# The $\mu$-calculus and model checking

[J. Bradfield and I. Walukiewicz, Handbook of MC]

<u>So far</u>: Linear-time properties

<u>Now</u>: Branching time.

## Syntax and Semantics:

<u>Transition systems</u> are finite graphs whose transitions are labelled by <u>actions</u> from $Act = \{a, b, c, \dots\}$ and whose states are labelled by <u>propositions</u> from $Prop = \{p_1, p_2, \dots\}$.

Formally,

$$M = (S, \{R_a\}_{a \in Act}, \{P_i\}_{i \in \mathbb{N}})$$

with $R_a \subseteq S \times S$ and $P_i \subseteq S$.

// One can also study the $\mu$-calculus over infinite structures.

### Syntax:

Let $Var = \{X, Y, Z, \dots\}$ be a countable set of variables that will denote sets of states.

The set of $\mu$-calculus formulas $\alpha$ is defined by

$$\alpha ::= p \mid \neg p \mid X \mid \alpha_1 \wedge \alpha_2 \mid \alpha_1 \vee \alpha_2$$
$$\mid \langle a \rangle \alpha \mid [a] \alpha \mid \mu X. \alpha \mid \nu X. \alpha$$

<u>Convention</u>: $\langle a \rangle$ and $[a]$ bind stronger than Boolean connectives.

We write $\sigma X. \alpha$ for $\mu X. \alpha$ or $\nu X. \alpha$.

We write $tt$ for $p_1 \vee \neg p_1$, $ff$ for $p_1 \wedge \neg p_1$.

Example:

$p$ holds infinitely often along some a-path:

$$\nu Y.(\mu X.((p \wedge \langle a\rangle Y) \vee \langle a\rangle X)).$$

We write this as

$$\nu Y.\,\mu X.\,(p \wedge \langle a\rangle Y) \vee \langle a\rangle X.$$

## Semantics:

The meaning of a formula in a transition system is the set of states satisfying the formula.

Definition:

Given a transition system $\mathcal{M} = (S, \{R_a\}_{a\in Act}, \{P_i\}_{i\in\mathbb{N}})$ and a valuation $val : Vars \to \mathcal{P}(S)$, the meaning of formulas $[\![\alpha]\!]^{\mathcal{M}}_{val}$ is defined by induction:

$$[\![X]\!]^{\mathcal{M}}_{val} := val(X)$$

$$[\![p_i]\!]^{\mathcal{M}}_{val} := P_i \qquad [\![\neg p_i]\!]^{\mathcal{M}}_{val} := S \setminus P_i.$$

$$[\![\alpha_1 \underset{\vee}{\wedge} \alpha_2]\!]^{\mathcal{M}}_{val} := [\![\alpha_1]\!]^{\mathcal{M}}_{val} \underset{\cup}{\cap} [\![\alpha_2]\!]^{\mathcal{M}}_{val}$$

// there is an a-transition $\quad [\![\langle a\rangle\alpha]\!]^{\mathcal{M}}_{val} := \{s \in S \mid \exists s'.\, R_a(s,s') \wedge s' \in [\![\alpha]\!]^{\mathcal{M}}_{val}\}$

// for all a-transitions $\quad [\![[a]\alpha]\!]^{\mathcal{M}}_{val} := \{s \in S \mid \forall s'.\, R_a(s,s') \Rightarrow s' \in [\![\alpha]\!]^{\mathcal{M}}_{val}\}.$

To define the semantics of fixed-point operators, we understand a formula $\alpha(X)$ with free variable $X$ as an operator

$$\alpha(X) : \mathbb{P}(S) \longrightarrow \mathbb{P}(S)$$
$$S' \longmapsto [\![\alpha]\!]^{M}_{val[X \mapsto S']} .$$

This operator is monotonic,
so we can rely on Knaster-Tarski.

$$[\![\mu X.\alpha]\!]^{M}_{val} := \bigcap \{ S' \subseteq S \mid [\![\alpha]\!]^{M}_{val[X\mapsto S']} \subseteq S' \}$$

// Meet over all prefix points,
so $\mu X.\alpha$ is the lfp of $\alpha$.

$$[\![\nu X.\alpha]\!]^{M}_{val} := \bigcup \{ S' \subseteq S \mid S' \subseteq [\![\alpha]\!]^{M}_{val[X\mapsto S']} \}$$

// Join over all postfix points,
so $\nu X.\alpha$ is the gfp of $\alpha$.

