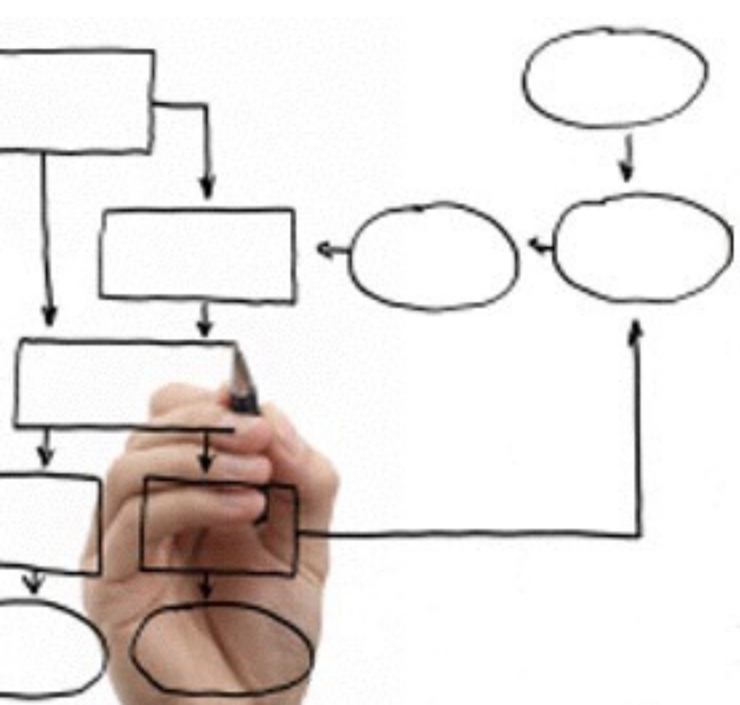
Methods for the specification and verification of business processes

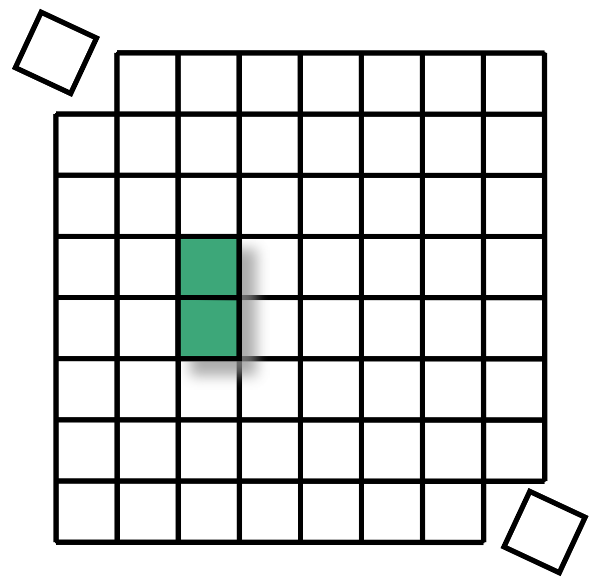
MPB (6 cfu, 295AA)

Roberto Bruni
http://www.di.unipi.it/~bruni



11 - Invariants

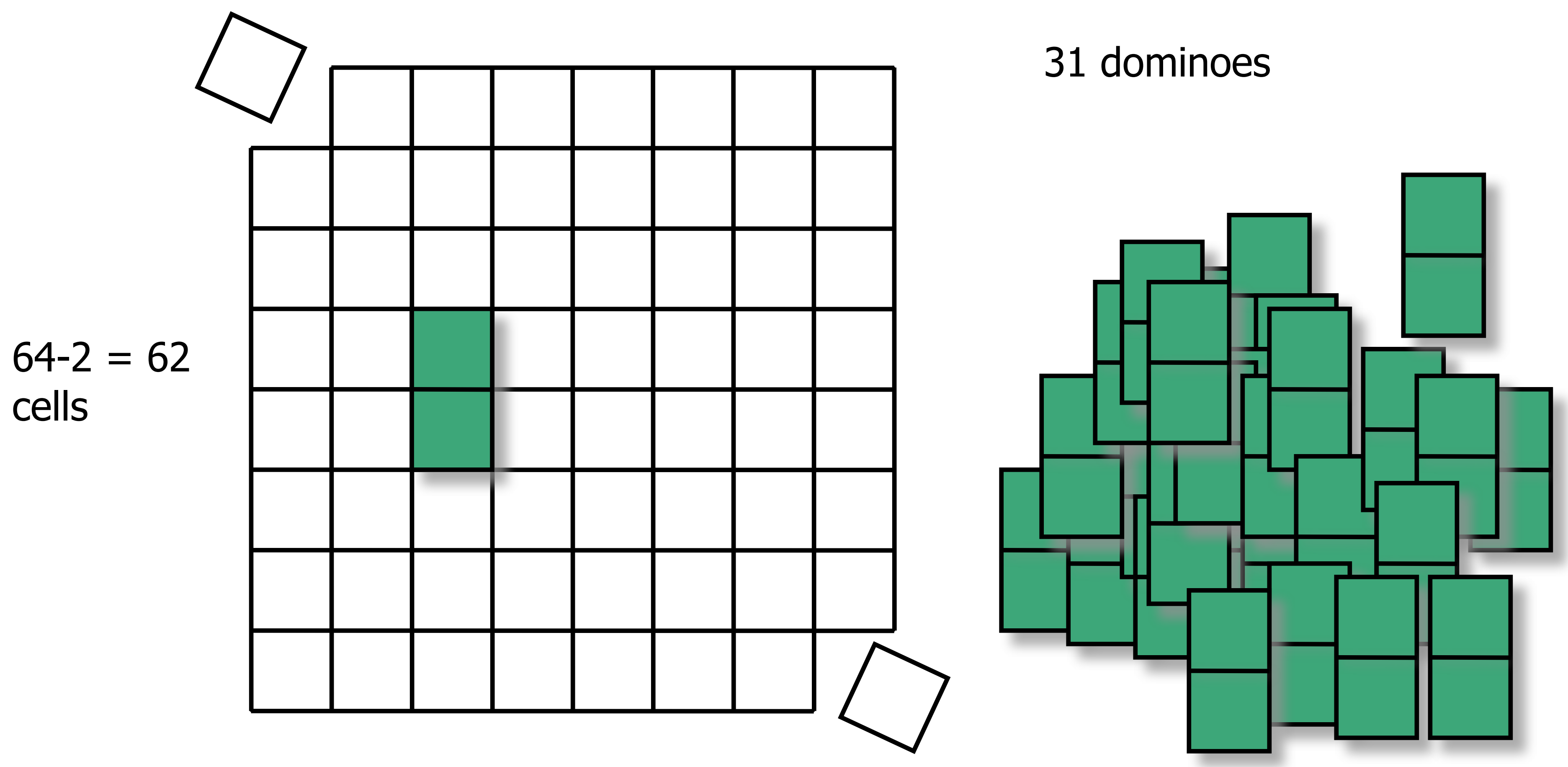
Object



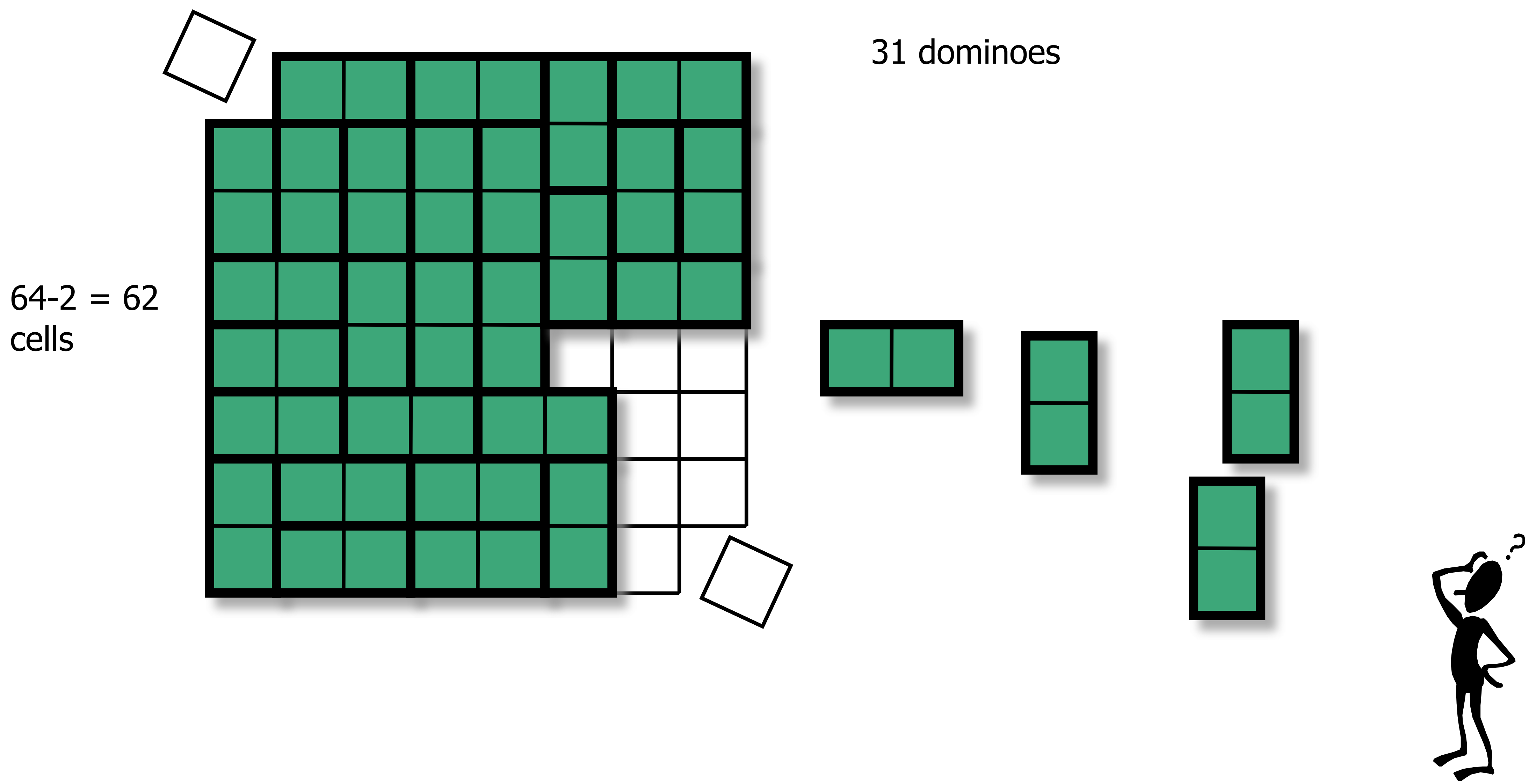
We introduce two relevant kinds of invariants for Petri nets

Free Choice Nets (book, optional reading)
https://www7.in.tum.de/~esparza/bookfc.html

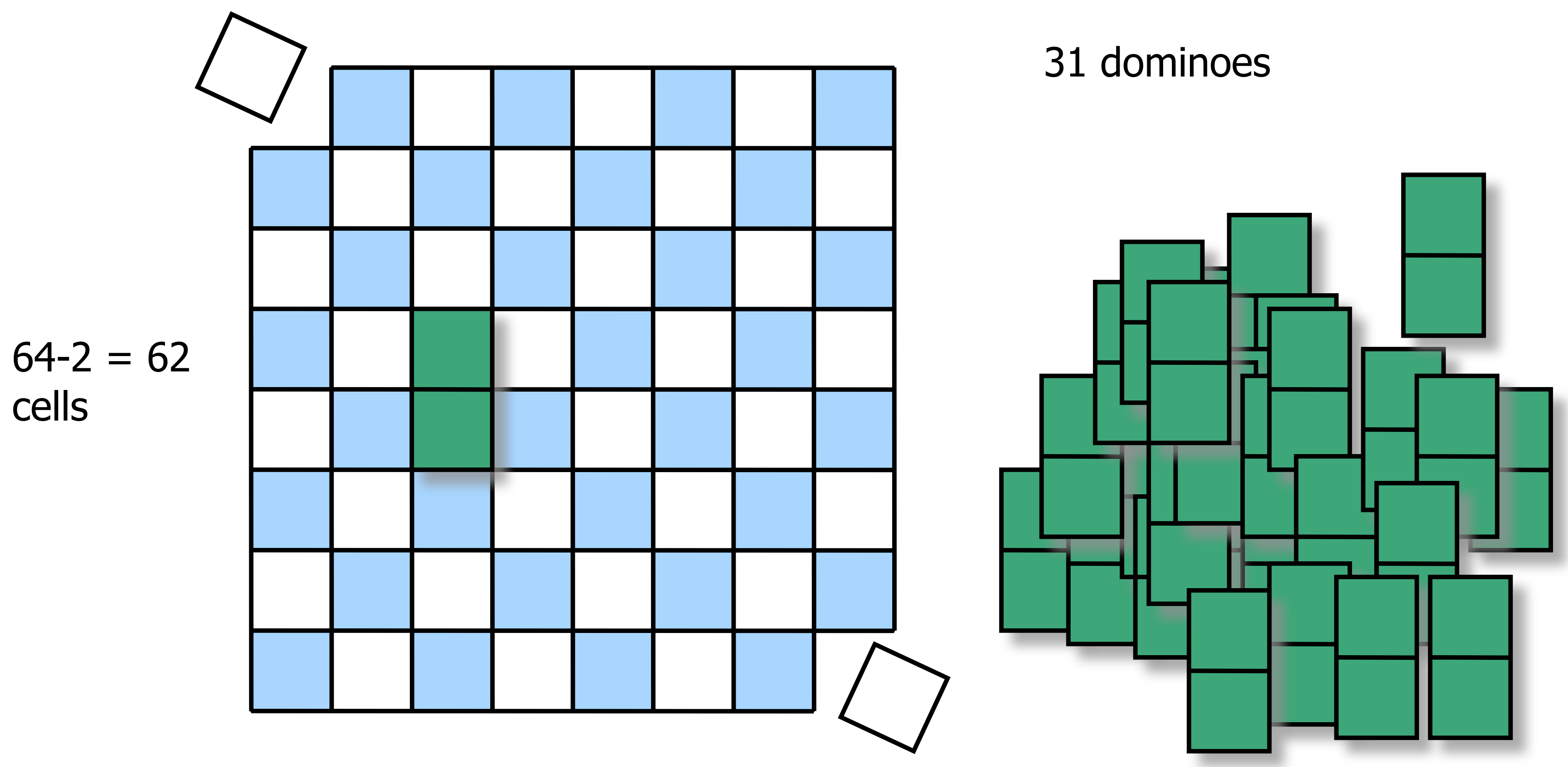
Puzzle time: tiling a chessboard with dominoes



Puzzle time: tiling a chessboard with dominoes



Puzzle time: tiling a chessboard with dominoes



Puzzle: from MI to MU

You can compose words using symbols **M**, **I**, **U**

Given the initial word **MI**, you can apply the following transformations, in any order, as many times as you like:

1. Add a **U** to the end of any string ending in **I** (e.g., **MI** to **MIU**).
2. Double the string after the **M** (e.g., **MIU** to **MIUIU**).
3. Replace any **III** with a **U** (e.g., **MUIIIU** to **MUUU**).
4. Remove any **UU** (e.g., **MUUU** to **MU**).

Can you transform **MI** to **MU**?
(*Hint*: count the **I**s modulo 3)

Invariant

An invariant of a dynamic system is an assertion that holds at every reachable state

Examples:
liveness of a transition t
deadlock freedom
boundedness

Recall: Liveness, formally

$$(P, T, F, M_0)$$

$$\forall t \in T, \quad \forall M \in [\, M_0 \,\rangle, \quad \exists M' \in [\, M \,\rangle, \quad M' \xrightarrow{t}$$

Liveness as invariant

Lemma
If (P, T, F, M_0) is live and $M \in [\, M_0 \,\rangle$, then (P, T, F, M) is live.

Let $t \in T$ and $M' \in [\, M \,\rangle$.

Since $M \in [\, M_0 \,\rangle$, then $M' \in [\, M_0 \,\rangle$.

Since (P, T, F, M_0) is live, $\exists M'' \in [\, M' \,\rangle$ with $M'' \xrightarrow{t}$.

Therefore (P, T, F, M) is live.

Recall: Deadlock freedom, formally

$$(P, T, F, M_0)$$

$$\forall M \in [\, M_0 \,\rangle, \quad \exists t \in T, \quad M \xrightarrow{t}$$

Deadlock freedom as invariant

Lemma: If (P, T, F, M_0) is deadlock-free and $M \in [\, M_0 \,\rangle$, then (P, T, F, M) is deadlock-free.

Let $M' \in [\, M \,\rangle$.

Since $M \in [\, M_0 \,\rangle$, then $M' \in [\, M_0 \,\rangle$.

Since (P, T, F, M_0) is deadlock-free, $\exists t \in T$ with $M' \xrightarrow{t}$.

Therefore (P, T, F, M) is deadlock-free.

Exercise

Give the formal definition of Boundedness

Then prove that Boundedness is an invariant

Or give a counter-example

Exercise

Give the formal definition of Cyclicity

Then prove that Cyclicity is an invariant

Or give a counter-example

Structural invariants

In the case of Petri nets, it is possible to compute
certain vectors of **rational** numbers(*)
(directly from the structure of the net)
(independently from the initial marking)
which induce nice invariants, called

S-invariants

T-invariants

(*) it is not necessary to consider real-valued solutions, because incidence matrices only have integer entries

Why invariants?

Can be calculated efficiently
(polynomial time for a basis)

Independent of initial marking

Structural property with behavioural consequences

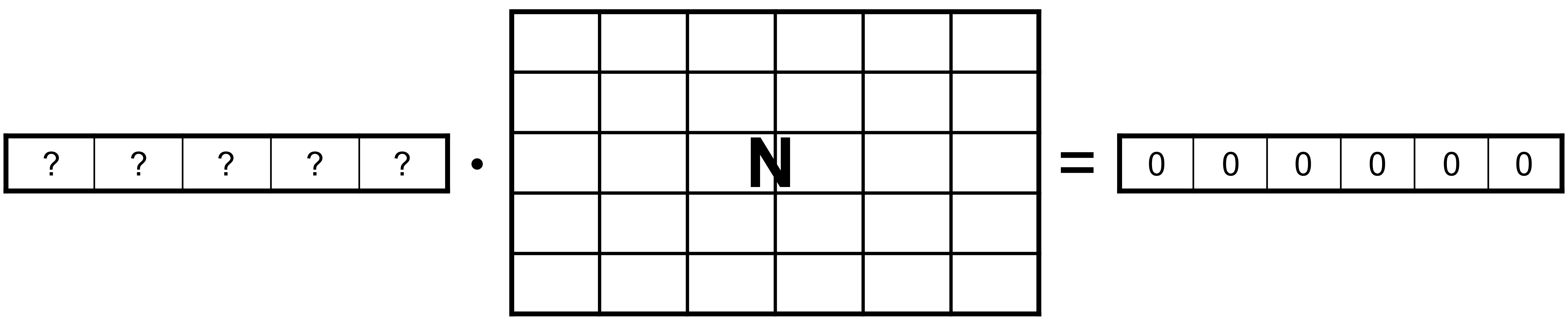
However, the main reason is didactical!
You only truly understand a model if you think
about it in terms of invariants!

S-invariants

S-invariant
(aka place-invariant)

Definition: An **S-invariant** of a net N=(P,T,F) is a rational-valued solution **x** of the equation

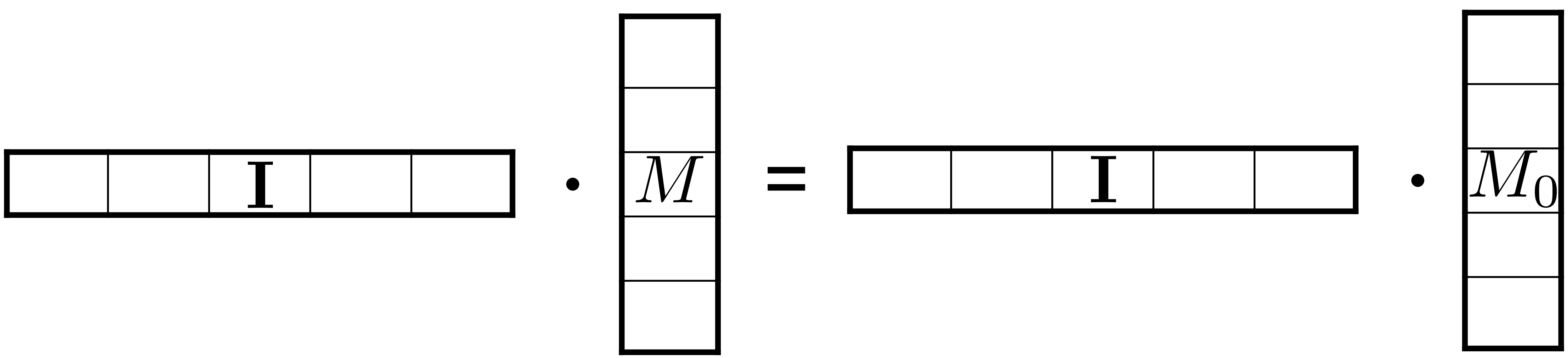
$$\mathbf{x} \cdot \mathrm{N} = \mathbf{0}$$



Fundamental property of S-invariants

Proposition: Let $\mathbf{I}$ be an invariant of N.

For any $M \in [\, M_0 \,\rangle$ we have $\mathbf{I} \cdot M = \mathbf{I} \cdot M_0$



Fundamental property of S-invariants

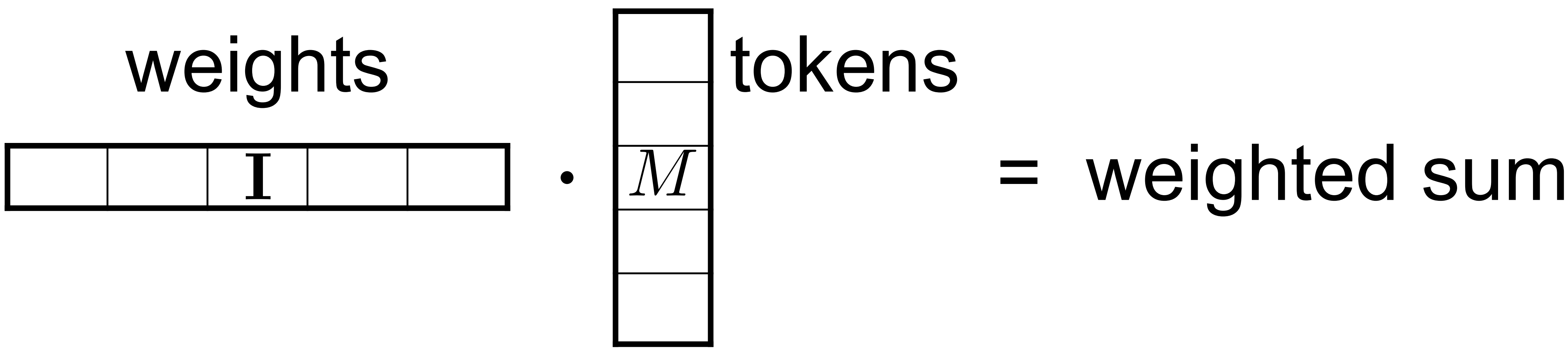
Proposition: Let $\mathbf{I}$ be an invariant of N.

