is 2-definable:

$$\varphi_S(x) : V_2(x) = x$$
Multi-dimensional Integer Sets
**$p$-Recognizability and $p$-Definability**

Let $(u, v) \in (\{0, 1, \ldots, p - 1\}^2)^*$ be a word, where $u, v \in \{0, 1, \ldots, p - 1\}^*$ such that $|u| = |v|$.

We can pad $u$ and $v$ to the right with 0’s to become equal in length.

**$p$-recognizability**: a $p$-automaton is defined now over $(\{0, 1, \ldots, p - 1\}^2)^*$.

**$p$-definability**: we consider formulae $\varphi_S(x_1, x_2)$ of $\langle \mathbb{N}, +, V_p \rangle$.

The definitions of $p$-recognizability and $p$-definability are easily adapted to the $m$-dimensional case, for any $m > 0$. 
**p-Recognizability and p-Definability**

Consider $T \subseteq \mathbb{N}^2$ defined as:

$$(n, m) \in T \iff \forall k \geq 0 . \, \neg(n)_2(k) \lor \neg(m)_2(k)$$

\[\uparrow m\]

\[
\begin{array}{cccccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{array}
\]
### $p$-Recognizability and $p$-Definability

Consider $T \subseteq \mathbb{N}^2$ defined as:

$$(n, m) \in T \iff \forall k \geq 0 . \neg (n)_2(k) \lor \neg (m)_2(k)$$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$m$</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>00</td>
</tr>
<tr>
<td>11</td>
<td>00</td>
</tr>
<tr>
<td>01</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>01</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>00</td>
<td>11</td>
</tr>
</tbody>
</table>

$$(n)_2 = (4)_2 = 110$$  
$$(m)_2 = (5)_2 = 100$$
\textit{p}-Recognizability and \textit{p}-Definability

Consider $T \subseteq \mathbb{N}^2$ defined as:

\[(n, m) \in T \iff \forall k \geq 0 . \neg(n)_2(k) \lor \neg(m)_2(k)\]

\[\begin{array}{cccccccccccc}
\uparrow m \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{array}\]

\[(n)_2 = (3)_2 = 0 \ 1 \ 1 \]

\[(m)_2 = (4)_2 = 1 \ 0 \ 0 \]
The set $T$ is 2-recognizable.

The set $T$ is 2-definable:

$$\varphi(x_1, x_2) : \forall z . \neg(z \in_2 x_1) \lor \neg(z \in_2 x_2)$$

where

$$x \in_2 y : P_2(x) \land [\exists z \exists t . y = z + x + t \land z < x \land (t = 0 \lor x < V_2(t))]$$
\textbf{\textit{p-}\-Recognizability and \textit{p-}\-Definability}

\textbf{Theorem 1} Let $M \subseteq \mathbb{N}^m$, $m \geq 1$ and $p \geq 2$. Then $M$ is $p$-recognizable if and only if $M$ is $p$-definable.

For any $p$-automaton $A$ there exists a $\langle \mathbb{N}, +, V_p \rangle$-formula $\varphi_A$ which defines $L(A)$.

For any $\langle \mathbb{N}, +, V_p \rangle$-formula $\varphi$ there exists a $p$-automaton $A_\varphi$ such that $L(A)$ is the subset of $\mathbb{N}^m$ defined by $\varphi$. 
From Automata to Formulae

Let \( A = \langle S, q_0, T, F \rangle \) be a \( p \)-automaton.

Suppose \( S = \{ q_0, q_1, \ldots, q_{\ell-1} \} \) and replace w.l.o.g. \( q_k \) by

\[
e_k = \langle 0, \ldots, 0, 1, 0, \ldots, 0 \rangle \in \{0, 1\}^\ell
\]

We build a formula that defines all successful runs of \( A \)

A run is a tuple \( \langle n_1, \ldots, n_m, y_1, \ldots, y_\ell \rangle \) where:

- \( \langle (n_1)_p, \ldots, (n_m)_p \rangle \) is the word read by \( A \)
- \( \langle y_1, \ldots, y_\ell \rangle \) is the sequence of states during the run
From Automata to Formulae

\[ x \in_{j,p} y \text{ iff } x \text{ is a power of } p \text{ and the coefficient of } x \text{ in } (y)_p \text{ is } j: \]

\[ x \in_{j,p} y : P_p(x) \land [\exists z \exists t . y = z + j \cdot x + t \land z < x \land (x < V_p(t) \lor t = 0)] \]

\( \lambda_p(x) \) denotes the greatest power of \( p \) occurring in \( (x)_p \) (\( \lambda_p(0) = 1 \)):

- \( \lambda_p(x) = p^k \), where \( k \) = the minimal length of the \( p \)-expansion of \( x \)

\[ \lambda_p(x) = y : (x = 0 \land y = 1) \lor [P_p(y) \land y \leq x \land \forall z . (P_p(z) \land y < z) \rightarrow (x < z)] \]
From Automata to Formulae

\( \langle (n_1)_p, \ldots, (n_m)_p \rangle \in \mathcal{L}(A) \) iff exists \( y_1, \ldots, y_\ell \in \mathbb{N} \) such that:

- The first state on the run is \( q_0 : \langle (y_1)_p(0), \ldots, (y_\ell)_p(0) \rangle = \langle 1, 0, \ldots, 0 \rangle :\)

  \[
  \varphi_1 : \bigwedge_{j=1}^{\ell} 1 \in q_0(j)_p y_j
  \]