We write $M, s, val \models \alpha$ for $s \in [\![\alpha]\!]^{M}_{val}$.

<u>Examples:</u>

The way to read a formula

- $\nu X.\alpha$ is there is an <u>infinite</u> set of positions $X$ in the run tree for which $\alpha$ holds.
- $\mu X.\alpha$ is there is a <u>finite</u> set of positions $X$ in the run tree for which $\alpha$ holds.

(1) There is an $\langle a \rangle$-labelled transition: $\langle a \rangle tt$.

(2) Termination, all sequences of $a$-transitions are finite: $\mu X.[a]X$.

To understand that this is the meaning, consider

$M$
$$\begin{tikzcd} & s_1 \\ s \arrow[ur, "a"] \arrow[dr, "a"'] & \\ & s_2 \end{tikzcd}$$

- Is $\emptyset$ a prefix point?

$$[\![[a]X]\!]^{M}_{[X\mapsto \emptyset]}$$
$$= \{ s \in S \mid \forall s'. R_a(s,s') \Rightarrow s' \in \emptyset \}$$
$$= \{ s_1, s_2 \} \not\subseteq \emptyset$$

The least fixed point actually is $\{ s, s_1, s_2 \}$.

(3) Non-termination, there is an infinite sequence of a-transitions: $\nu X. \langle a \rangle X$.

Note that (2) and (3) only need one fixed point.

(4) There is an infinite sequence of a-transitions and all states on the sequence satisfy $p$: $\nu Y. p \wedge \langle a \rangle Y$.

(5) $\mu X. \langle a \rangle X$ is false.

Intuitively, this says that there is a finite set of positions so that from every position in the set one can take an a-transition to a position in the set.

The only finite set for which this holds is $\emptyset$, which is the semantics of false.

All other sets would have to be infinite.

Formally, the empty set is a prefix point:

$$\llbracket \langle a \rangle X \rrbracket^{\mathcal{M}}_{[X \mapsto \emptyset]} = \{ s \in S \mid \exists s'. R_a(s, s') \wedge s' \in \emptyset \}$$

$$= \emptyset \subseteq \emptyset.$$

(6) There is a sequence of a-transitions to a state where $p$ holds: $\mu X. p \vee \langle a \rangle X$.

(7) Two fixed points allow us to define <u>fairness</u>: on some a-path there are infinitely many states where $p$ holds: $\nu Y. \mu X. (p \wedge \langle a \rangle Y) \vee \langle a \rangle X$

(8) On some a-path, <u>almost always</u> $p$ holds: $\mu X. \nu Y. (p \wedge \langle a \rangle Y) \vee \langle a \rangle X$

Note that the fixed points are swapped between (7) and (8).

Why do formulas mean what they mean? Introduce alternative semantics!

The intuitive way of reading nested fixed points like

$$\nu Y.\ \mu X.\ (p \wedge \langle a\rangle Y) \vee \langle a\rangle X$$

> The arrows say: when I arrive at $X$/$Y$, I continue with the formula the arrow leads to.