For any $M \in [\, M_0 \,\rangle$ we have $\mathbf{I} \cdot M = \mathbf{I} \cdot M_0$

Since $M \in [\, M_0 \,\rangle$, there is σ s.t. $M_0 \xrightarrow{\sigma} M$
By the marking equation: $M = M_0 + \mathbf{N} \cdot \vec{\sigma}$

$$\begin{aligned} \text{Therefore:} \quad \mathbf{I} \cdot M &= \mathbf{I} \cdot (M_0 + \mathbf{N} \cdot \vec{\sigma}) \\ &= \mathbf{I} \cdot M_0 + \mathbf{I} \cdot \mathbf{N} \cdot \vec{\sigma} \\ &= \mathbf{I} \cdot M_0 + \mathbf{0} \cdot \vec{\sigma} \\ &= \mathbf{I} \cdot M_0 \end{aligned}$$

Place-invariant, intuitively



Place-invariant, intuitively

A place-invariant assigns a **weight to each place** such that the weighted token sum remains constant during any computation

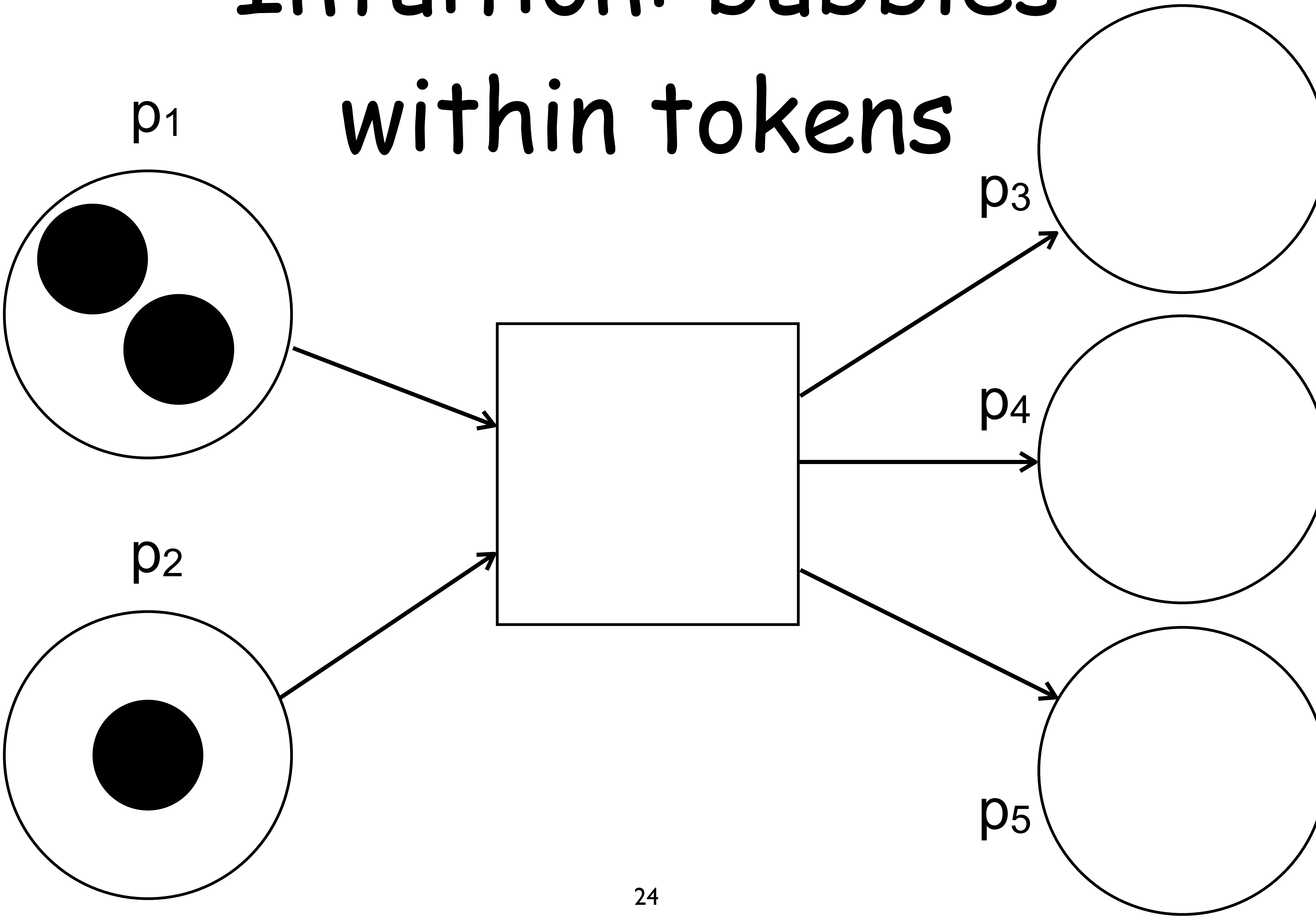
For example, you can imagine that tokens are coins,
places are the different kinds of available coins,
the S-invariant assigns a value to each coin:
the value of a marking is the sum of the values of the tokens/coins in it and it is not changed by firings

Place-invariant, intuitively

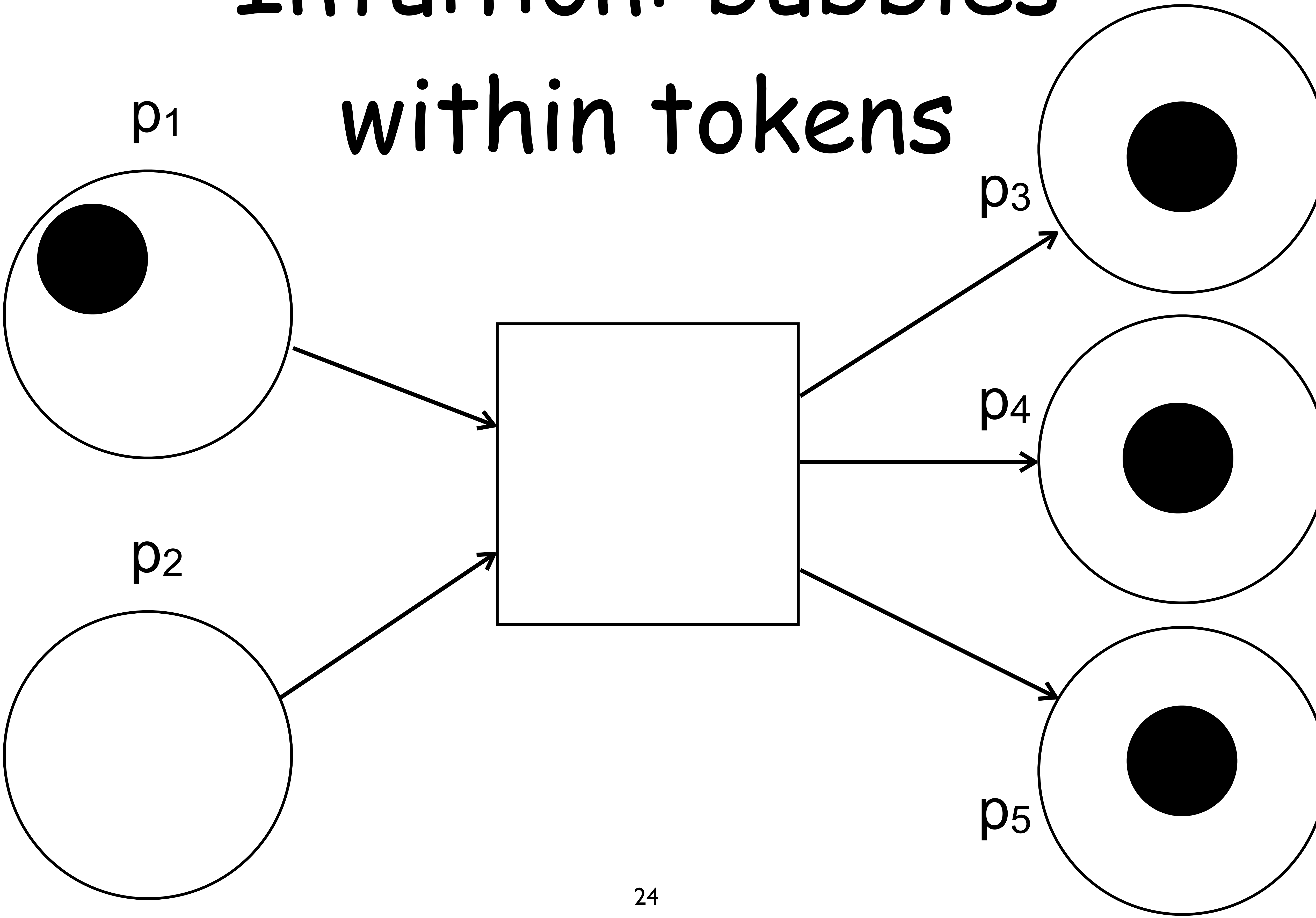
A place-invariant assigns a **weight to each place** such that the weighted token sum remains constant during any computation

For example, you can imagine that tokens are molecules,
places are different kinds of molecules,
the S-invariant assigns the number of atoms needed to form each molecule:
the overall number of atoms is not changed by firings