- \( \langle (y_1)_p(k), \ldots, (y_\ell)_p(k) \rangle \) is a final state of \( A \), where \( k \) is greater or equal to the length of all \( p \)-expansions of \( y_i \), i.e. \( z = p^k :\)

  \[
  \varphi_2 : P_p(z) \land \bigwedge_{j=1}^{\ell} z \geq \lambda_p(y_j) \land \bigvee_{q \in F} \bigwedge_{j=1}^{\ell} z \in q(j)_p y_j
  \]
From Automata to Formulae

\[ \langle (n_1)_p, \ldots, (n_m)_p \rangle \in \mathcal{L}(A) \text{ iff exists } y_1, \ldots, y_\ell \in \mathbb{N} \text{ such that:} \]

- for all \(0 \leq i < k:\)

\[
\begin{align*}
\langle (y_1)_p(i), \ldots, (y_\ell)_p(i) \rangle & \xrightarrow{\langle (n_1)_p(i), \ldots, (n_m)_p(i) \rangle} \langle (y_1)_p(i + 1), \ldots, (y_\ell)_p(i + 1) \rangle \\

\varphi_3 & : \ \forall t. P_p(t) \land t < z \land \\
& \bigwedge_{T(q,(a_1,\ldots,a_m))=q'} \left[ \bigwedge_{j=1}^\ell t \in q(j)_p \ y_j \land \bigwedge_{j=1}^m t \in a_j_p \ n_j \rightarrow \bigwedge_{j=1}^\ell p \cdot t \in q'(j)_p \ y_j \right]
\end{align*}
\]
From Formulae to Automata

Build automata for the atomic formulae $x + y = z$ and $V_p(x) = y$, then compose them with union, intersection, negation and projection.

Corollary 1 The theories $\langle \mathbb{N}, +, V_p \rangle$, $p \geq 2$ are decidable.
The Big Picture

Presburger Arithmetic $\subset \langle \mathbb{N}, +, V_p \rangle$

$\upharpoonright \upharpoonleft$

Semilinear Sets $\subset p$-Automata
Base Dependence Theorems
Base Dependence

Definition 1 Two integers \( p, q \in \mathbb{N} \) are said to be multiplicatively dependent if there exist \( k, l \geq 1 \) such that \( p^k = q^l \).

Equivalently, \( p \) and \( q \) are multiplicatively dependent iff there exists \( r \geq 2 \) and \( k, l \geq 1 \) such that \( p = r^k \) and \( q = r^l \) (why?).
**Base Dependence**

**Lemma 1** Let $p, q \geq 2$ be multiplicatively dependent integers. Let $m \geq 1$ and $S \subseteq \mathbb{N}^m$ be a set. Then $S$ is $p$-recognizable iff it is $q$-recognizable.

$p^k$-definable $\Rightarrow$ $p$-definable Let $\phi(x, y) : P_{p^k}^k(y) \land y \leq V_p(x)$.

We have $V_{p^k}(x) = y \iff \phi(x, y) \land \forall z \cdot \phi(x, z) \rightarrow z \leq y$.

We have to define $P_{p^k}$ in $\langle \mathbb{N}, +, V_p \rangle$. 
Base Dependence

\[ P_{p^k}(x) : P_p(x) \land \exists y . \ x - 1 = (p^k - 1)y \]

Indeed, if \( x = p^{ak} \) then \( p^k - 1 | x - 1 \).

Conversely, if assume \( x \) is a power of \( p \) but not of \( p^k \), i.e. \( x = p^{ak + b} \), for some \( 0 < b < k \).

Then \( x - 1 = p^b(p^{ak} - 1) + (p^b - 1) \), and since \( p^k - 1 | x - 1 \), we have \( p^k - 1 | p^b - 1 \), contradiction.
Base Dependence

\( p\)-definable \( \implies p^k\)-definable

\[
V_{p^k}(x) = V_{p^k}(p^{k-1}x) \implies V_p(x) = V_{p^k}(x)
\]
\[
V_{p^k}(x) = V_{p^k}(p^{k-2}x) \implies V_p(x) = pV_{p^k}(x)
\]
\[
\ldots
\]
\[
V_{p^k}(x) = V_{p^k}(px) \implies V_p(x) = p^{k-2}V_{p^k}(x)
\]
else
\[
V_p(x) = p^{k-1}V_{p^k}(x)
\]

Example 4

\[
V_4(x) = V_4(2x) \implies V_4(x) = V_2(x)
\]
\[
V_4(x) \neq V_4(2x) \implies 2V_4(x) = V_2(x)
\]
Theorem 2 (Cobham-Semenov) \( \text{Let } m \geq 1, \text{ and } p, q \geq 2 \) be multiplicatively independent integers. Let \( s : \mathbb{N}^m \rightarrow \mathbb{N} \) be a sequence. If \( s \) is \( p \)-recognizable and \( q \)-recognizable, then \( s \) is definable in \( \langle \mathbb{N}, + \rangle \).

\[
\text{semilinear sets} = \text{\( p \)-recognizable } \cap \text{\( q \)-recognizable}
\]

\[p,q \text{ multiplicatively independent}\]
Exercise

1) Prove that every strictly positive natural number $n \in \mathbb{N}^+$ has a prime factorization. Prove that this factorization is unique.

2) The arithmetic of Skolem is the first order theory of strictly positive natural numbers, with multiplication $\langle \mathbb{N}^+, \cdot \rangle$. Prove the decidability of this theory.