is to say:

there is an <u>infinite</u> set of positions $Y$ in the run tree

so that <u>for every position</u> $y \in Y$

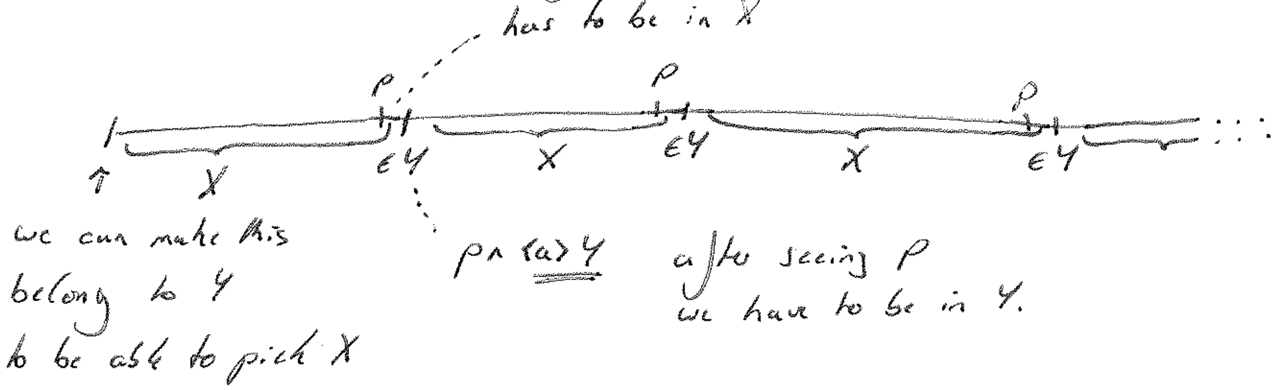
<u>there is a</u> <u>finite</u> <u>set</u> of positions $X_y$

so that $(p \wedge \langle a\rangle Y) \vee \langle a\rangle X$ holds.

So the alternation $\nu Y. \mu X. \alpha$ translates into

for all $y \in Y$ there is a set $X_y$.

We illustrate the meaning on a run (not a tree):




<u>Conventions</u>:

- $\mu X$ and $\nu X$ <u>bind</u> the variable $X$.
- The meaning of $\sigma X. \alpha$ does not depend on the valuation of $X$.
- A formula is <u>closed</u> or a <u>sentence</u>, if it does not contain free variables.
- We write $\alpha[\beta/X]$ to denote the substitution of $\beta$ for every free occurrence of $X$ in $\alpha$.

We assume that the free variables of $\beta$ are disjoint from the bound variables in $\alpha$.

This can always be achieved by renaming bound variables.

$$\sigma Y.\, \alpha \quad \text{is equivalent to} \quad \sigma Z.\, \alpha[Z/Y].$$

- We write $\sigma X.\, \alpha(X)$ to indicate that $\alpha$ depends on the value of $X$.

We write $\alpha(\beta)$ for $\alpha[\beta/X]$.

- A fixed point formula $\sigma X.\, \alpha(X)$ is equivalent to its <u>unfolding</u> $\alpha(\sigma X.\, \alpha(X))$.

This means we can delay reasoning about fixed points.

## Semantics based on approximations:

<u>Idea</u>: Use Kleene's theorem to obtain the meaning of fixed point constructs.

<u>Definition</u>:

$$\mu^0 X.\, \alpha(X) \quad := \emptyset$$

$$\mu^{n+1} X.\, \alpha(X) \quad := \alpha(\mu^n X.\, \alpha(X))$$

$$\mu^\omega X.\, \alpha(X) \quad := \bigcup_{n<\omega} \mu^n X.\, \alpha(X).$$

If $\mu^{k+1} X.\, \alpha(X) = \mu^k X.\, \alpha(X)$, we say the approximation <u>closes</u> <u>at $k$</u>.

<u>Examples</u>:

(1) $\mu^0 X.\, [a]X = \emptyset$ // false

$\mu^1 X.\, [a]X = [a]\emptyset$ // states without a-transitions.

$\mu^2 X.\, [a]X = [a][a]\emptyset$ // states without an aa-path.

(2) $\nu Y.\, \mu X.\, \langle a \rangle ((p \wedge Y) \vee X)$

// along some a-path there are infinitely many states where $p$ holds.

We have to calculate the approximation of $\mu$ relative to the current approximation of $\nu$.