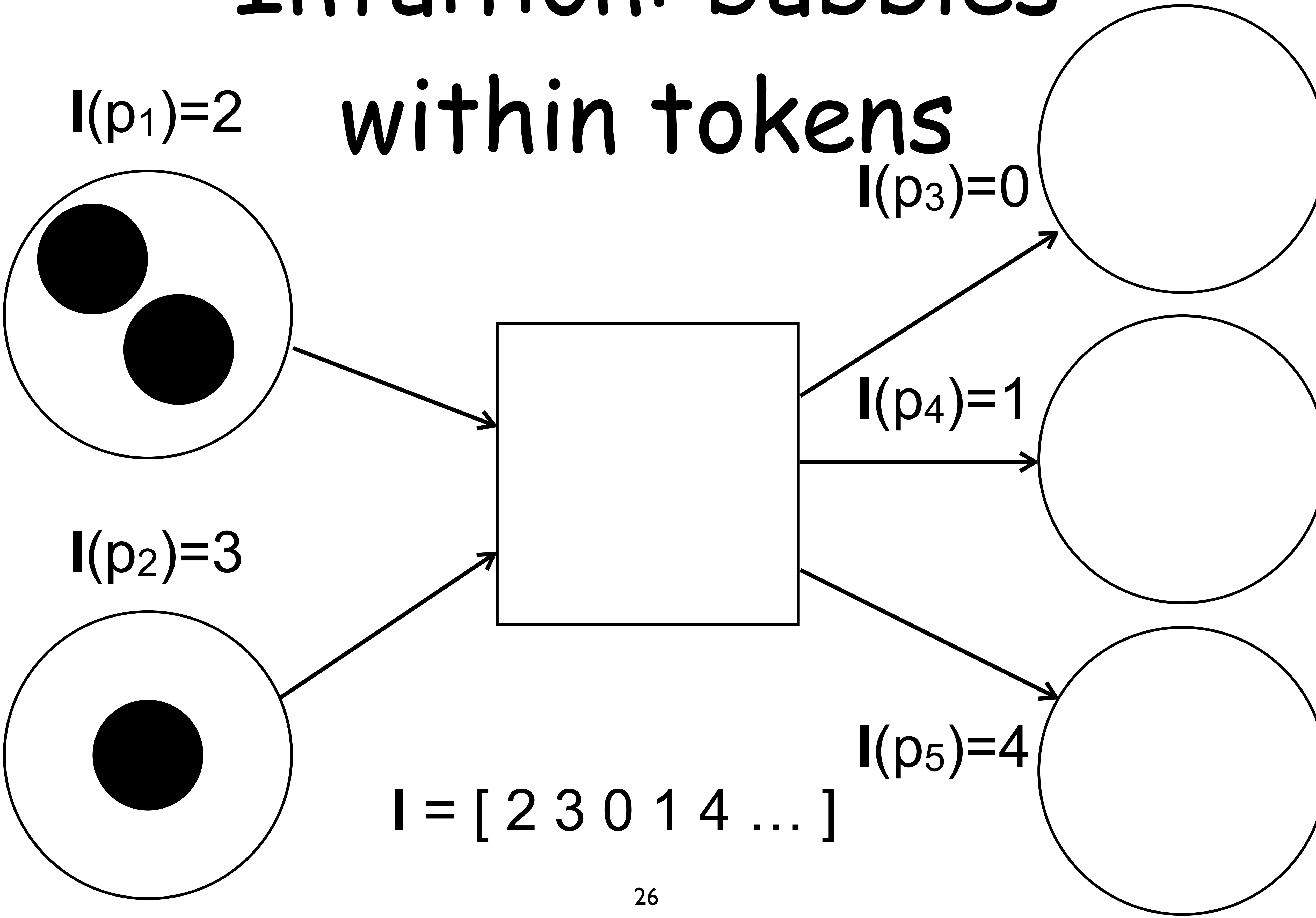
Intuition: bubbles within tokens



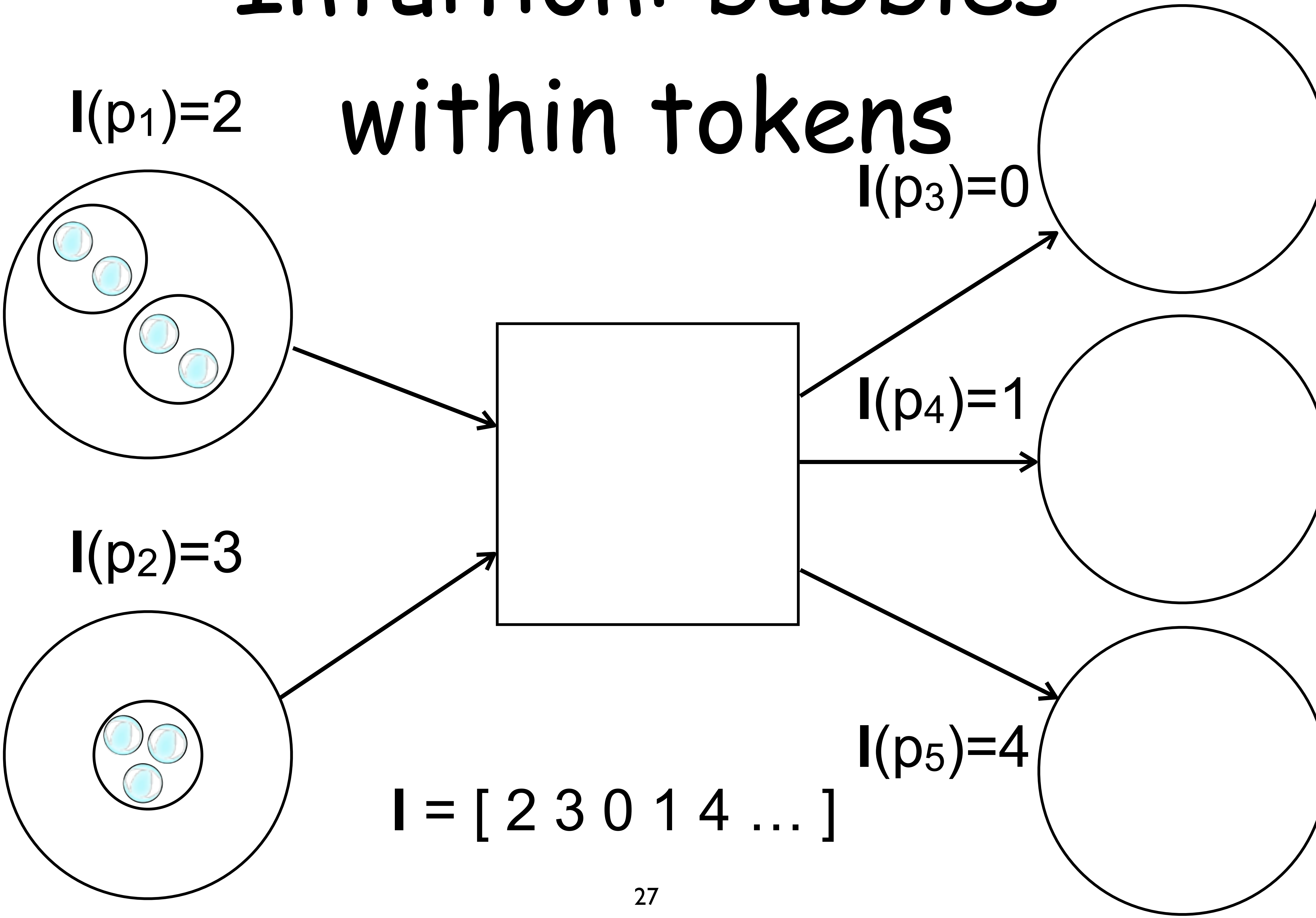
Intuition: bubbles within tokens



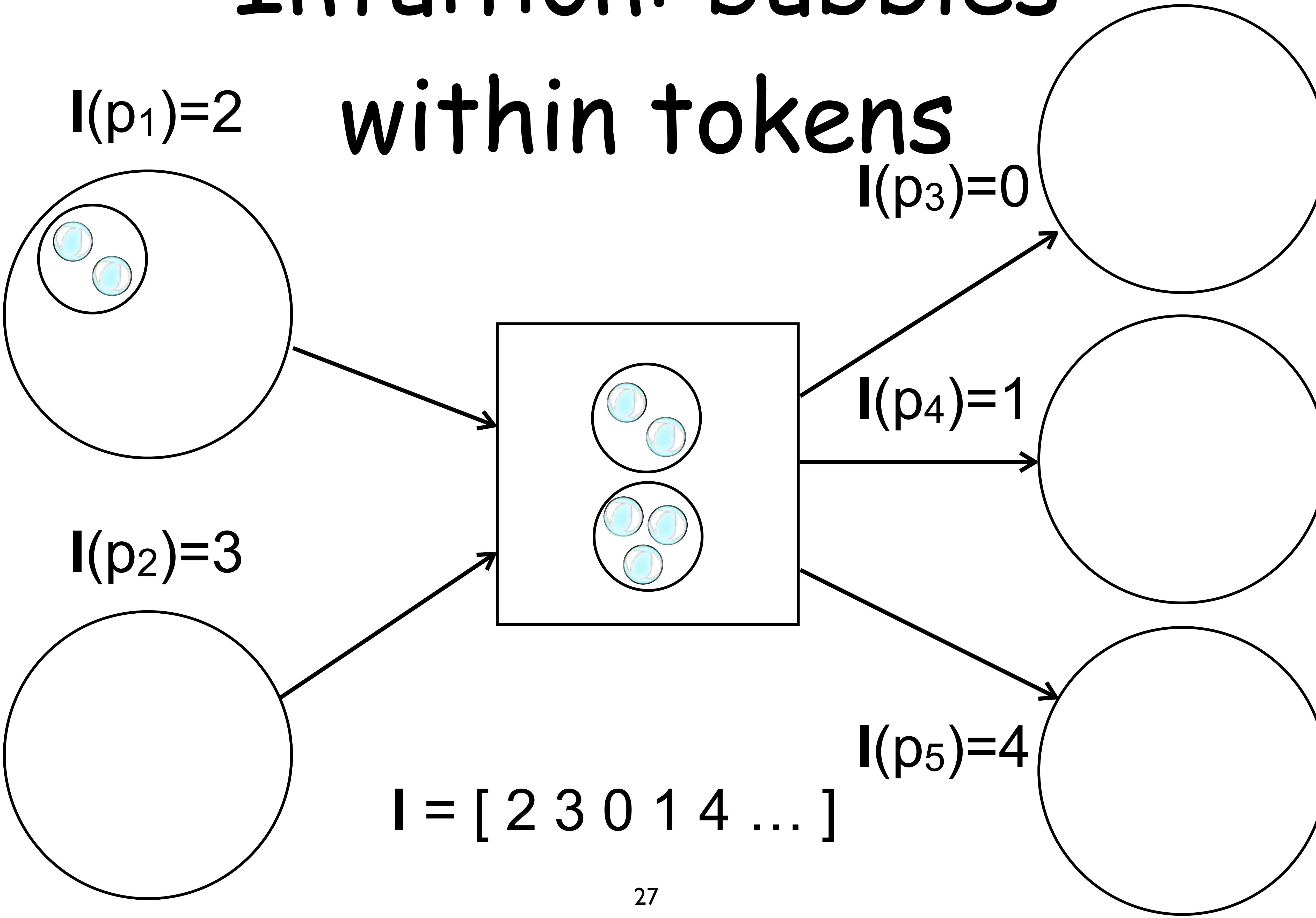
Intuition: bubbles within tokens



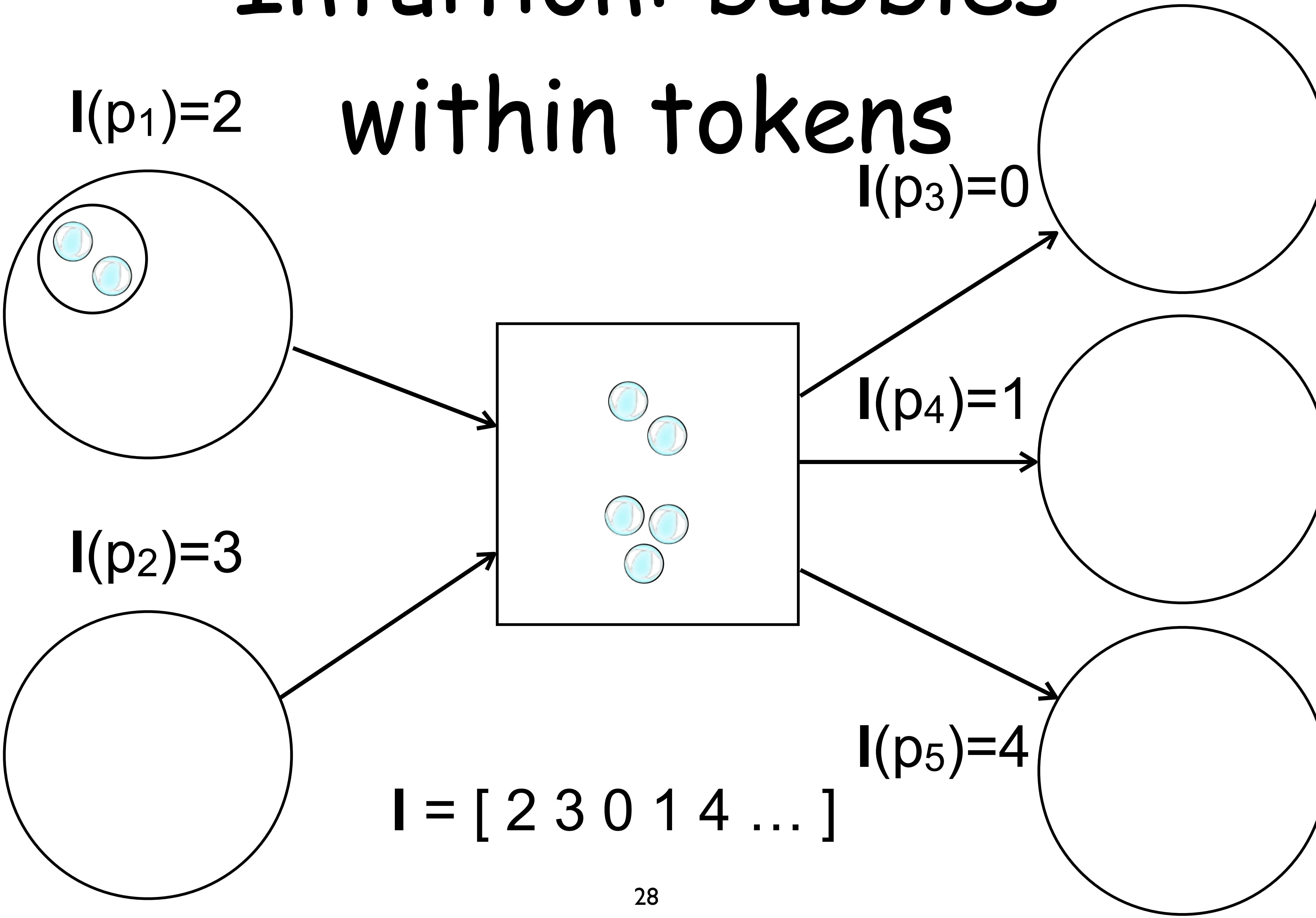
Intuition: bubbles within tokens



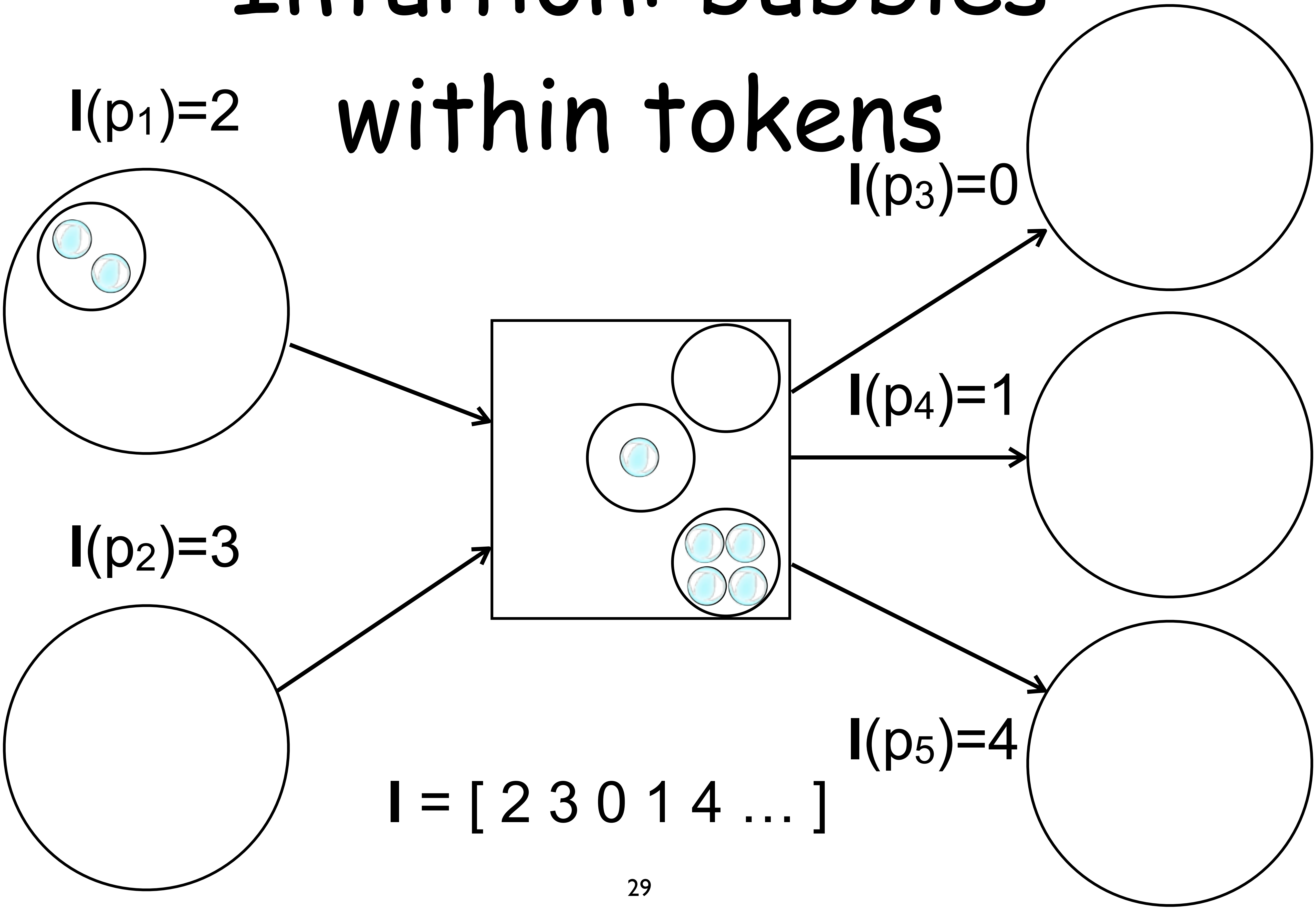
Intuition: bubbles within tokens



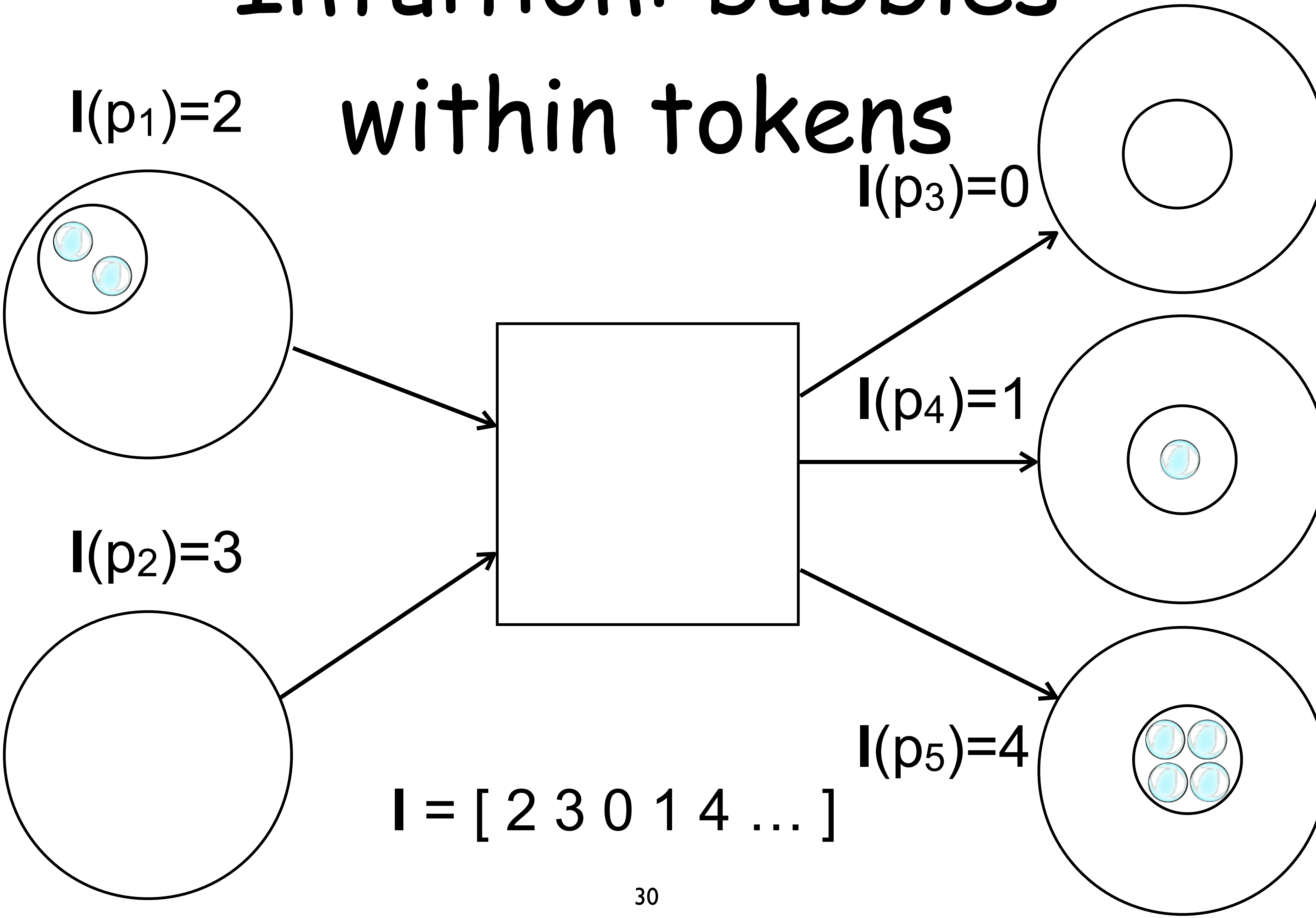
Intuition: bubbles within tokens



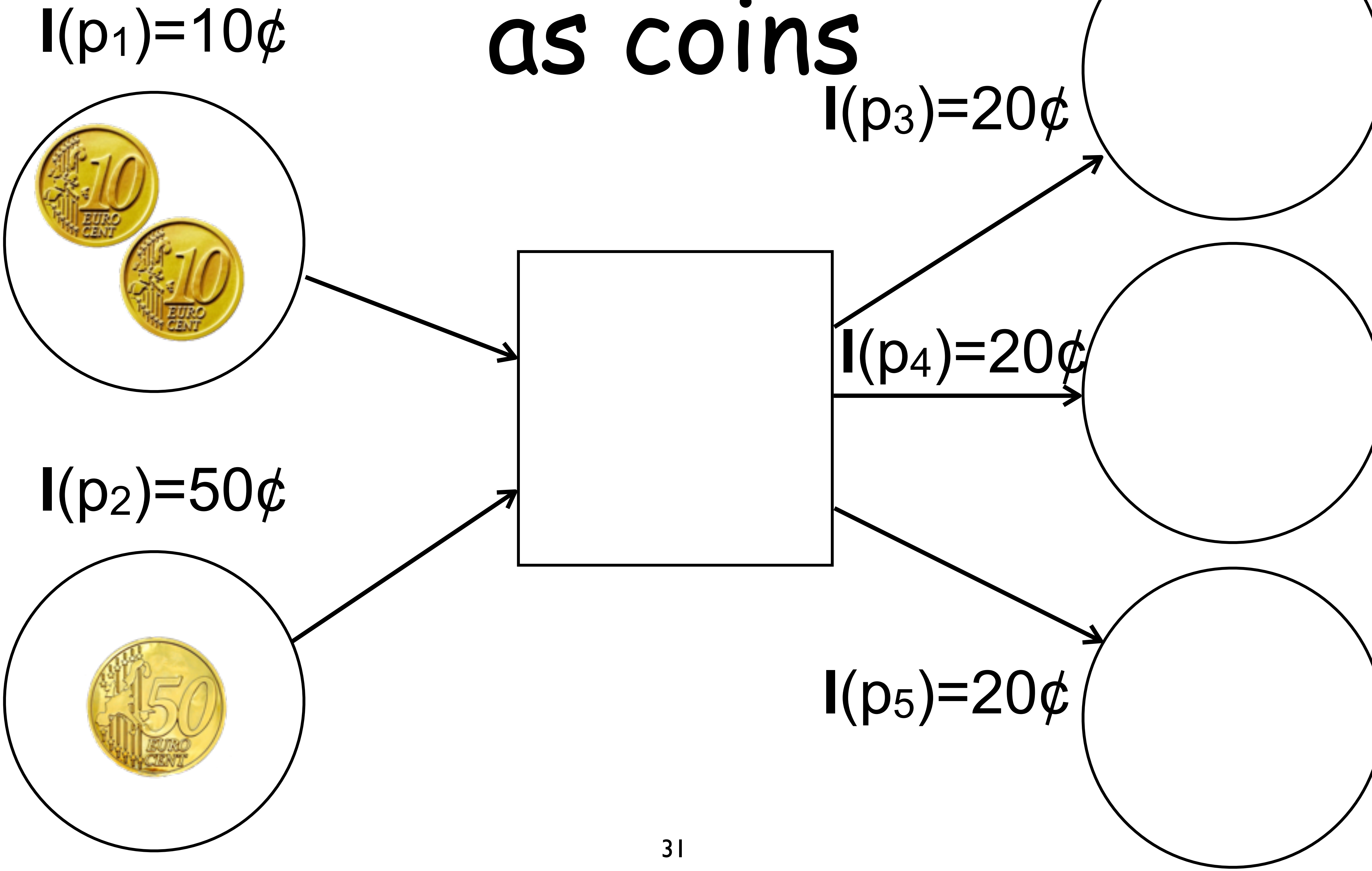
Intuition: bubbles within tokens



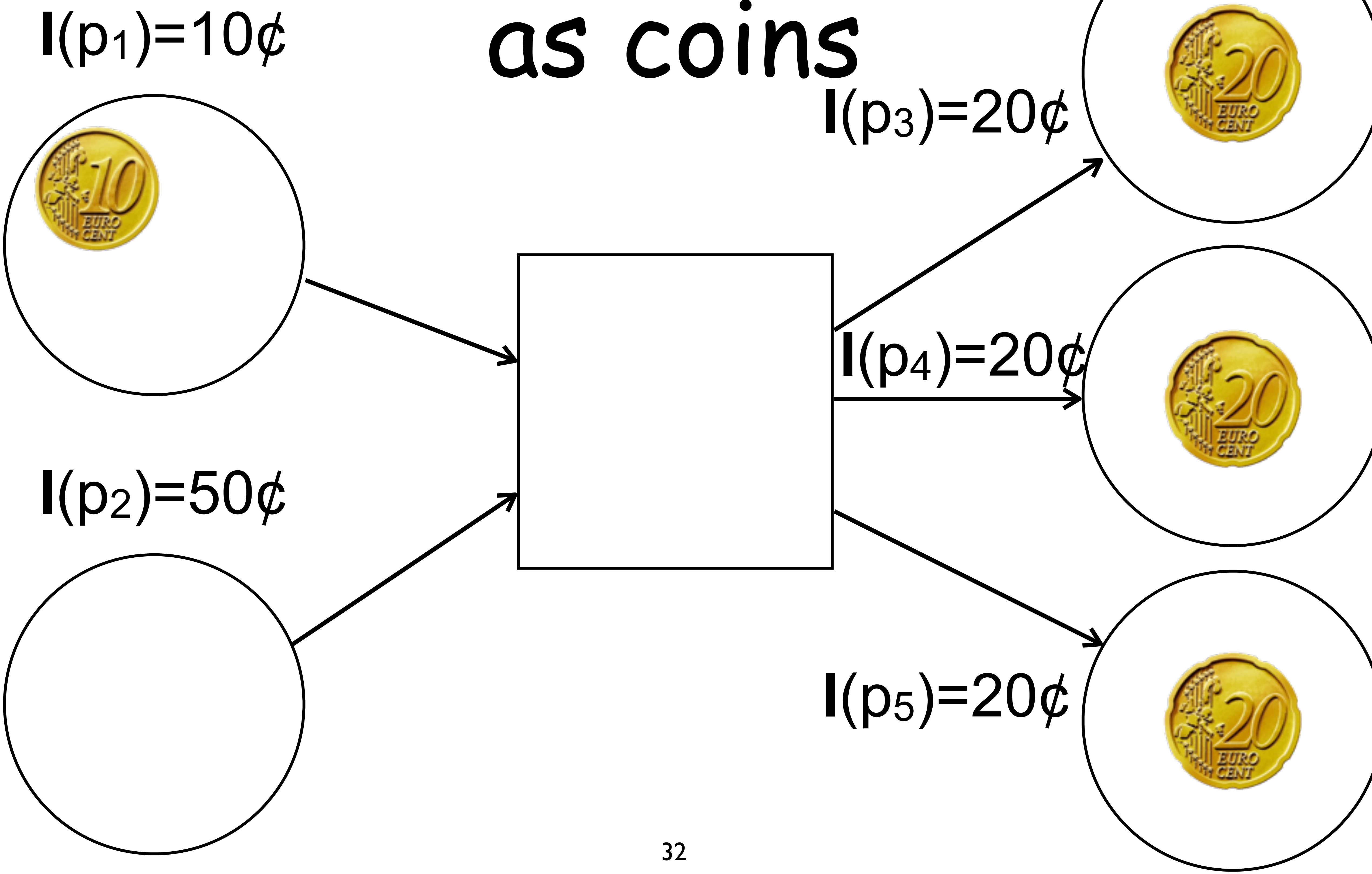
Intuition: bubbles within tokens



Intuition: tokens as coins



Intuition: tokens as coins



Linear combination

Proposition:
Any linear combination of S-invariants is an S-invariant

Take any two S-Invariants $\mathbf{I}_1$ and $\mathbf{I}_2$ and any two values k_1, k_2.
We want to prove that $k_1\,\mathbf{I}_1 + k_2\,\mathbf{I}_2$ is an S-invariant.

$$\begin{aligned}(k_1\,\mathbf{I}_1 + k_2\,\mathbf{I}_2)\cdot\mathbf{N} &= k_1\,\mathbf{I}_1\cdot\mathbf{N} + k_2\,\mathbf{I}_2\cdot\mathbf{N}\\ &= k_1\,\mathbf{0} + k_2\,\mathbf{0}\\ &= \mathbf{0}\end{aligned}$$

Alternative definition of S-invariant

Proposition:

A mapping $\mathbf{I} : P \to \mathbb{Q}$ is an S-invariant of N iff for any $t \in T$:

$$\sum_{p \in \bullet t} \mathbf{I}(p) = \sum_{p \in t \bullet} \mathbf{I}(p)$$

Exercise

Prove the proposition about the alternative characterization of S-invariants

Consequence of alternative definition

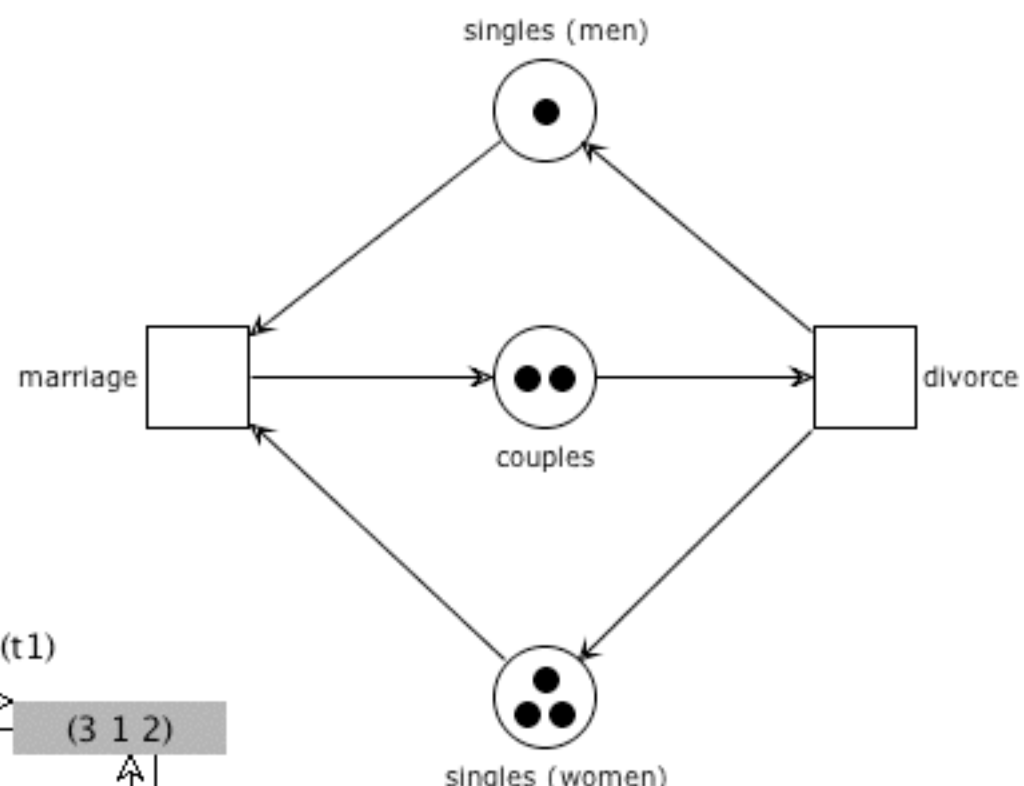
Very useful in proving S-invariance!

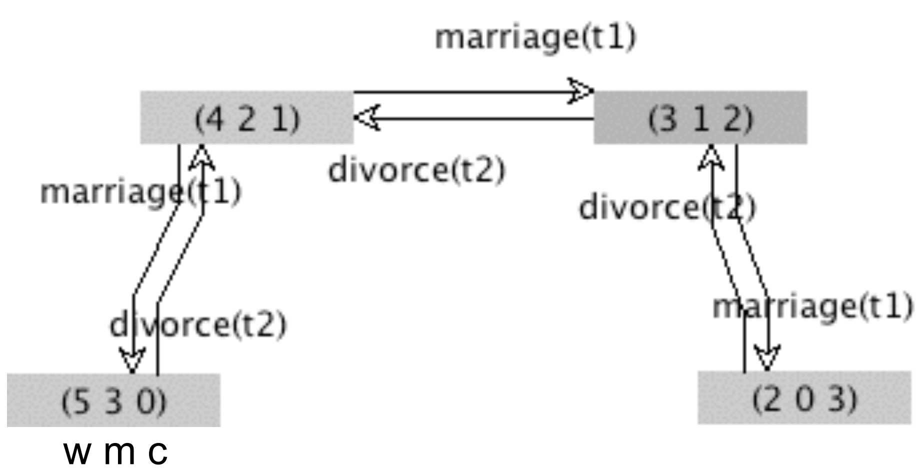
The check is possible without constructing the incidence matrix

It can also help to build S-invariants directly over the picture

Question time

Which of the following are S-invariants?

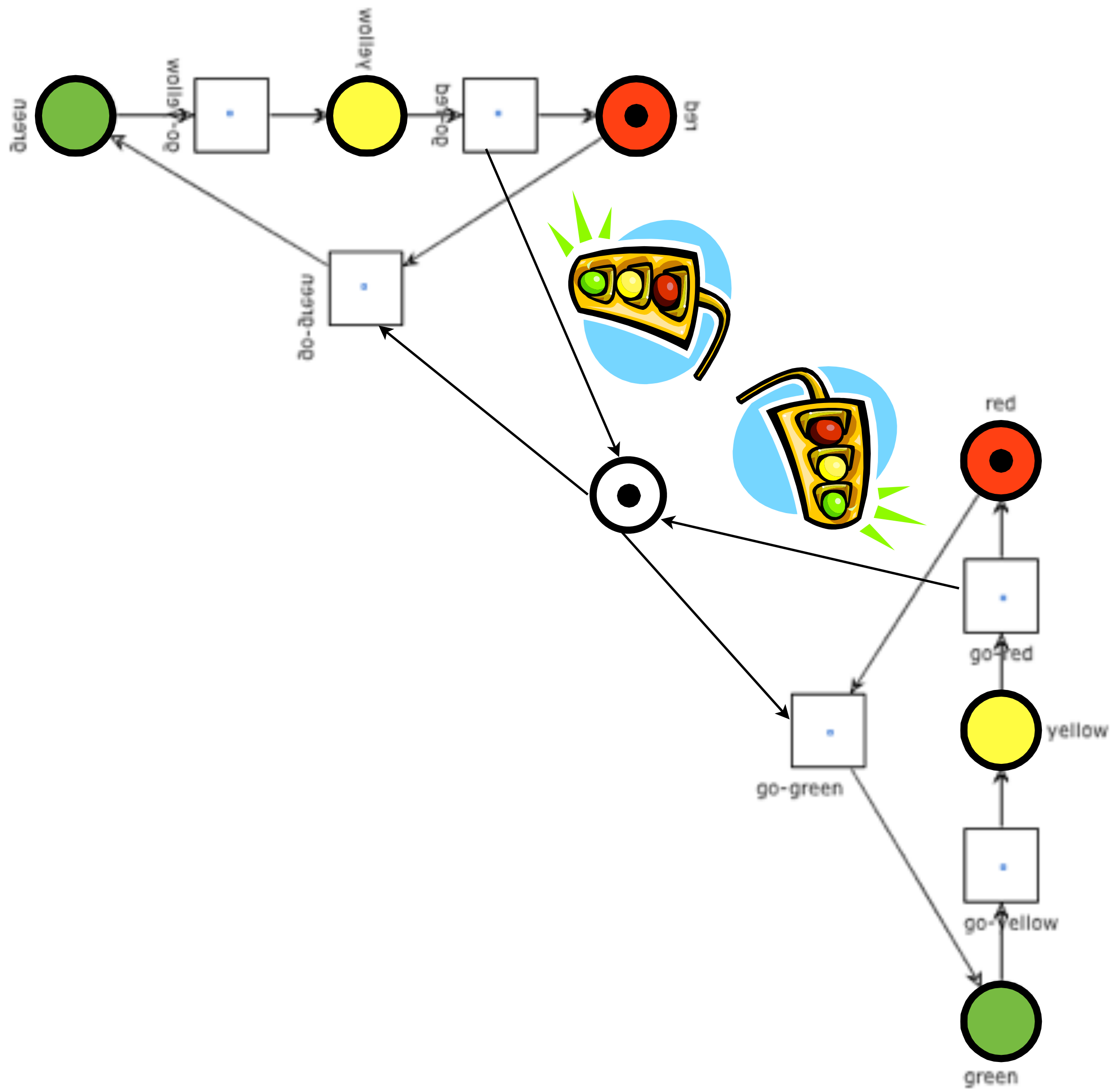




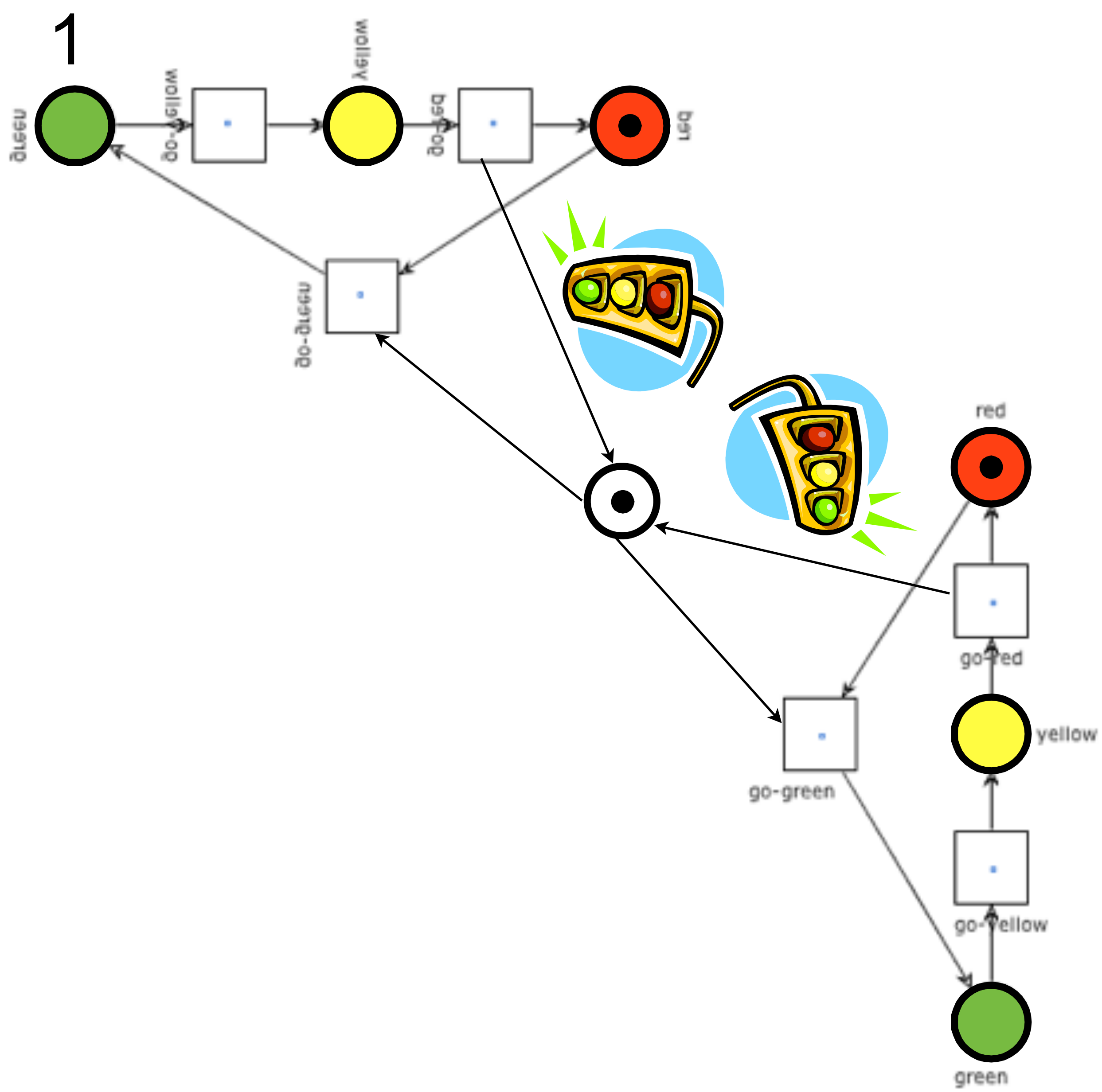
m	w	c
[1	1	-1]
[1	0	1]
[0	1	1]
[1	1	1]
[1	-1	0]
[1	1	2]
[1	2	2]

$$\forall t \in T,\ \sum_{p \in \bullet t} \mathbf{I}(p) \stackrel{?}{=} \sum_{p \in t \bullet} \mathbf{I}(p)$$