Let $\nu^i$ represent $\nu^i Y.\, \mu X.\, \langle a \rangle ((p \wedge Y) \vee X)$

$\mu^{i,j}$ represent $\mu^j X.\, \langle a \rangle ((p \wedge Y) \vee X)[\nu^i / Y]$

$\nu^0 \qquad S$

$\mu^{0,0} \qquad \emptyset$

$\mu^{0,1} \qquad [\![ \langle a \rangle ((p \wedge S) \vee \mu^{0,0}) ]\!] = [\![ \langle a \rangle p ]\!]$

$\mu^{0,2} \qquad [\![ \langle a \rangle ((p \wedge S) \vee \mu^{0,1}) ]\!] = [\![ \langle a \rangle (p \vee \langle a \rangle p) ]\!]$

$\vdots$

$\nu^1 = \mu^{0,\infty} \qquad \langle a \rangle$- eventually $p$

$\mu^{1,1} \qquad [\![ \langle a \rangle ((p \wedge \nu^1) \vee \emptyset) ]\!] = [\![ \langle a \rangle (p \wedge \nu^1) ]\!]$

$\mu^{1,2} \qquad [\![ \langle a \rangle ((p \wedge \nu^1) \vee \mu^{1,1} ]\!] = [\![ \langle a \rangle ((p \wedge \nu^1) \vee \langle a \rangle (p \wedge \nu^1) ]\!]$

$\vdots$

$\nu^2 = \mu^{1,\infty} \qquad \langle a \rangle$- eventually ($p \wedge \langle a \rangle$- eventually $p$)

$\vdots$

$\nu^\infty \qquad$ infinitely often $p$.

## Negation:

Our logic does not have negation.
We now define negation as a derived operator and then show that it has the required properties:

$\neg(\neg p) := p \qquad \neg(\neg X) := X$

$\neg(\alpha \vee \beta) := \neg\alpha \wedge \neg\beta \qquad \neg(\alpha \wedge \beta) := \neg\alpha \vee \neg\beta.$

$\neg\langle a\rangle\alpha \; := \; [a]\neg\alpha$ $\qquad$ $\neg[a]\alpha := \langle a\rangle\neg\alpha.$

$\neg\mu X.\alpha(X) \; := \; \nu X.\neg\alpha(\neg X)$ $\qquad$ $\neg\nu X.\alpha(X) := \mu X.\neg\alpha(\neg X).$

the two negations
cancel out

Lemma:

For every formula $\alpha$, transition system $\mathcal{M}$ with states $S$,
and every valuation val,

$$[\![\neg\alpha]\!]^{\mathcal{M}}_{val} = S \setminus [\![\alpha]\!]^{\mathcal{M}}_{val}.$$

Example:

$$\neg\underbrace{\nu X.\, p \wedge [a]X}_{\text{everywhere always } p} = \mu X.\neg(p \wedge [a]\neg X)$$

$$= \mu X.\, \neg p \vee \neg[a]\neg X$$

$$= \underbrace{\mu X.\, \neg p \vee \langle a\rangle X}_{\text{eventually somewhere } \neg p \text{ holds.}}$$

Normal Forms:

Well-named:
- Bound and free variables are disjoint
- Variables are bound at most once.
- One can even assume variables appear at most once.

  How? $\mu X.\alpha(X,X)$ is equivalent to $\mu X.\mu Y.\alpha(X,Y)$.

One can also convert a formula
into a guarded one
where every occurrence of a variable
is preceded by a modality.
We will not need this and it may cause an exponential blow-up.

Alternation Depth

Insight: The nesting of the two fixed point operators
is what makes the expressiveness of the $\mu$-calculus.

<u>Goal</u>: Make this nesting formal.

Let $\alpha$ be a well-named formula,

so for every variable $Y$

we have a unique subformula $\sigma Y. \beta_Y$.

We call $Y$ a $\mu$-variable or $\nu$-variable depending on $\sigma$.