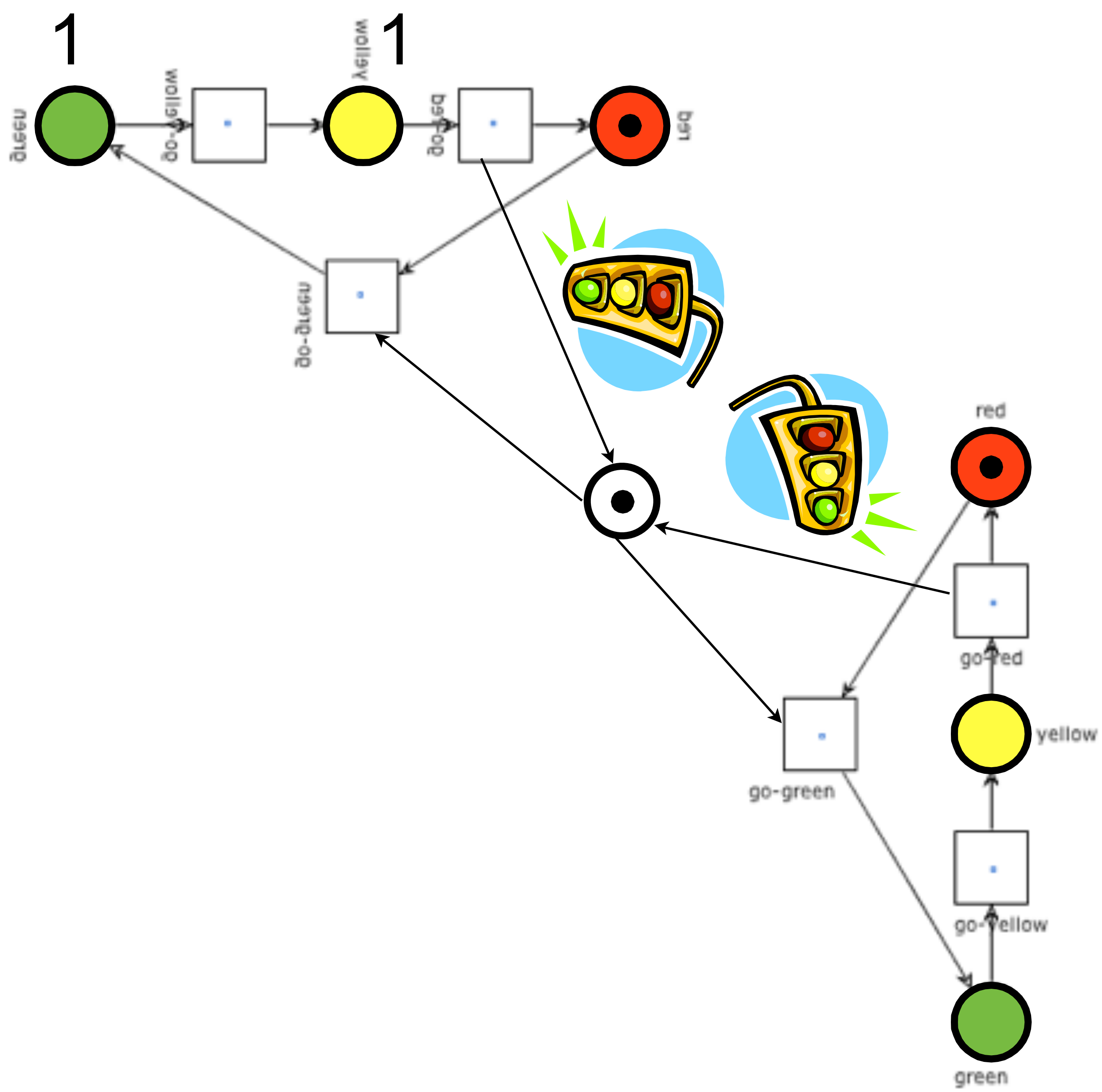
Traffic-lights example



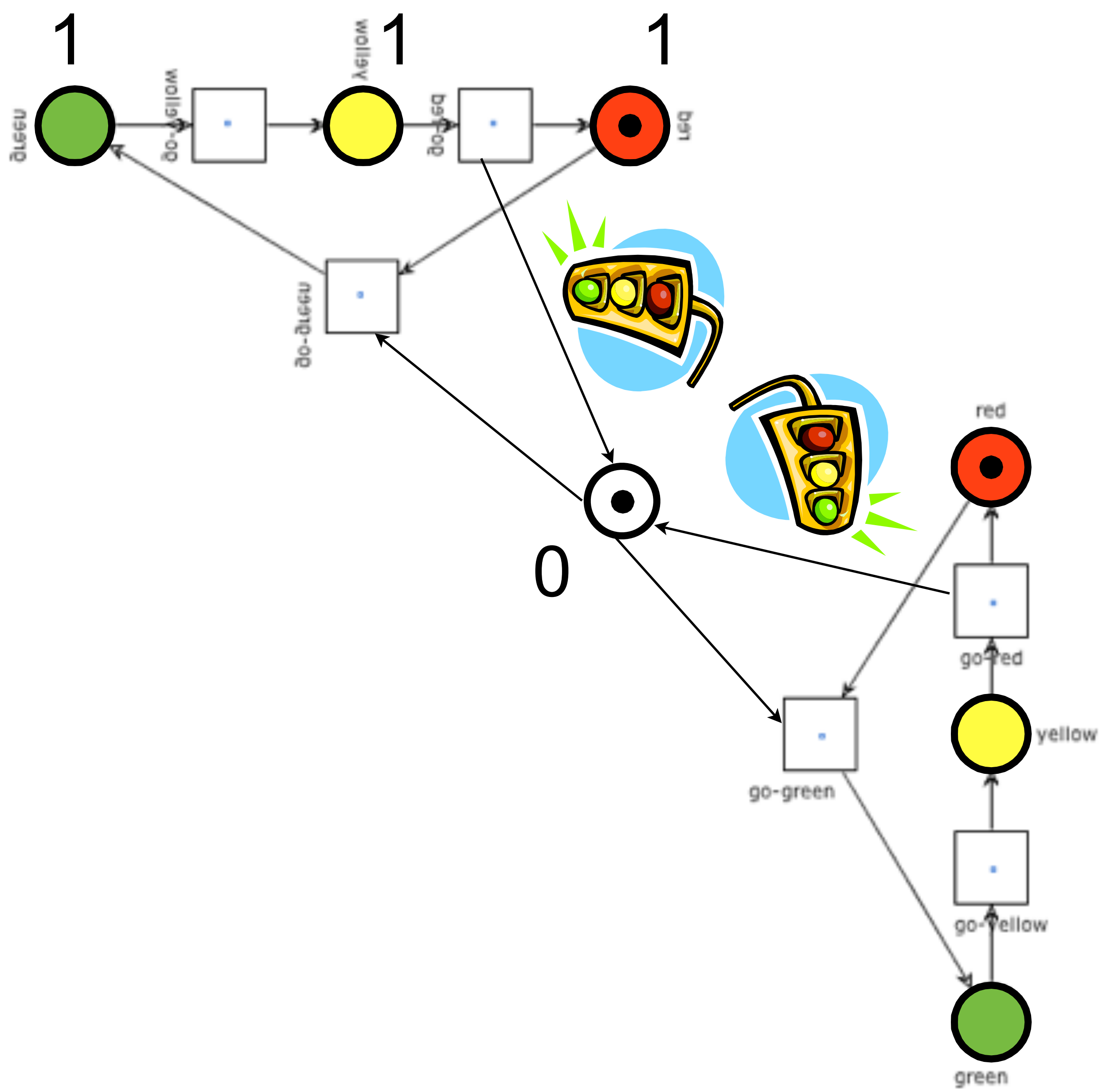
Traffic-lights example



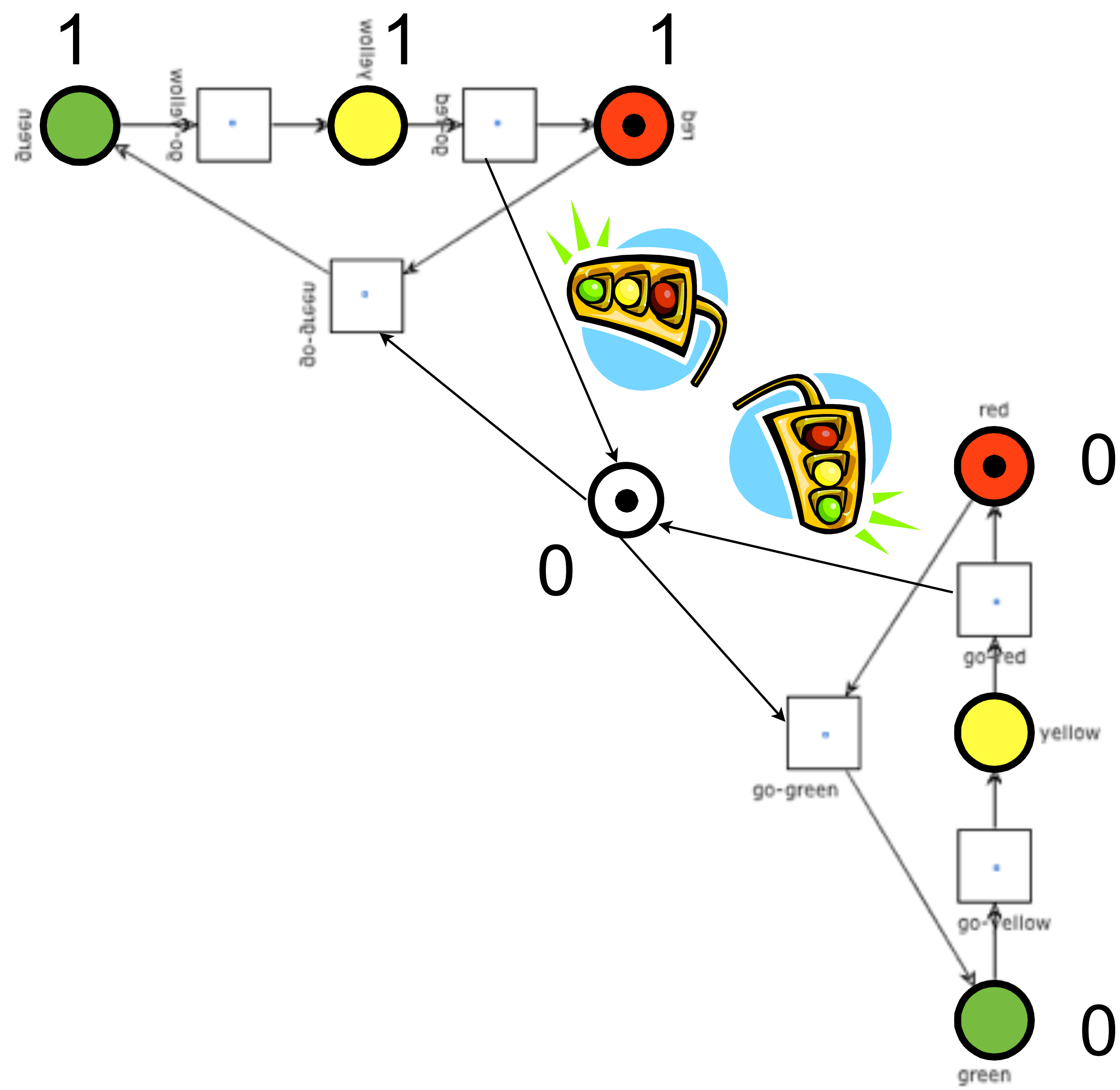
Traffic-lights example



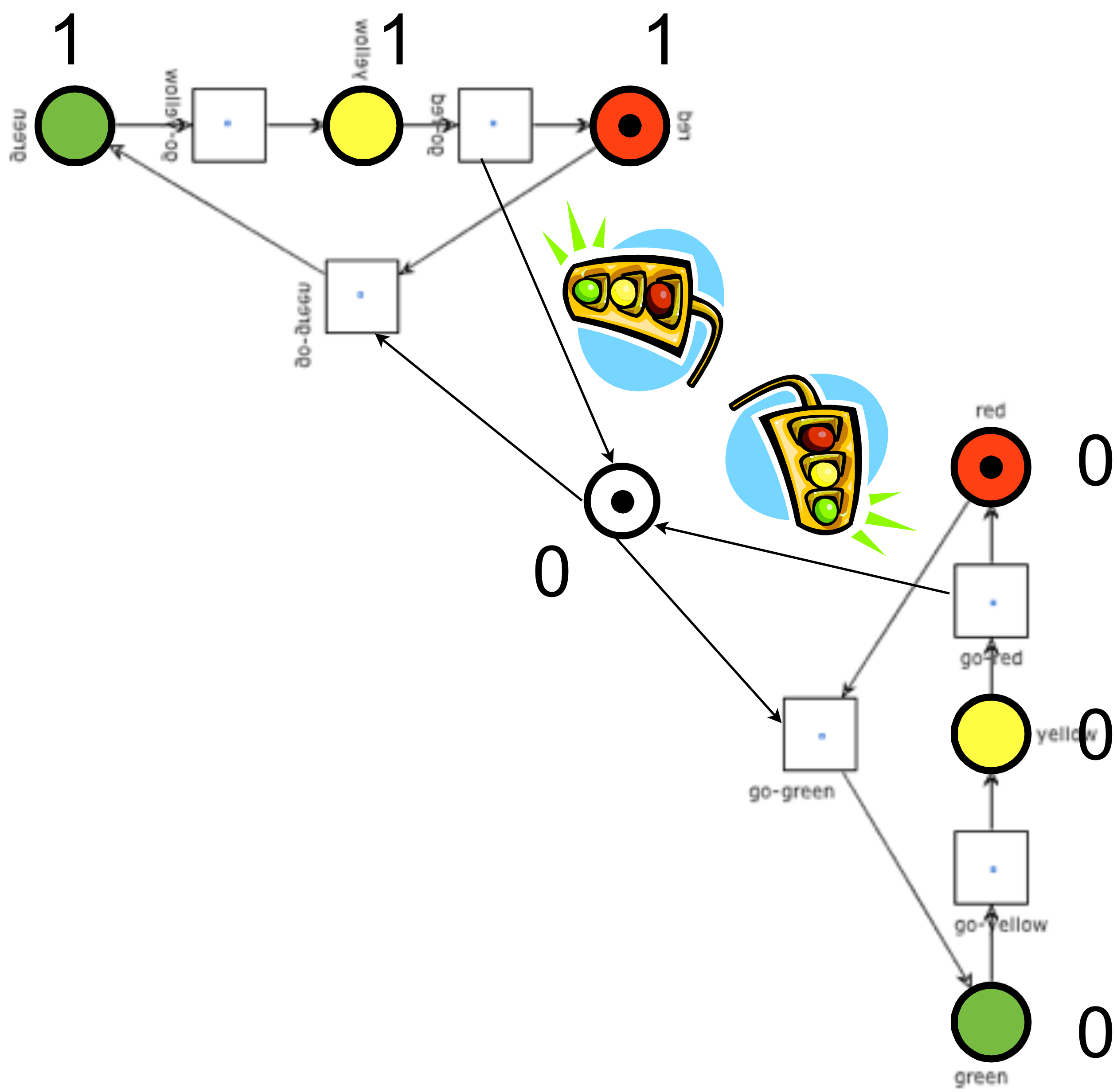
Traffic-lights example



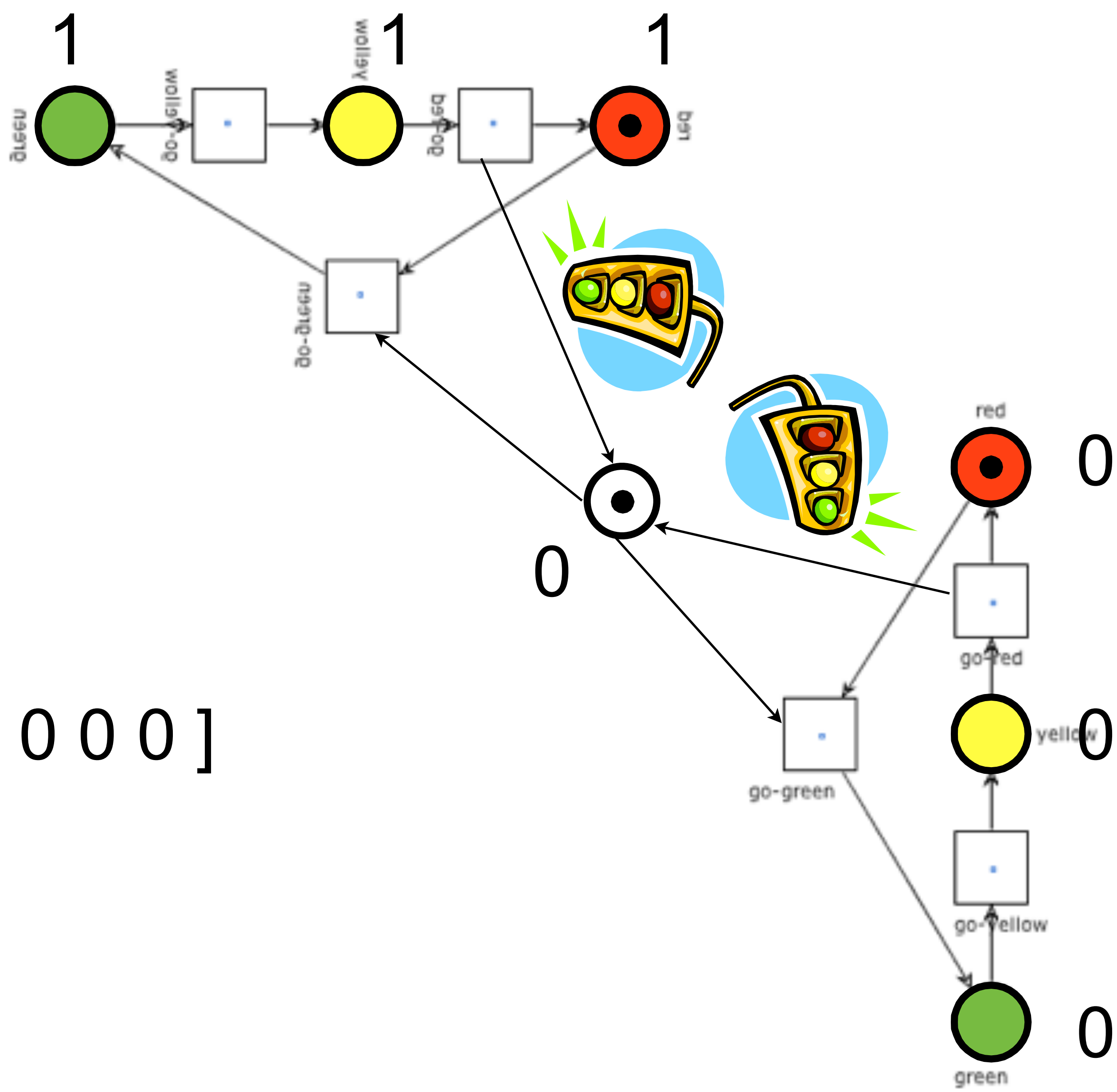
Traffic-lights example



Traffic-lights example



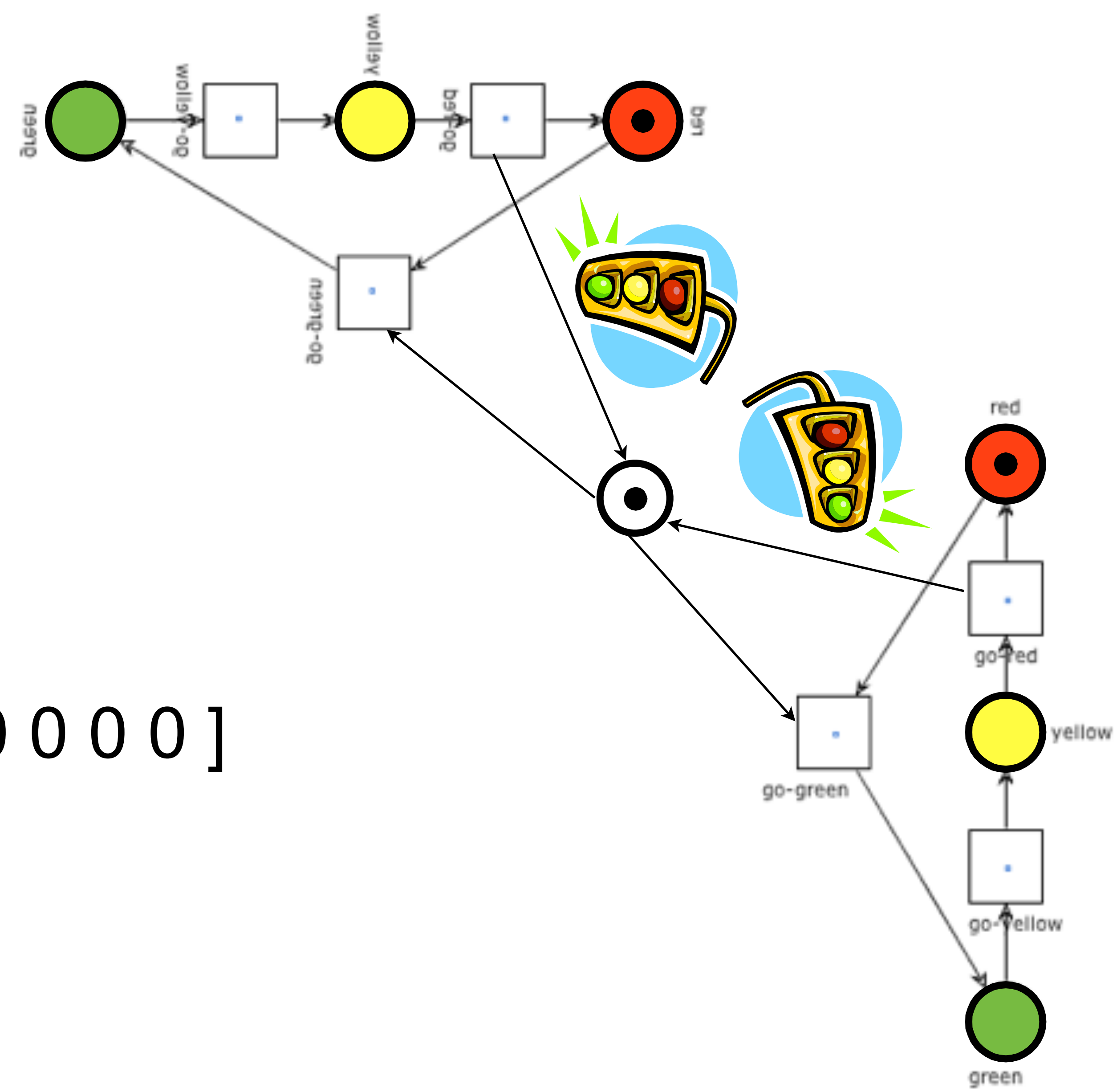
Traffic-lights example



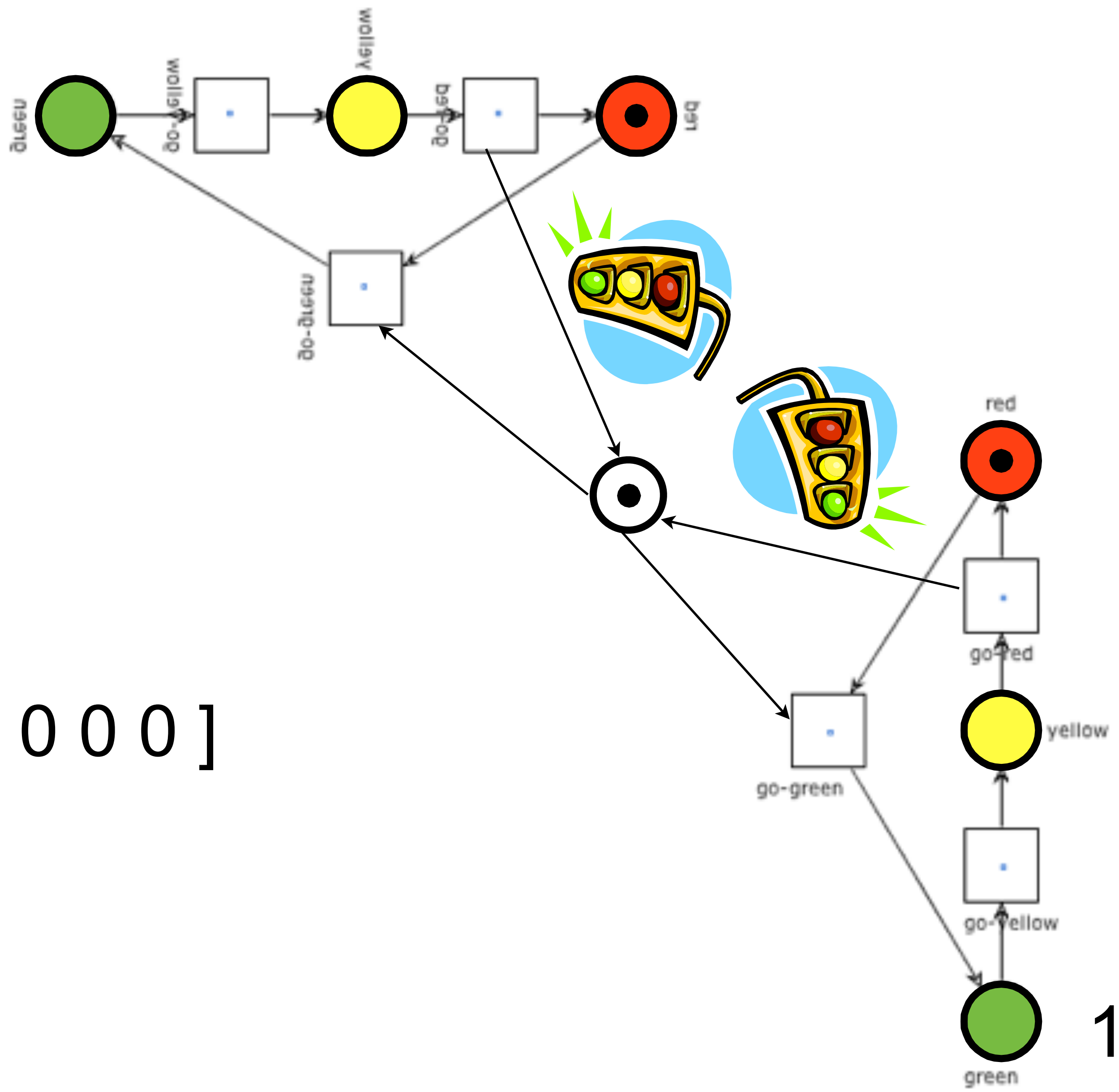
[1 1 1 0 0 0 0]

Traffic-lights example

[1 1 1 0 0 0 0]



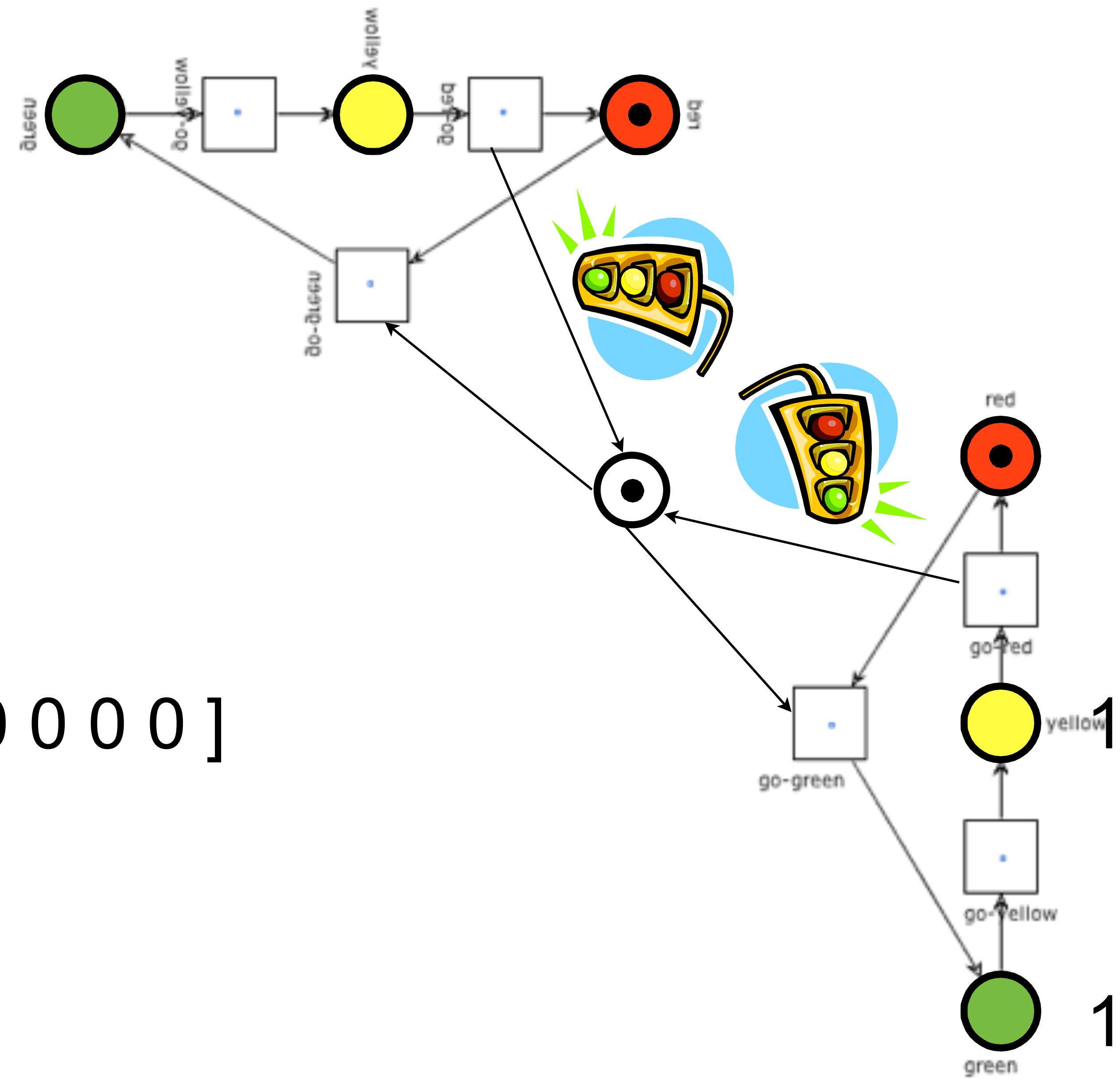
Traffic-lights example



[1 1 1 0 0 0 0]

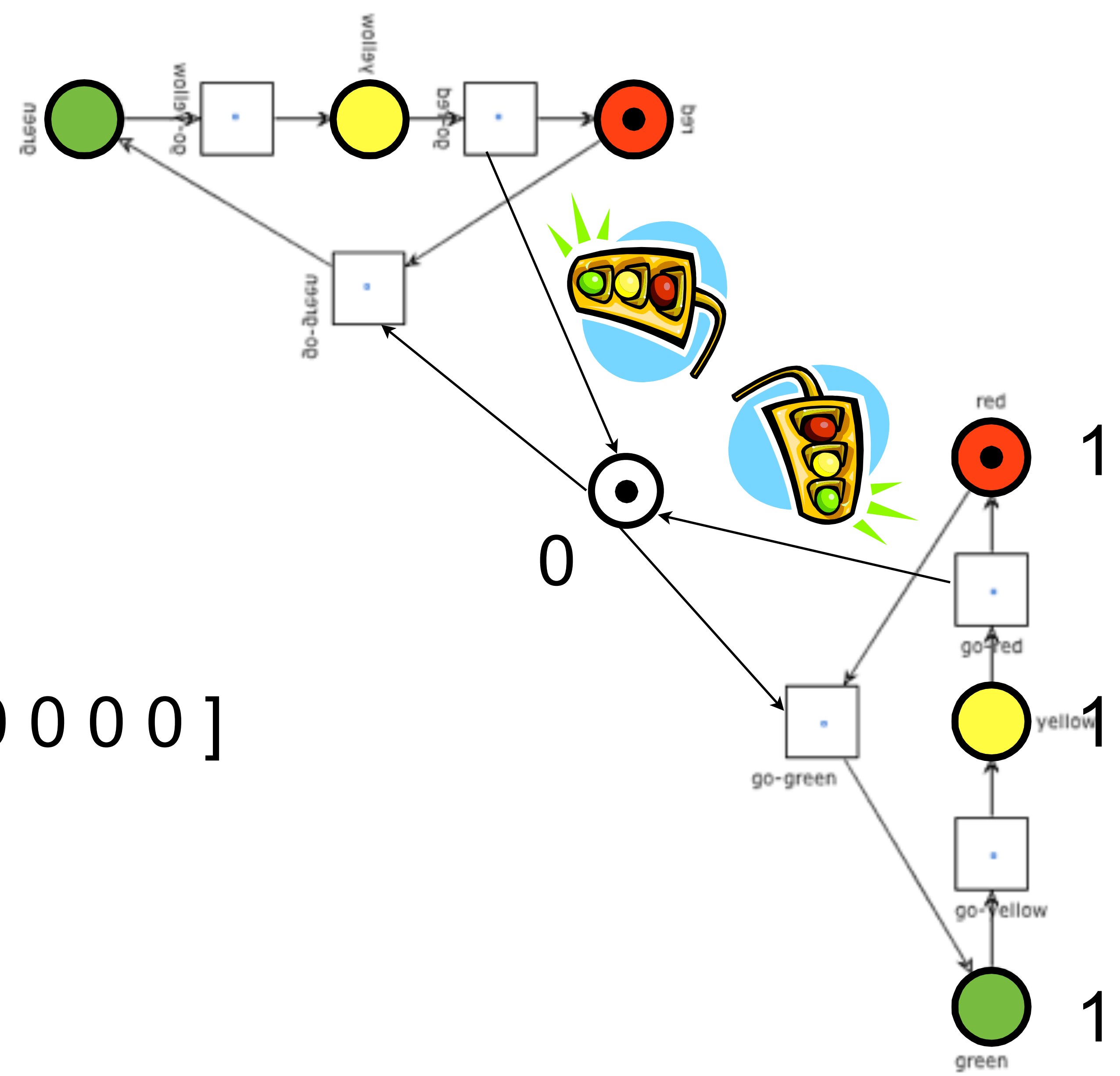
1

Traffic-lights example



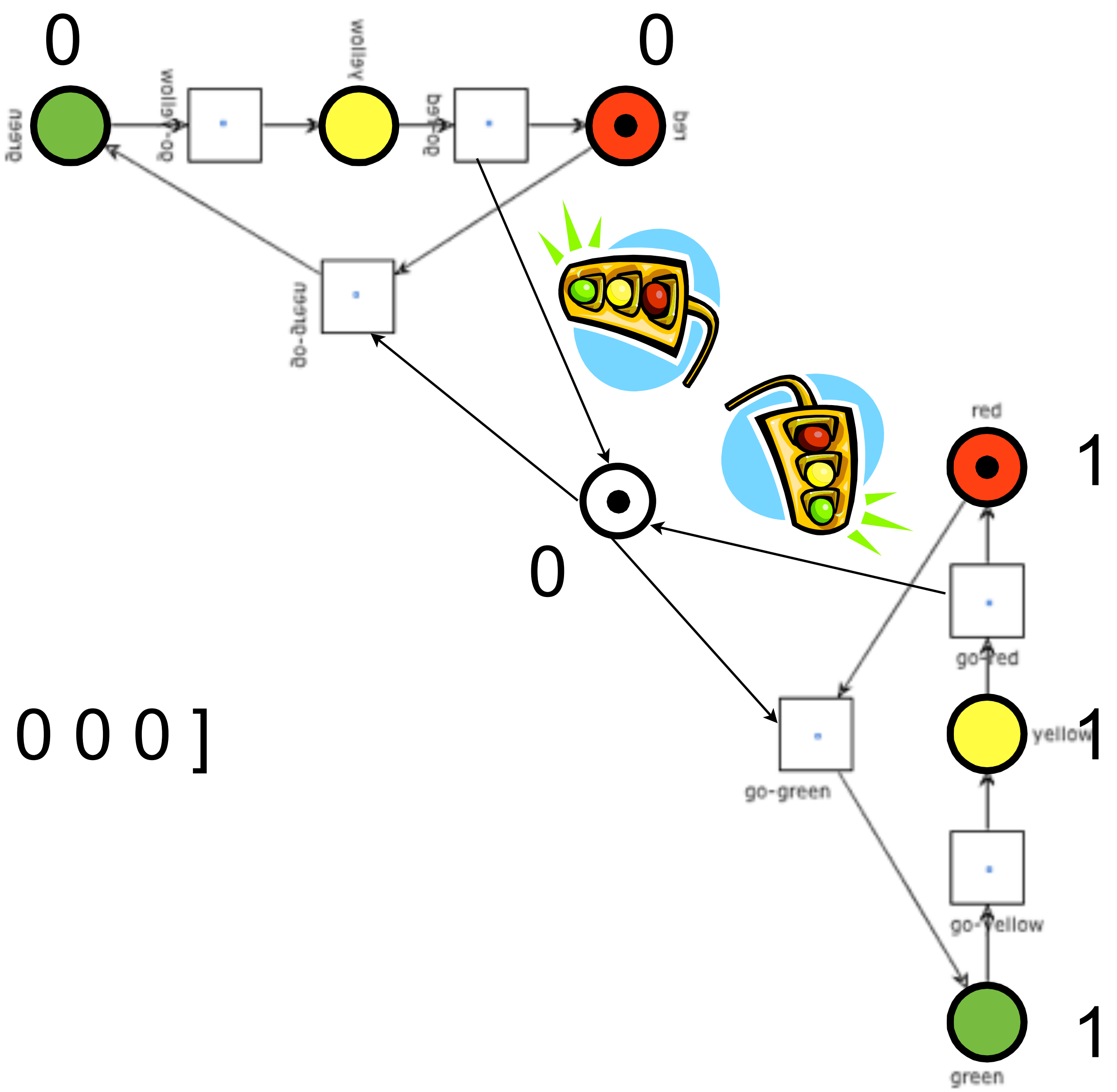
[1 1 1 0 0 0 0]

Traffic-lights example



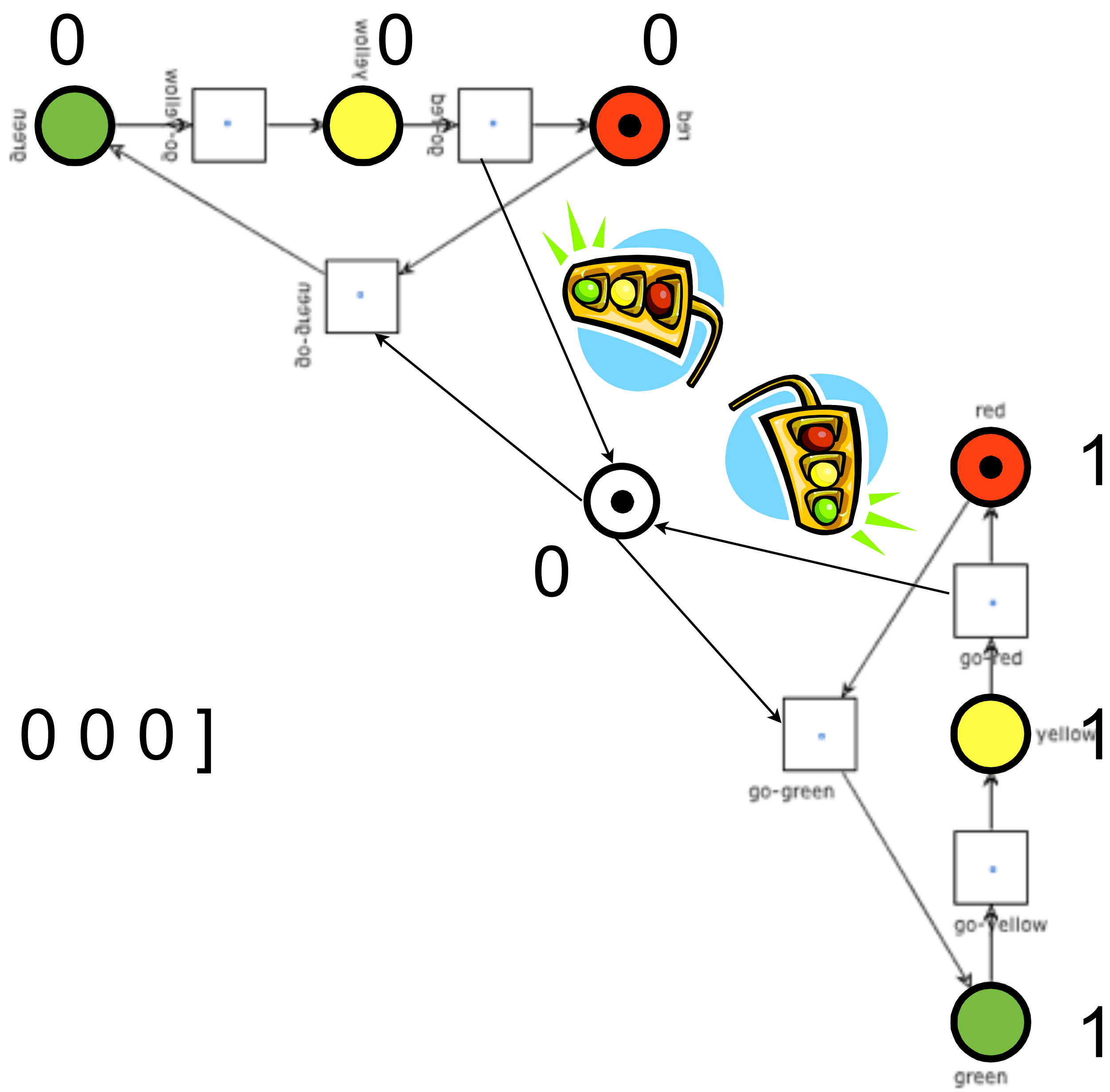
[1 1 1 0 0 0 0]

Traffic-lights example



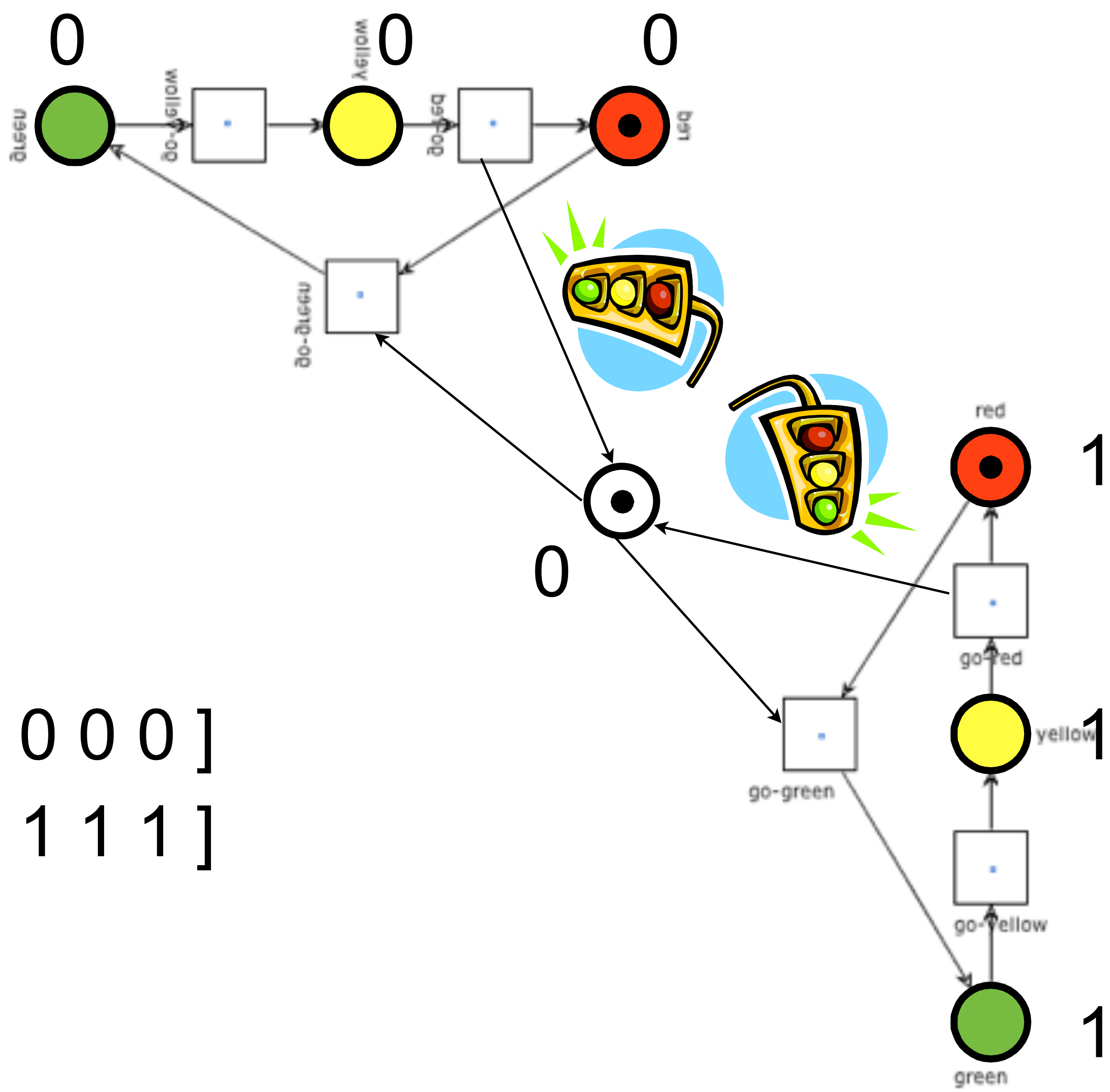
[1 1 1 0 0 0 0]

Traffic-lights example



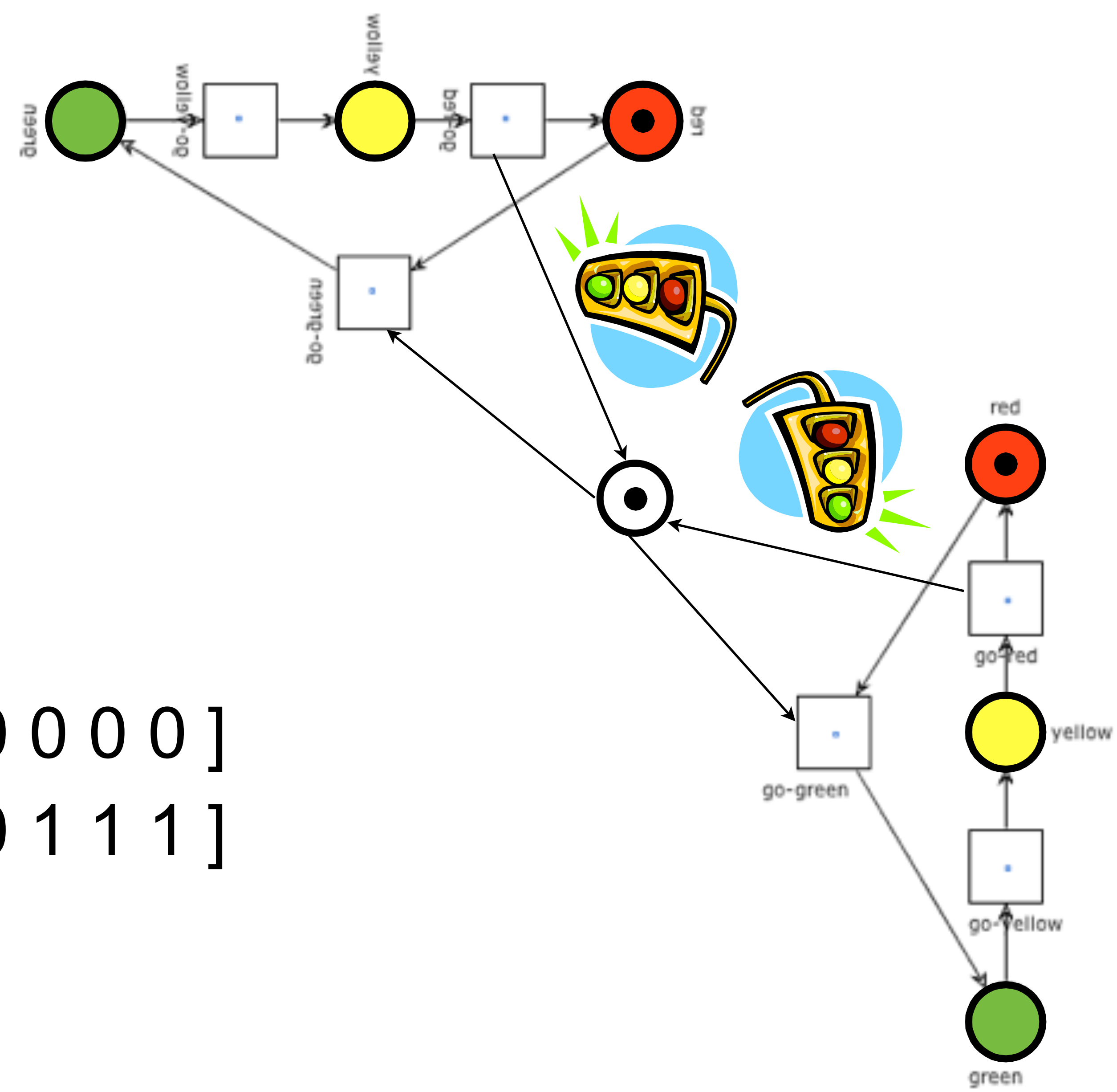
[1 1 1 0 0 0 0]