<u>Definition</u>:

- The <u>dependency order</u> on the bound variables of $\alpha$ is the smallest partial order so that

$$X \leq_\alpha Y, \text{ if } X \text{ occurs free in } \sigma Y. \beta_Y.$$

- The <u>alternation depth of a $\mu$-variable $X$</u> is the maximal length of a chain

$$X = X_1 \leq_\alpha X_2 \leq_\alpha X_3 \leq_\alpha X_4 \leq_\alpha \dots \leq_\alpha X_n$$

$\mu$-variables $\nu$-variables.

For $\nu$-variables, the definition is similar.

- The <u>alternation depth of $\alpha$</u>, adepth($\alpha$), is the maximal alternation depth of the variables bound in $\alpha$.

It is 0 if there are no fixed points.

<u>Example</u>:

- $\alpha = \nu Y. \mu X. (p \wedge \langle a \rangle Y) \vee \langle a \rangle X$ // There are infinitely many states where $p$ holds.

Then adepth$(\alpha) = 2$ since $Y \leq_\alpha X$,

$Y$ is a $\nu$-variable, and

$X$ is a $\mu$-variable.

- $\alpha = \mu X. (\nu Y. (p \wedge \langle a \rangle Y) \wedge \langle a \rangle X)$

  There is a path where $p$ holds almost always.

  We have $\operatorname{adepth}(\alpha) = 1$,

  because $X$ does not occur in $\nu Y. \, p \wedge \langle a \rangle Y$.

Fact: $\operatorname{adepth}(\sigma X. \beta(X)) = \operatorname{adepth}(\beta(\sigma X. \beta(X)))$.

Why? The dependency order of $\beta(\sigma X. \beta(X))$ is the dependency order of $\sigma X. \beta(X)$ plus (disjoint union) the order of $\beta(X)$.
The number of alternations in $\beta(X)$ is bounded by the number of alternations in $\sigma X. \beta(X)$.

## Verification Game

Goal: Understand when a $\mu$-calculus sentence $\alpha$ holds in a state $s$ of $M$.

Approach: Characterize this by the existence of a winning strategy in a game $G(M, \alpha)$:

$M, s \models \alpha$ iff Eve has a winning strategy from a position corresponding to $s$ and $\alpha$.

Idea: (1)

$\boxed{s \models^{?} [a](p_1 \vee (p_2 \wedge p_3))}$ ... Adam node

$\swarrow$ ... for all $t$, $s \xrightarrow{a} t$

$t \models^{?} p_1 \vee (p_2 \wedge p_3)$ ... Eve node

$\swarrow$ $t \models^{?} p_1$ — Owner depends on where $p_1$ holds

$\searrow$ $\boxed{t \models^{?} p_2 \wedge p_3}$

$\swarrow$ $t \models^{?} p_2$ $\searrow$ $t \models^{?} p_3$

(2) Owner does not matter .... $s \models^? \underbrace{\nu Y.\ \underline{\mu Z.\ [a](Z \vee (p \wedge Y))}_{\alpha_Z}}_{\alpha_Y}$

$$\downarrow$$

$$s \models^? \mu Z.\ [a](Z \vee (p \wedge \alpha_Y))$$

$$\downarrow$$

$$\boxed{s \models^? [a](\alpha_Z \vee (p \wedge \alpha_Y))}$$

$\swarrow$ ... for all $t : s \xrightarrow{a} t$

$$t \models^? \alpha_Z \vee (p \wedge \alpha_Y)$$

$$\swarrow \qquad\qquad \searrow$$

$$t \models^? \mu Z.[a](Z \vee (p \wedge \alpha_Y)) \qquad \boxed{t \models^? p \wedge \alpha_Y}$$

$$\swarrow \qquad \searrow$$

$$t \models^? p \qquad t \models^? \nu Y.\mu X.\ [a](Z \vee (p \wedge Y)).$$

A play will be winning for Eve,
if it passes infinitely often through $\alpha_Y$.
This is captured by a parity winning condition.