Traffic-lights example



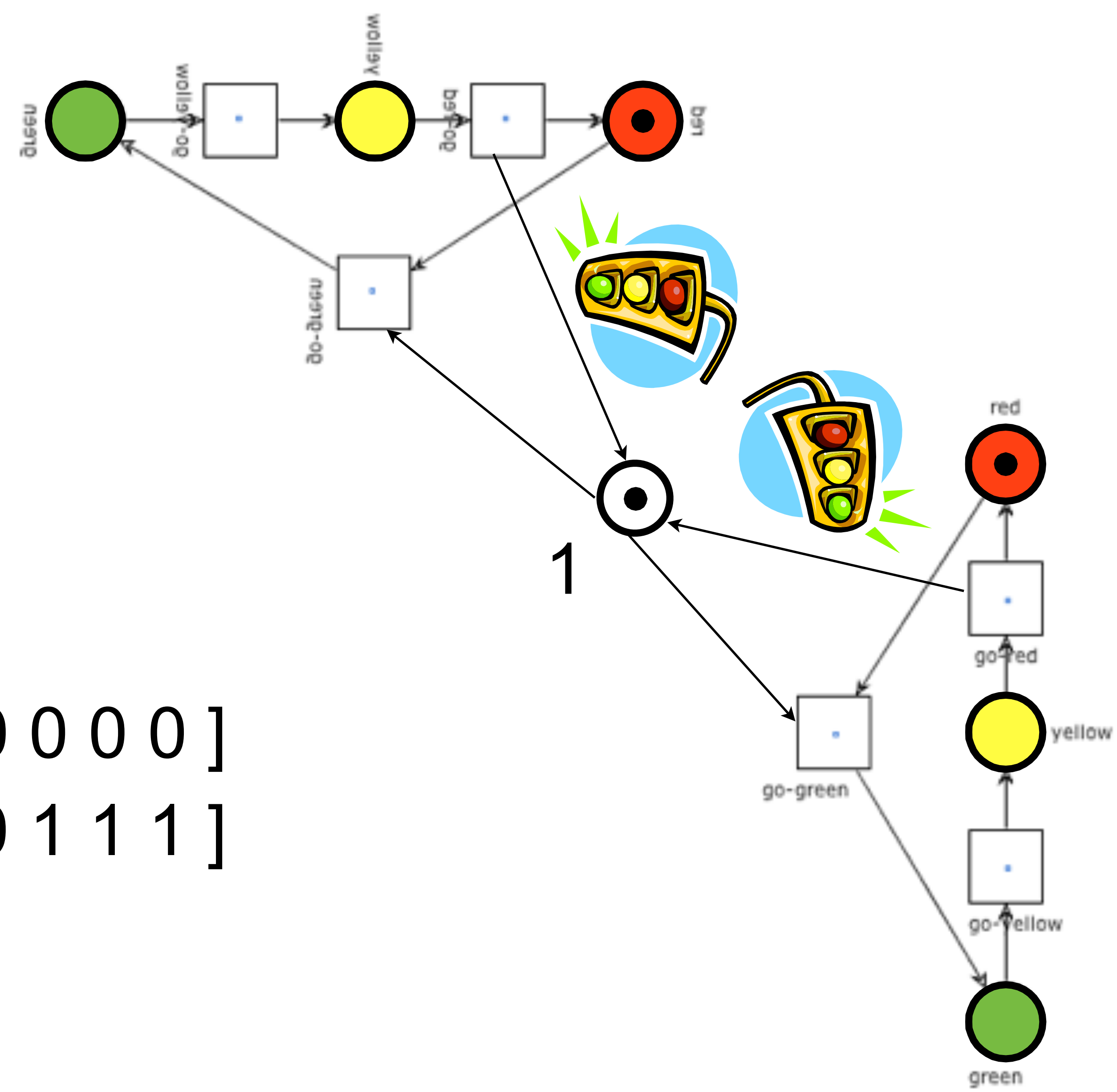
[1 1 1 0 0 0 0]
[0 0 0 0 1 1 1]

Traffic-lights example



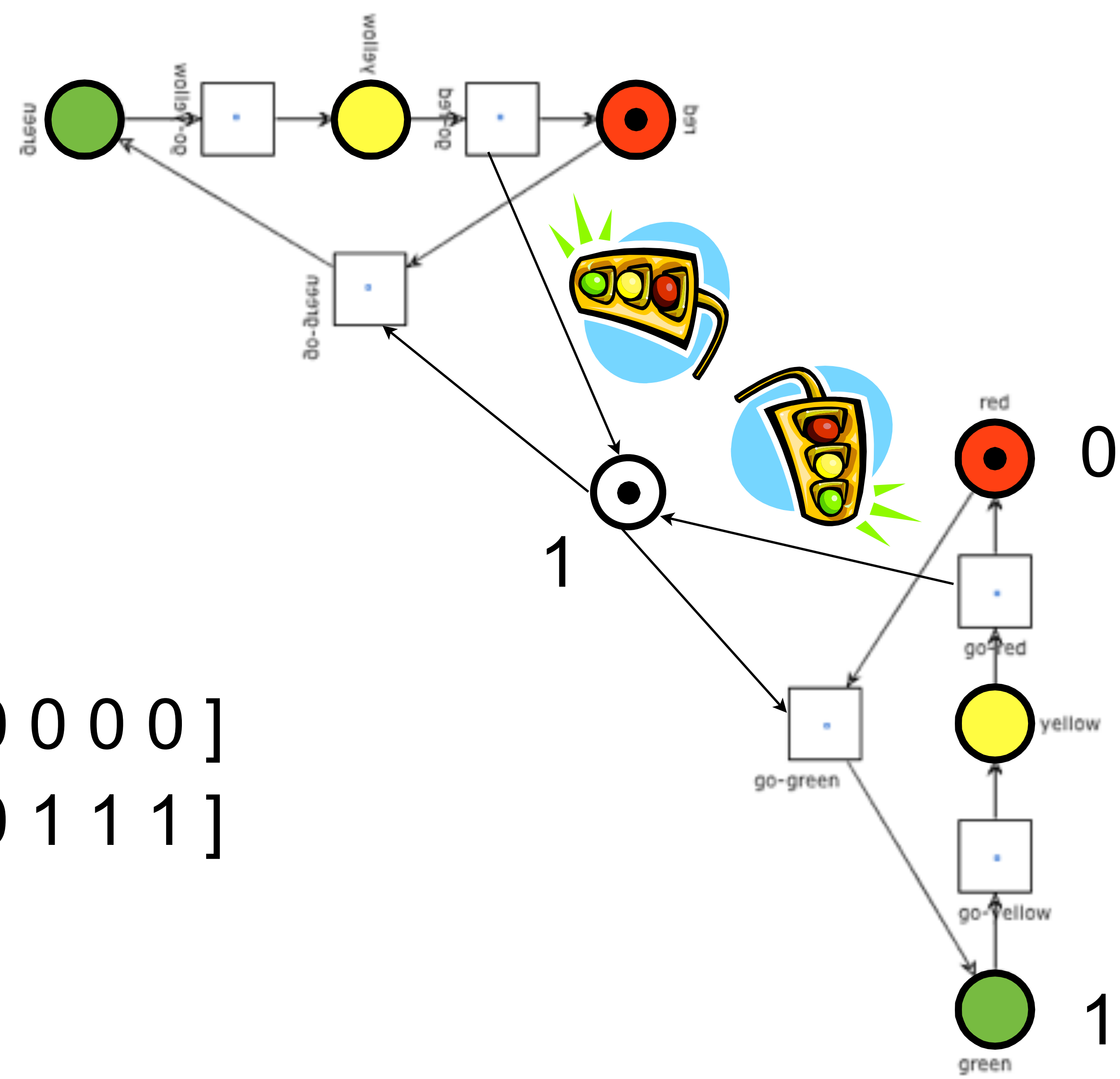
[1 1 1 0 0 0 0]
[0 0 0 0 1 1 1]

Traffic-lights example



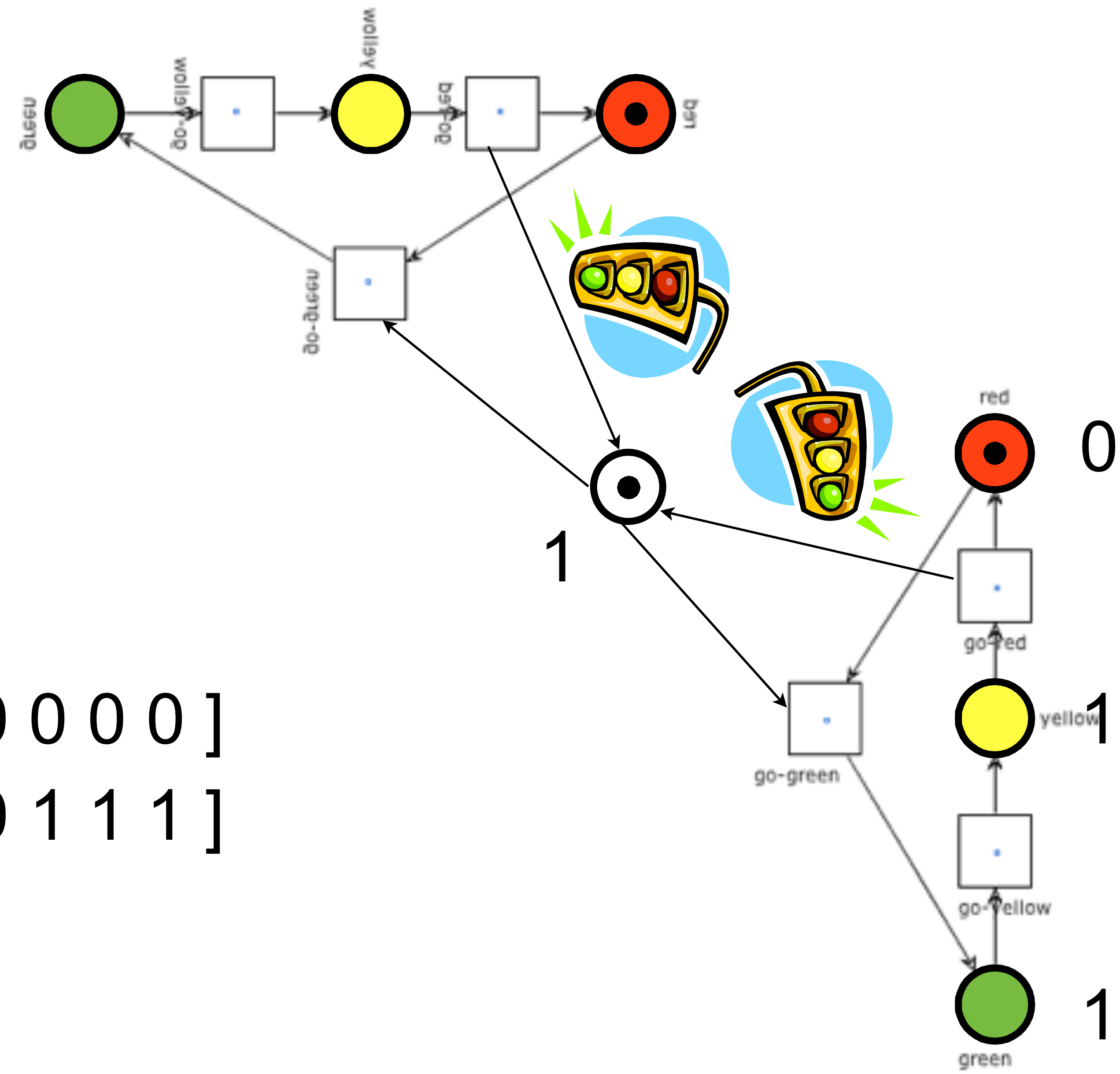
[1 1 1 0 0 0 0]
[0 0 0 0 1 1 1]

Traffic-lights example



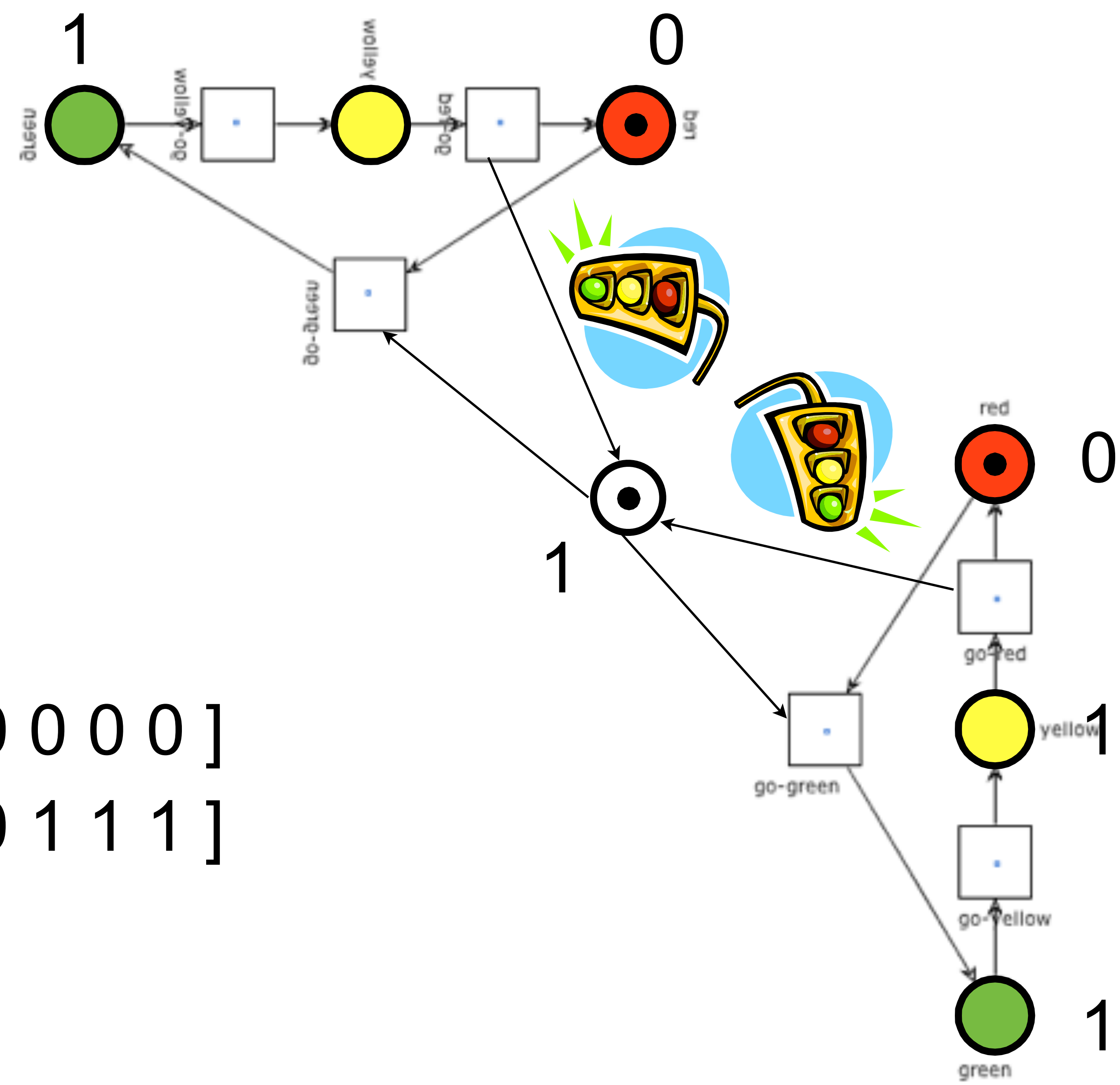
[1 1 1 0 0 0 0]
[0 0 0 0 1 1 1]

Traffic-lights example



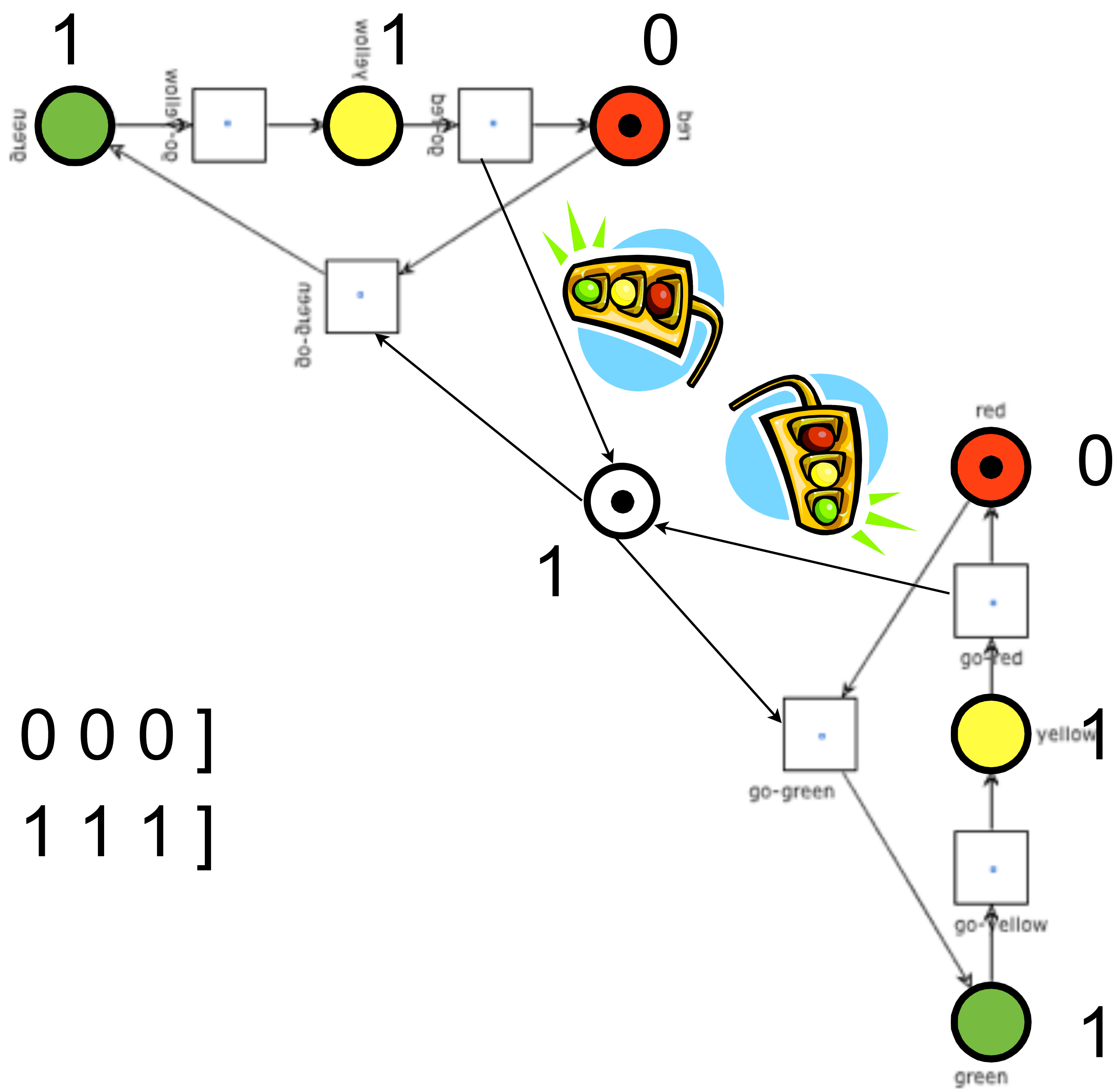
[1 1 1 0 0 0 0]
[0 0 0 0 1 1 1]

Traffic-lights example



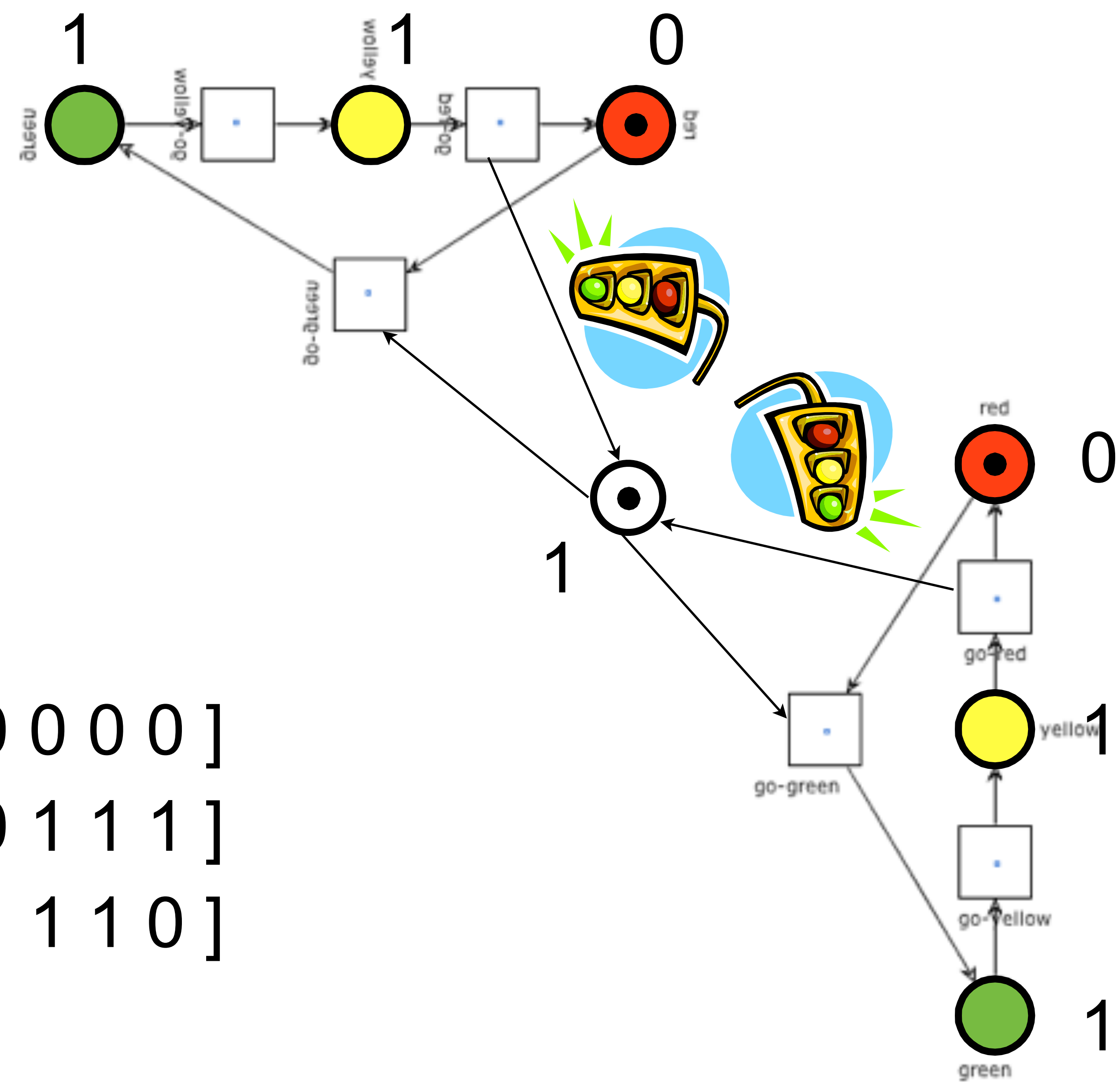
[1 1 1 0 0 0 0]
[0 0 0 0 1 1 1]

Traffic-lights example



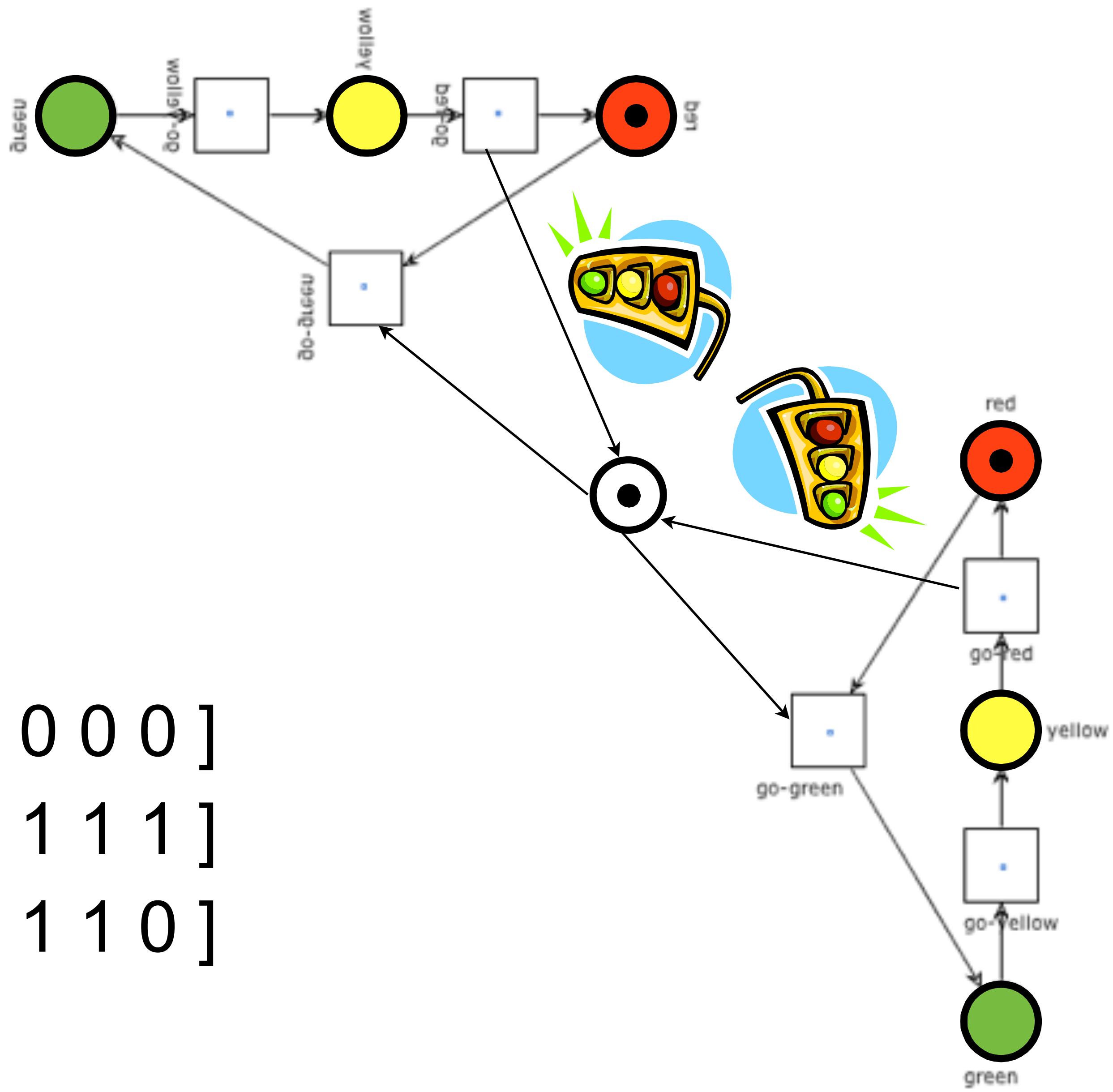
[1 1 1 0 0 0 0]
[0 0 0 0 1 1 1]

Traffic-lights example



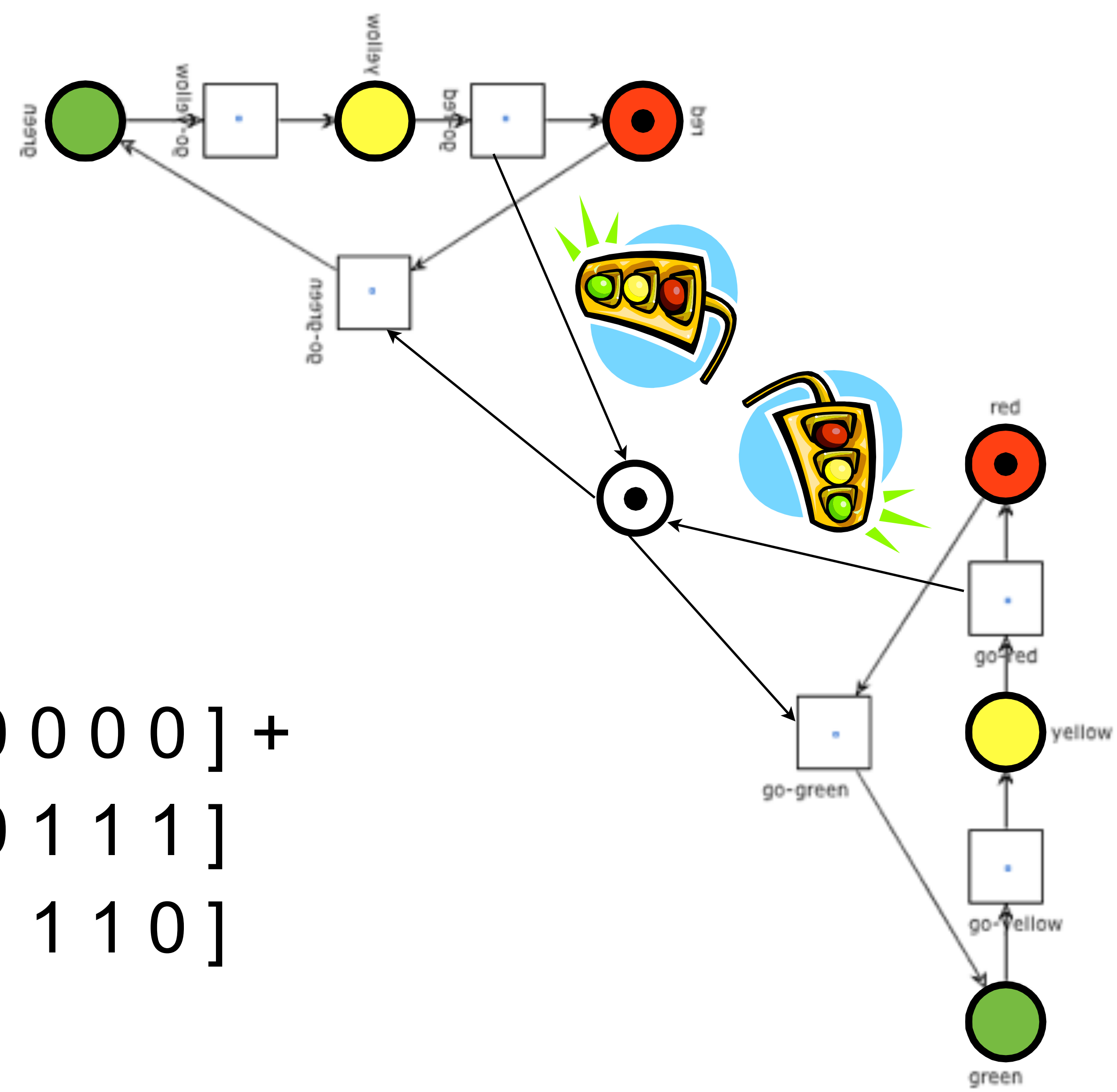
[1 1 1 0 0 0 0]
[0 0 0 0 1 1 1]
[1 1 0 1 1 1 0]

Traffic-lights example



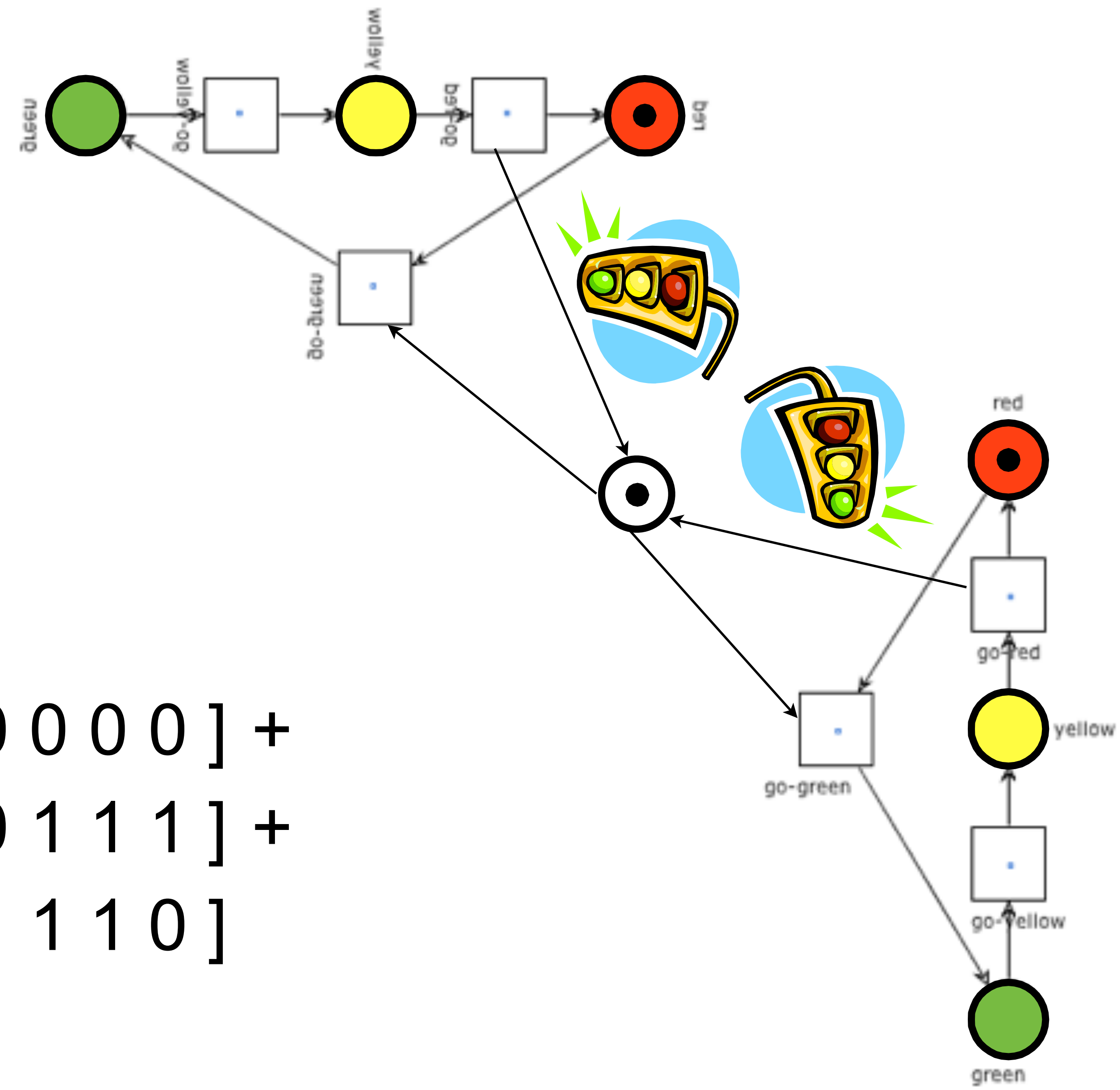
[1 1 1 0 0 0 0]
[0 0 0 0 1 1 1]
[1 1 0 1 1 1 0]

Traffic-lights example



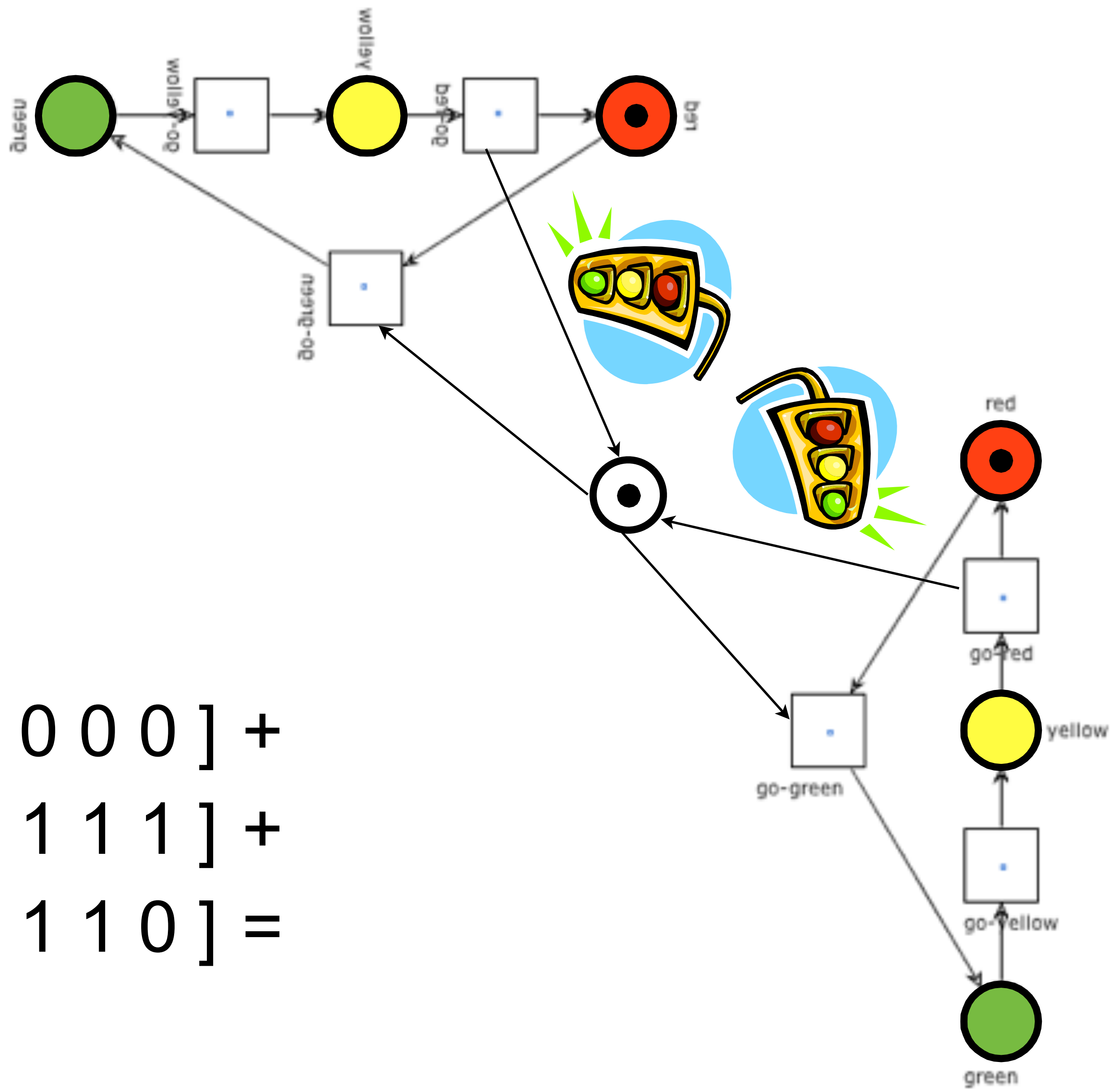
[1 1 1 0 0 0 0] +
[0 0 0 0 1 1 1]
[1 1 0 1 1 1 0]

Traffic-lights example



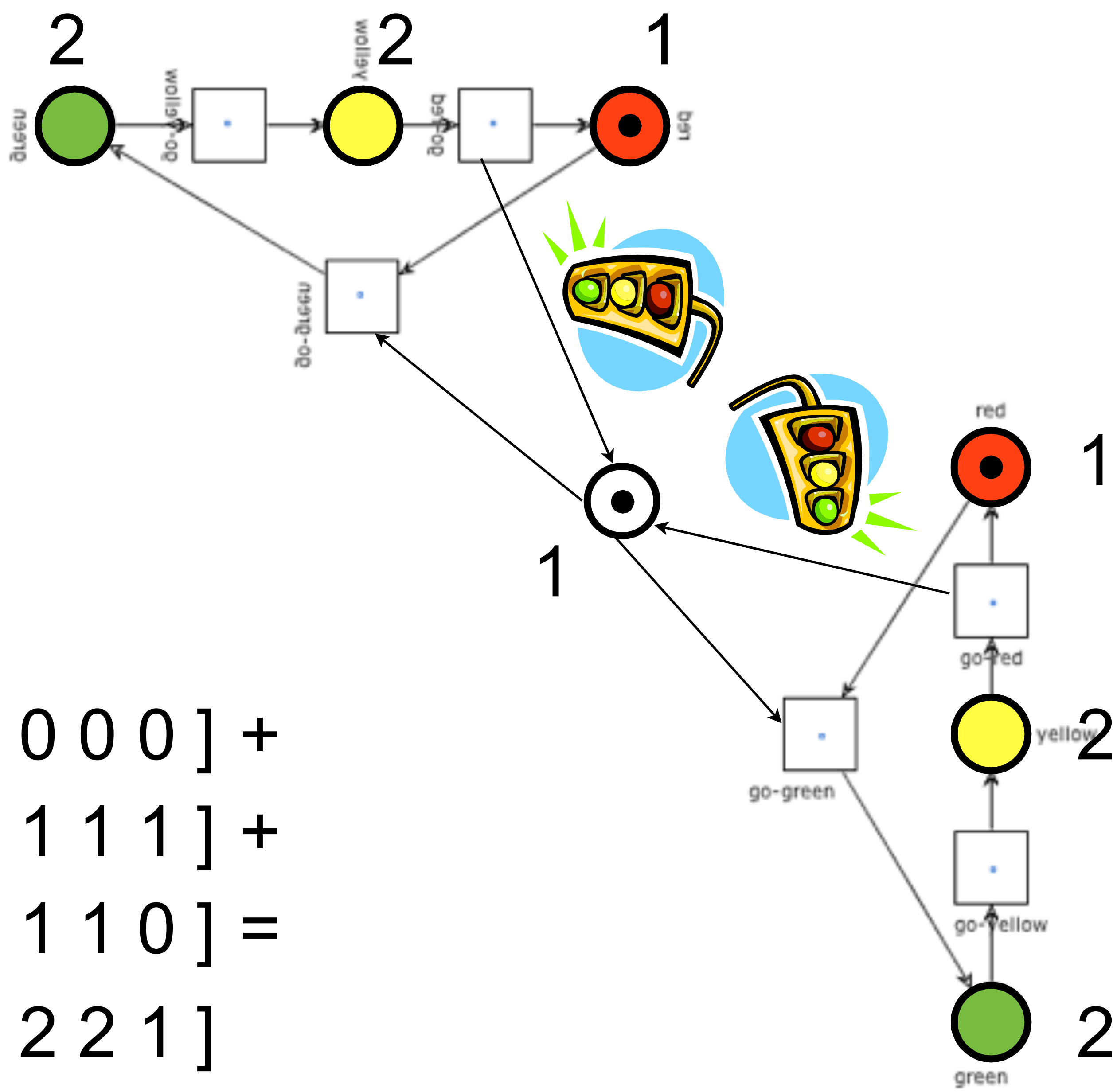
[1 1 1 0 0 0 0] +
[0 0 0 0 1 1 1] +
[1 1 0 1 1 1 0]

Traffic-lights example



[1 1 1 0 0 0 0] +
[0 0 0 0 1 1 1] +
[1 1 0 1 1 1 0] =

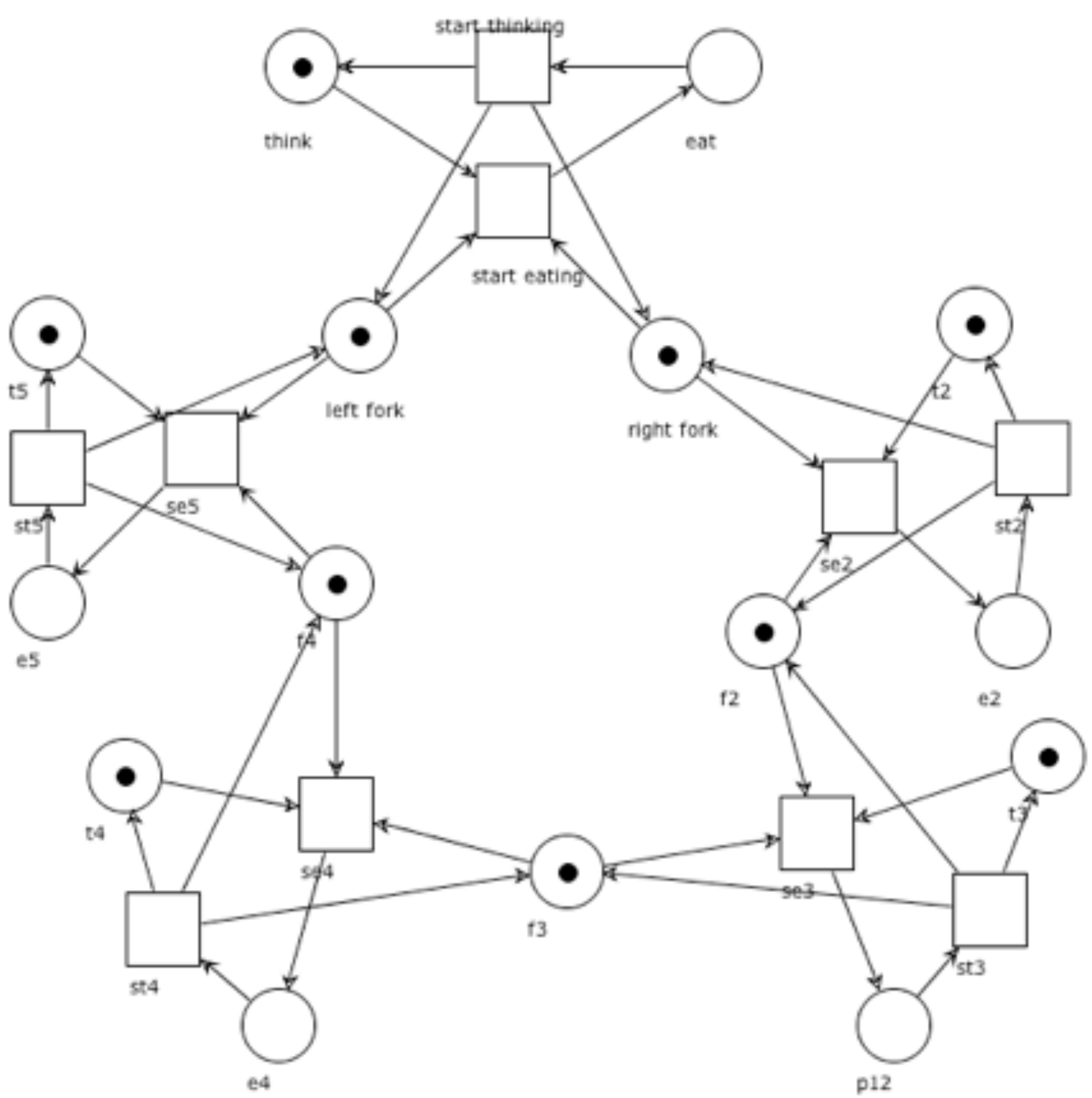
Traffic-lights example

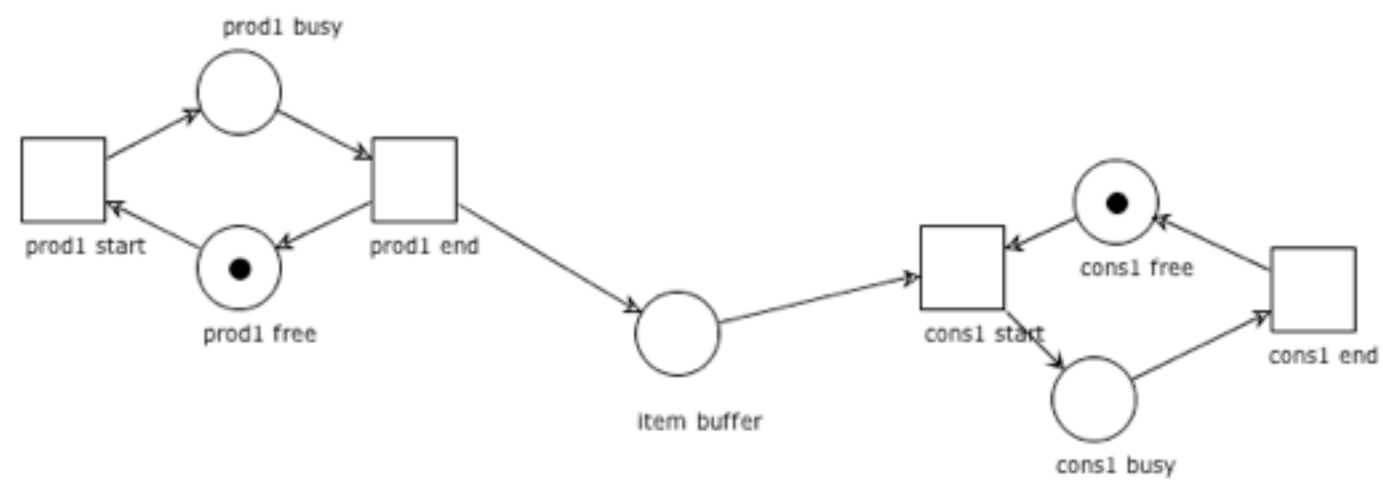


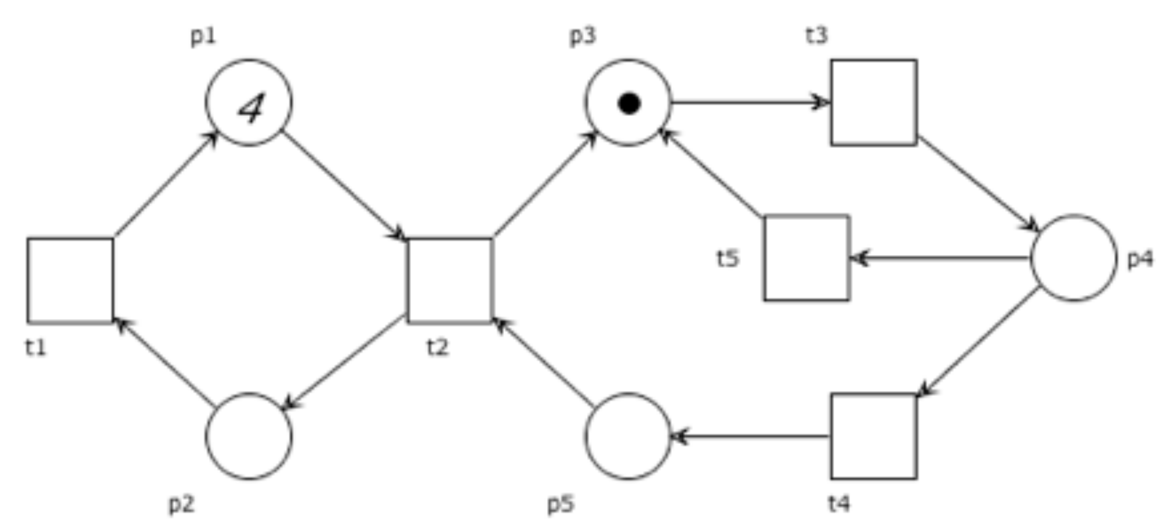
[1 1 1 0 0 0 0] +
[0 0 0 0 1 1 1] +
[1 1 0 1 1 1 0] =
[2 2 1 1 2 2 1]

Exercises

Define two (linearly independent) S-invariants for each of the nets below







S-invariants and system properties

Semi-positive S-invariants

The S-invariant $\mathbf{I}$ is **semi-positive** if $\mathbf{I} > \mathbf{0}$
(i.e. $\mathbf{I} \geq \mathbf{0}$ and $\mathbf{I} \neq \mathbf{0}$)

The **support** of $\mathbf{I}$ is: $\langle \mathbf{I} \rangle = \{ \, p \mid \mathbf{I}(p) > 0 \, \}$

The S-invariant $\mathbf{I}$ is **positive** if $\mathbf{I} \succ \mathbf{0}$
(i.e. $\mathbf{I}(p) > 0$ for any place $p \in P$)
(i.e. $\langle \mathbf{I} \rangle = P$)

A (semi-positive) S-invariant whose coefficients are all 0 and 1 is called **uniform**

Note

Notation: $\bullet S = \bigcup_{s \in S} \bullet s$

Every semi-positive invariant
satisfies the equation

$$\bullet\langle \mathbf{I} \rangle = \langle \mathbf{I} \rangle\bullet$$

pre-sets of support equal post-sets of support

(the result holds for both S-invariant and T-invariant)

A sufficient condition for boundedness

Theorem:
If (P, T, F, M_0) has a positive S-invariant then it is bounded

Let $M \in [\, M_0 \,\rangle$ and let $\mathbf{I}$ be a positive S-invariant.