## Intermezzo: Games

A game is a structure

$$G = (V = V_A \uplus V_E,\ T \subseteq V \times V,\ Acc \subseteq V^\omega).$$

The vertices $V$ are called positions,
the transitions $T$ are called moves.
A play is a maximal sequence in $V^* \uplus V^\omega$
that respects $T$.

If the play is finite, $v_0 v_1 \dots v_n$,

the player who cannot make a move loses

and the opponent wins.

If the play is infinite, $v_0 v_1 \dots$,

Eve wins and Adam loses if $v_0 v_1 \dots \in Acc$,

otherwise Adam wins and Eve loses.

A strategy for player $P \in \{E, A\}$ is a function

$$\theta : V^* . V_P \longrightarrow V$$

that respects $T$, meaning $\theta(\sigma . v) = v'$ implies $(v, v') \in T$.

The strategy is positional, if the history of the play does not matter:

$$\theta(\sigma . v) = \theta(\sigma' . v) \quad \text{for all } \sigma, \sigma' \in V^*.$$

The strategy is winning (for player $P$) from position $v \in V$,

if every play starting in $v$

that respects the strategy is winning for $P$.

A position $v \in V$ is winning,

if there is a strategy that is winning from that position.

We consider parity winning conditions.

Let $\Omega : V \longrightarrow \{0, \dots, d\}$.

Then $Acc := \{ \sigma = v_0 v_1 \dots \in V^\omega \mid \limsup_{i \to \infty} \Omega(v_i) \text{ is even} \}$

$\qquad\qquad \shortparallel$

$\inf \{ \sup \{ \Omega(v_k) \mid k \geq i \} \mid i \in \mathbb{N} \}$

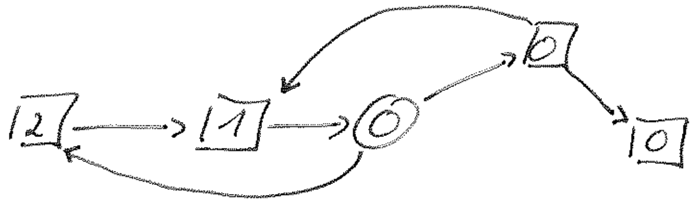
$\qquad\qquad \shortparallel$

largest number that occurs infinitely often is even.

Theorem:

Every position in a parity game is winning for Adam or Eve (but not for both).
It is in $NP \cap co\text{-}NP$ to check whether a position is winning for a player.

Example:



Adam loses here and Eve wins.

Also all other positions are winning for Eve.

## Back to the verification game:

Positions in $G(M, \alpha)$ are of the form $(s, \beta)$,
where
- $s$ is a state in $M$ and
- $\beta$ is a formula in the closure of $\alpha$:
  the smallest set containing $\alpha$ and closed under
  - subformulas and
  - unfolding.

Ownership and Moves:

(1) $\boxed{(s, p)}$, if $s \in p$ // Adam loses as there are no moves

$(s, p)$, if $s \notin p$ // Eve loses

$(s, \neg p)$, if $s \in p$ // Eve loses

$\boxed{(s, \neg p)}$, if $s \notin p$ // Adam loses

(2) $(s, \alpha \vee \beta)$ $\qquad$ $\boxed{(s, \alpha \wedge \beta)}$

$\swarrow \quad \searrow \qquad\qquad \swarrow \quad \searrow$

$(s, \alpha) \quad (s, \beta) \qquad\qquad (s, \alpha) \quad (s, \beta)$

(3) $(s, \langle a \rangle \beta)$ $\qquad\qquad\qquad\qquad$ $\boxed{(s, [a]\beta)}$

$\swarrow$ ... for all $t : s \xrightarrow{a} t$ $\qquad\qquad$ $\swarrow$ ... for all $t : s \xrightarrow{a} t$

$(t, \beta)$ $\qquad\qquad\qquad\qquad\qquad\qquad$ $(t, \beta)$

Note that Eve loses resp. wins if there are no a-transitions.

(4) $(s, \mu X. \beta(X))$ ... Owner does not matter ... $(s, \nu X. \beta(X))$

$\downarrow$ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\downarrow$

$(s, \beta(\mu X. \beta(X)))$ $\qquad\qquad\qquad\qquad$ $(s, \beta(\nu X. \beta(X)))$

## Priorities:

We focus on formulas whose topmost operator is a fixed point.

Starting with $\mu$, we give odd priorities,
starting with $\nu$, we give even priorities,
if $\gamma$ is a subformula of $\beta$, then $\gamma$ should get smaller priorities.

$$\Omega((s, \nu X. \gamma(X))) := 2 \cdot \left\lfloor \frac{\mathrm{adepth}(X)}{2} \right\rfloor$$

$$\Omega((s, \mu X. \gamma(X))) := 2 \cdot \left\lfloor \frac{\mathrm{adepth}(X)}{2} \right\rfloor + 1.$$

$$\Omega((s, \gamma)) := 0 \quad , \quad \text{otherwise}.$$

## Examples:

$\Omega(\nu X. p \wedge [a]X) = 0$

$\Omega(\mu X. p \vee [a]X) = 1$

$\Omega(\mu X. (\nu Y. (p \wedge \langle a \rangle Y) \vee \langle a \rangle X)) = 1$

$\Omega(\nu Y. \mu X. (p \wedge \langle a \rangle Y) \vee \langle a \rangle X) = 2.$

**Theorem (Reducing model checking to parity games):**

$\mathcal{M}, s \models \alpha$ iff Eve has a winning strategy from $(s, \alpha)$ in $G(\mathcal{M}, \alpha)$.

If $\mathcal{M}$ has size $m$ and $\alpha$ size $n$, then $G(\mathcal{M}, \alpha)$ has size $O(m \cdot n)$.
The number of priorities in $G(\mathcal{M}, \alpha)$ is at most adepth$(\alpha)+1$.
But there will be at most adepth$(\alpha)$-many priorities in each strongly connected component of $G(\mathcal{M}, \alpha)$,
so solving the game is not harder than for adepth$(\alpha)$-many priorities.

We will now give a reduction from parity games to model checking.

**Definition:**
Let $G = (V = V_E \uplus V_A, T \subseteq V \times V, \Omega)$ be a parity game with priorities $0, \dots, 2d+1$.
The induced transition system is
$$\mathcal{M}_G := (V, R_b := T, (P_i)_{i \in \mathbb{P}}).$$
Here, $\mathbb{P} = \{\text{Eve}, \text{Adam}, 0, \dots, 2d+1\}$
and $P_{Eve} = V_E$ $\quad P_i = \Omega^{-1}(i) = \{v \in V \mid \Omega(v) = i\}$.
$P_{Adam} = V_A$

**Theorem (Reducing parity games to model checking):**
Given a parity game $G$, we can compute $\mathcal{M}_G$ and a $\mu$-calculus sentence $\alpha$ so that for every position $s$:

$s$ is winning for Eve in $G$ iff $\mathcal{M}_G, s \models \alpha$.

The size of $M_G$ is linear in the size of $G$.

The size of $\alpha$ is linear in the number of priorities of $G$.

The alternation depth of $\alpha$ is at most the number of priorities.

Proof:

We give a formula that characterizes Eve's winning positions, actually, in every game with the given number of priorities.

Let the priorities in $G$ be $0$ to $2d+1$.

The formula is

$$\mu Z_{2d+1} . \nu Z_{2d} . \mu Z_{2d-1} \ldots \nu Z_0 . \gamma(Z_0, \ldots, Z_{2d+1})$$

with

$$\gamma(Z_0, \ldots, Z_{2d+1}) := \bigwedge_{i=0,\ldots,2d+1} p_i \Rightarrow [(p_{Eve} \wedge \langle b \rangle Z_i) \vee (p_{Adam} \wedge [b] Z_i)].$$