Let $p \in P$. Then $\mathbf{I}(p)M(p) \leq \mathbf{I} \cdot M = \mathbf{I} \cdot M_0$

Since $\mathbf{I}$ is positive, we can divide by $\mathbf{I}(p)$:
$M(p) \leq (\mathbf{I} \cdot M_0)/\mathbf{I}(p)$

$$\mathbf{I} \cdot M = \sum_{q \in P} \mathbf{I}(q)M(q)$$

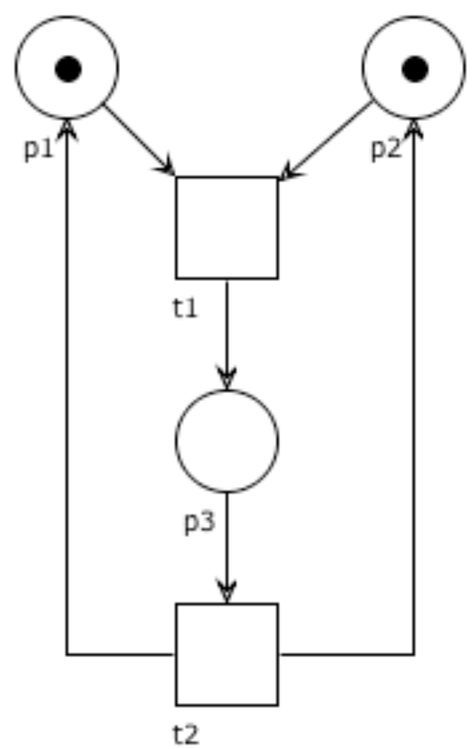
Consequences of previous theorem

By exhibiting a positive S-invariant we can prove that the system is **bounded for any initial marking**

Note that all places in the support of a semi-positive S-invariant are **bounded for any initial marking**

Example

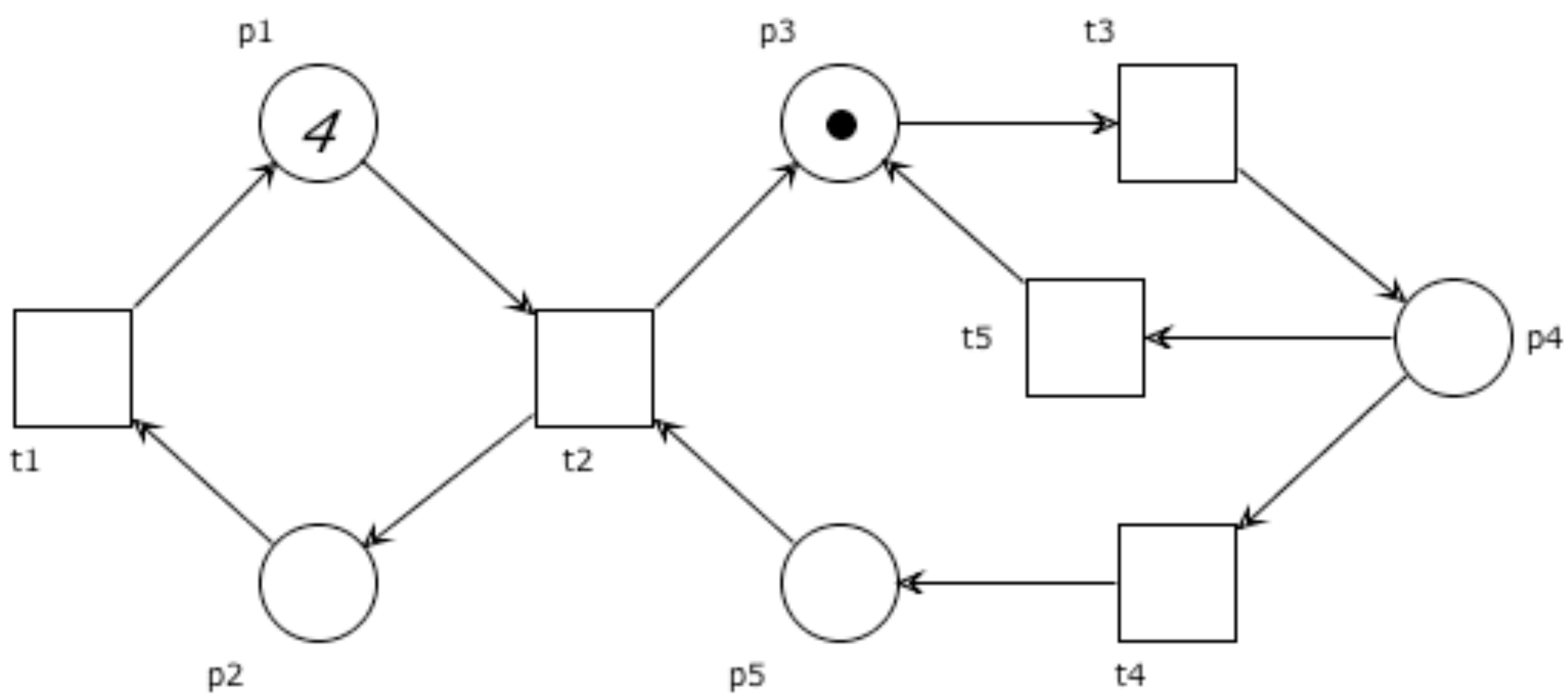
To prove that the system is bounded we can just exhibit a positive S-invariant



I = [1 1 2]

Exercises

Find a positive S-invariant for the net below



A necessary condition for liveness

Theorem:
If (P, T, F, M_0) is live then for every semi-positive invariant $\mathbf{I}$:

$$\mathbf{I} \cdot M_0 > 0$$

Let $p \in \langle \mathbf{I} \rangle$ and take any $t \in \bullet p \cup p\bullet$.

By liveness, there are $M, M' \in [\, M_0 \,\rangle$ with $M \xrightarrow{t} M'$

Then, $M(p) > 0$ (if $t \in p\bullet$) or $M'(p) > 0$ (if $t \in \bullet p$)

If $M(p) > 0$, then $\mathbf{I} \cdot M \geq \mathbf{I}(p)M(p) > 0$
If $M'(p) > 0$, then $\mathbf{I} \cdot M' \geq \mathbf{I}(p)M'(p) > 0$

In any case, $\mathbf{I} \cdot M_0 = \mathbf{I} \cdot M = \mathbf{I} \cdot M' > 0$

$$\mathbf{I} \cdot M = \sum_{q \in P} \mathbf{I}(q)M(q)$$

Consequence of previous theorem

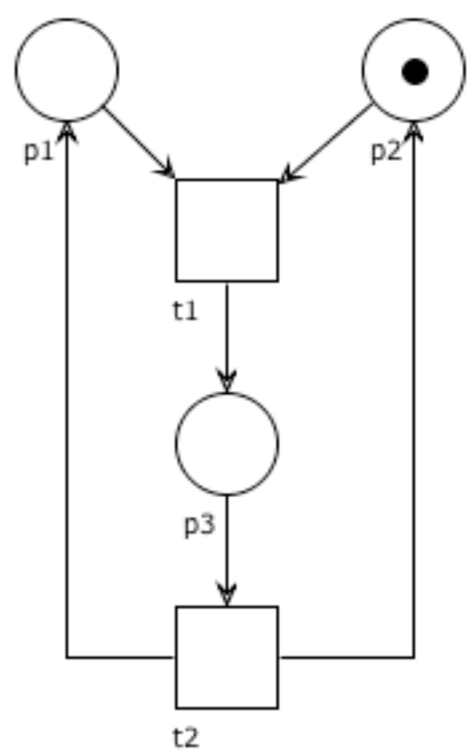
If we find a semi-positive invariant such that

$$\mathbf{I} \cdot M_0 = 0$$

Then we can conclude that the system **is not live**

Example

It is immediate to check the counter-example



$\mathbf{I} = [\ 1 \ \ 0 \ \ 1\ ]$

$$\underset{\mathbf{I}}{[\ 1\ 0\ 1\ ]} \underset{M_0}{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}} = 0$$

Markings that agree on all S-invariant

Definition: M and M' **agree on all S-invariants** if for every S-invariant **I** we have **I**$\cdot$M = **I**$\cdot$M'

Note: by properties of linear algebra, this corresponds to require that the equation on **y** M + **N**$\cdot$**y** = M' has some rational-valued solution

Remark: In general, there can exist M and M' that agree on all S-invariants but such that none of them is reachable from the other

A necessary condition for reachability

Reachability is decidable, but computationally expensive (EXPSPACE-hard)

S-invariants provide a preliminary check that can be computed efficiently

Let (P, T, F, M_0) be a system.

If there is an S-invariant $\mathbf{I}$ s.t. $\mathbf{I} \cdot M \neq \mathbf{I} \cdot M_0$ then $M \notin [\, M_0 \,\rangle$

If the equation $\mathbf{N} \cdot \mathbf{y} = M - M_0$ has no rational-valued solution, then $M \notin [\, M_0 \,\rangle$

S-invariants: recap

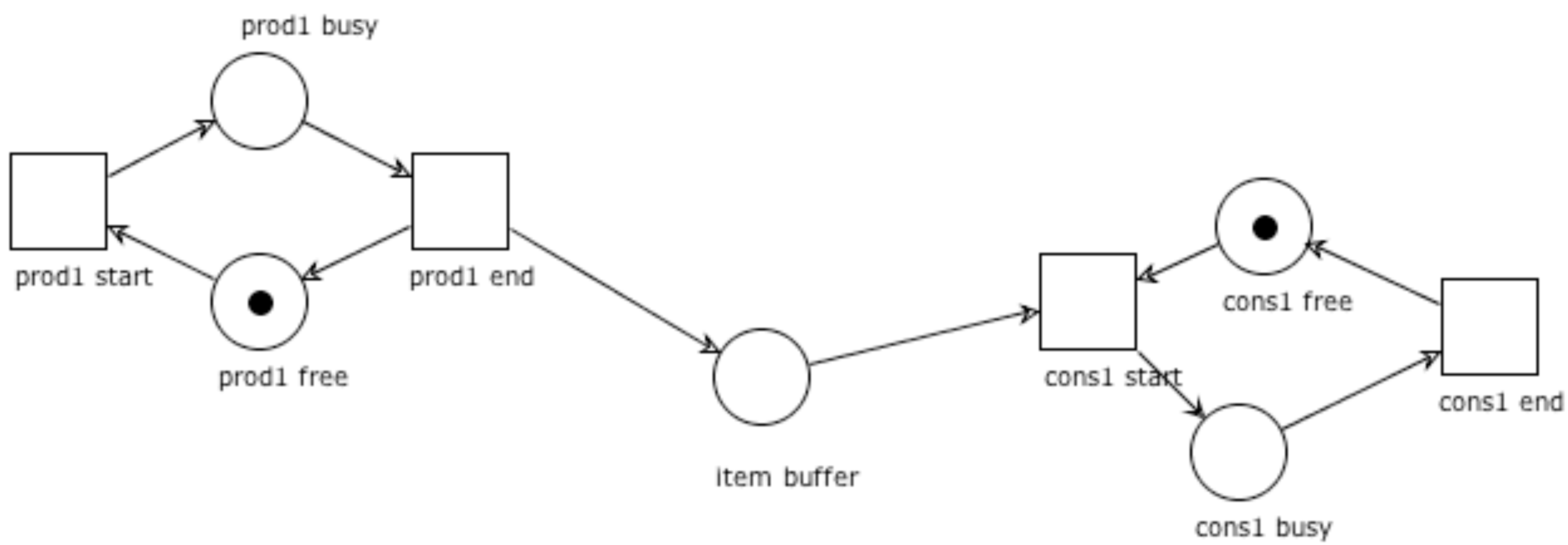
Positive S-invariant => boundedness
Unboundedness => no positive S-invariant

Semi-positive S-invariant **I** and liveness => $\mathbf{I} \cdot M_0 > 0$
Semi-positive S-invariant **I** and $\mathbf{I} \cdot M_0 = 0$ => non-live

S-invariant **I** and M reachable => $\mathbf{I} \cdot M = \mathbf{I} \cdot M_0$
S-invariant **I** and $\mathbf{I} \cdot M \neq \mathbf{I} \cdot M_0$ => M not reachable

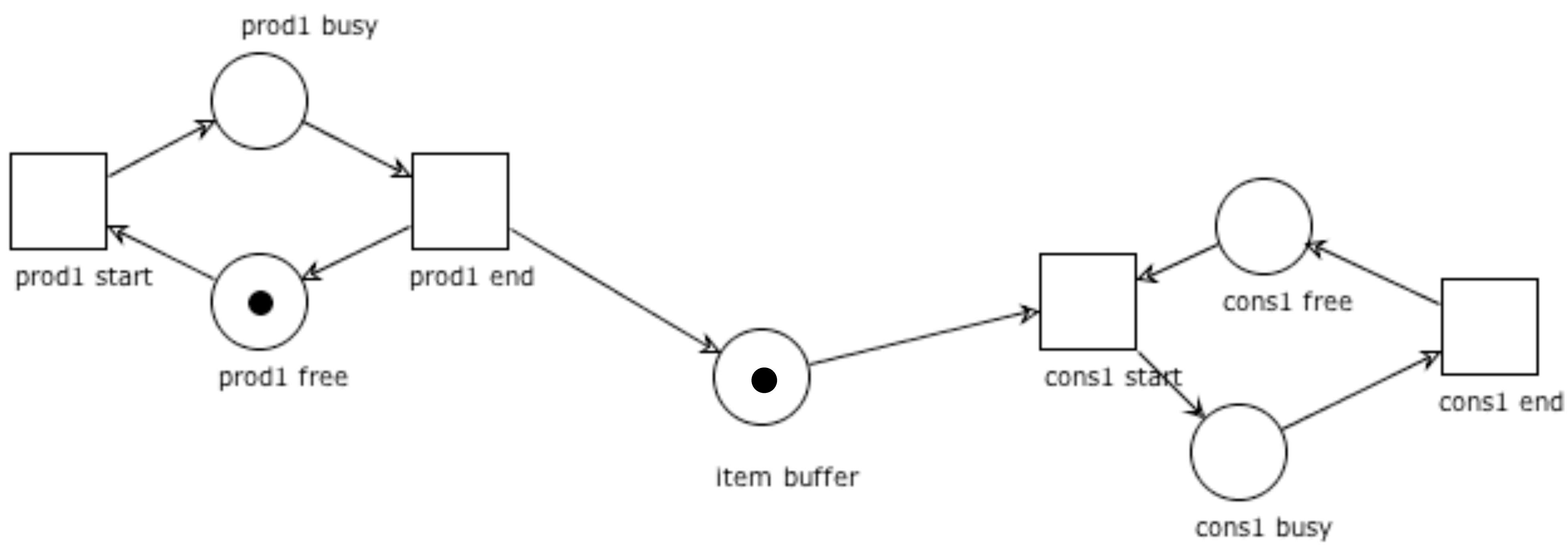
Exercises

Can you find a positive S-invariant?



Exercises

Prove that the system is not live by exhibiting a suitable S-invariant



T-invariants

Dual reasoning

The S-invariants of a net N are vectors satisfying the equation

$$\mathbf{x} \cdot \mathbf{N} = \mathbf{0}$$

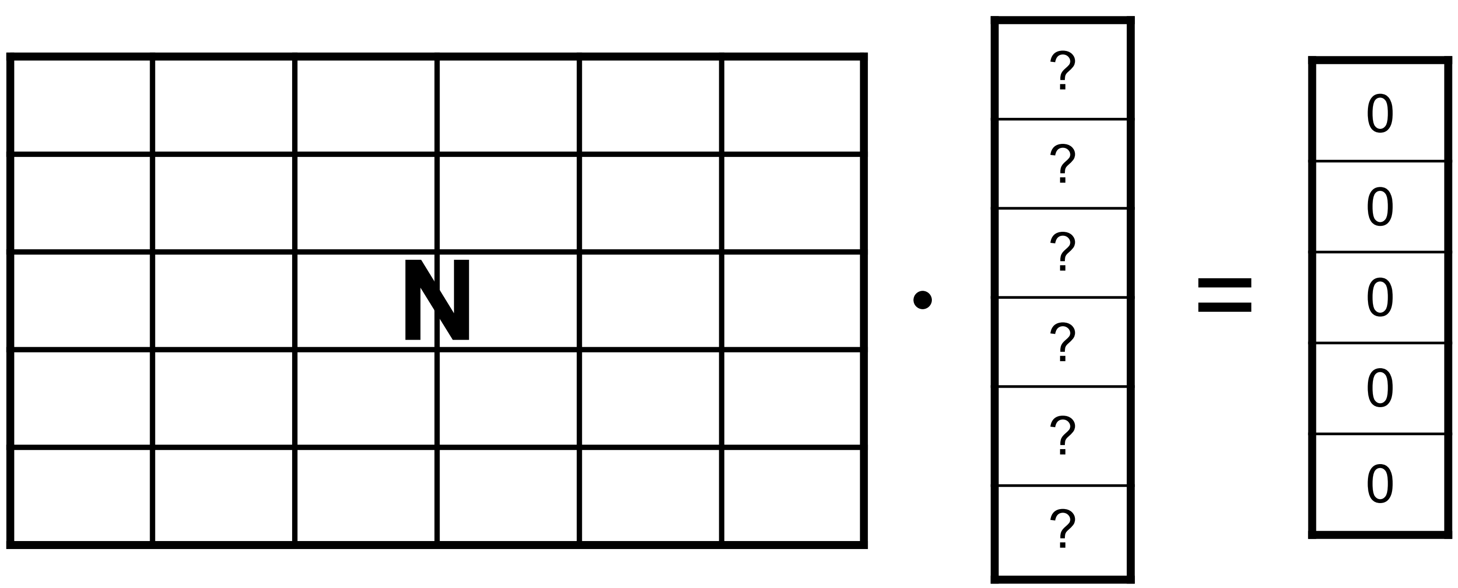
It seems natural to ask if we can find some interesting properties also for the vectors satisfying the equation

$$\mathbf{N} \cdot \mathbf{y} = \mathbf{0}$$

T-invariant
(aka transition-invariant)

Definition: A **T-invariant** of a net N=(P,T,F) is a rational-valued solution **y** of the equation

$$\mathbf{N} \cdot \mathbf{y} = \mathbf{0}$$



Fundamental property of T-invariants

Proposition: Let $M \xrightarrow{\sigma} M'$.

The Parikh vector $\vec{\sigma}$ is a T-invariant iff $M' = M$

$\Rightarrow$) By the marking equation lemma $M' = M + \mathbf{N} \cdot \vec{\sigma}$
Since $\vec{\sigma}$ is a T-invariant $\mathbf{N} \cdot \vec{\sigma} = \mathbf{0}$, thus $M' = M$.

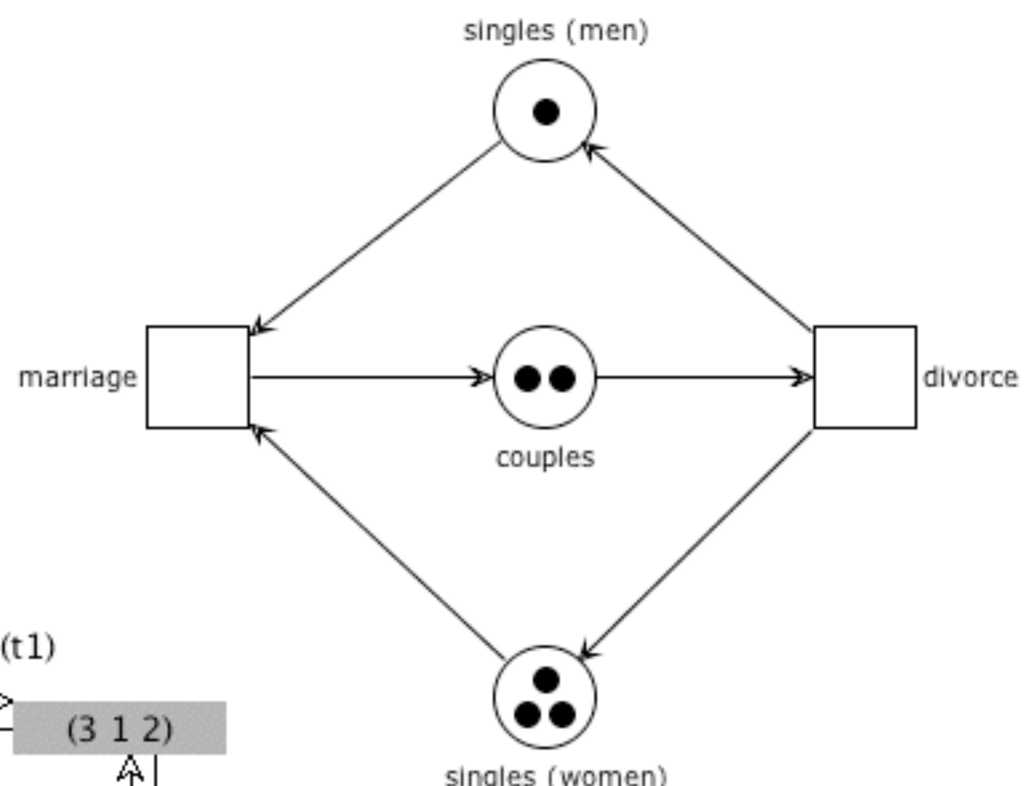
$\Leftarrow$) If $M \xrightarrow{\sigma} M$, by the marking equation lemma $M = M + \mathbf{N} \cdot \vec{\sigma}$
Thus $\mathbf{N} \cdot \vec{\sigma} = M - M = \mathbf{0}$ and $\vec{\sigma}$ is a T-invariant

Transition-invariant, intuitively

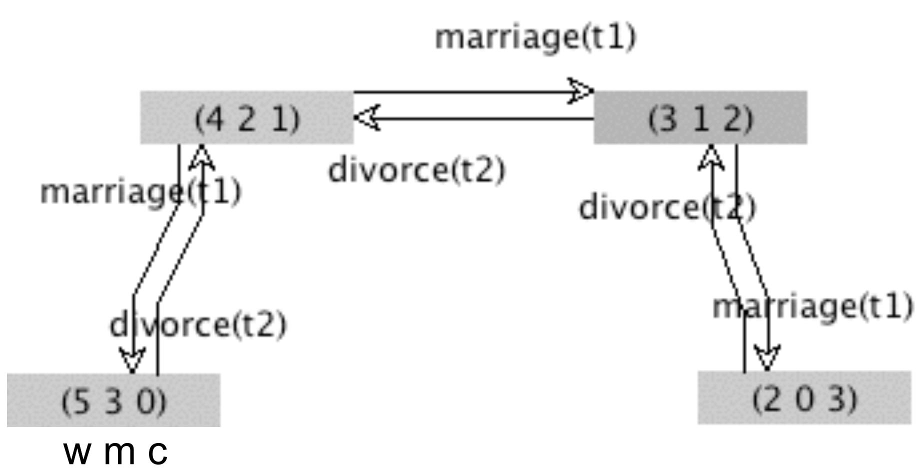
A transition-invariant assigns a **number of occurrences to each transition** such that any occurrence sequence comprising exactly those transitions leads to the same marking where it started (independently from the order of execution)

Example

An easy-to-be-found T-invariant



m d
[1 1]



Alternative definition of T-invariant

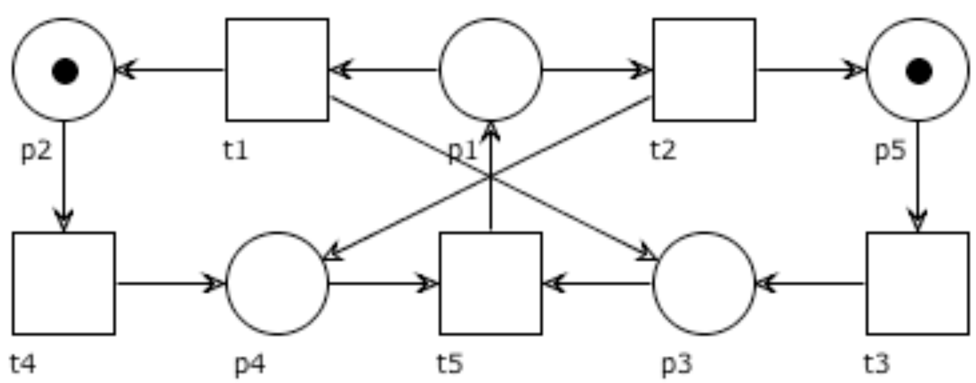
Proposition:

A mapping $\mathbf{J} : T \to \mathbb{Q}$ is a T-invariant of N iff for any $p \in P$:

$$\sum_{t \in \bullet p} \mathbf{J}(t) = \sum_{t \in p \bullet} \mathbf{J}(t)$$

Question time

Which of the following are T-invariants?



t_1	t_2	t_3	t_4	t_5
[1	0	0	1	1]
[1	1	2	1	2]
[1	1	1	0	2]
[1	1	1	1	2]
[0	1	1	0	1]

$$\forall p \in P, \ \sum_{t \in \bullet p} \mathbf{J}(t) \stackrel{?}{=} \sum_{t \in p \bullet} \mathbf{J}(t)$$

T-invariants and system properties

Pigeonhole principle

If n items are put into m slots, with n > m, then at least one slot must contain more than one item

Reproduction lemma

Lemma: Let (P, T, F, M_0) be a bounded system.
If $M_0 \xrightarrow{\sigma}$ for some infinite sequence σ, then
there is a semi-positive T-invariant $\mathbf{J}$ such that $\langle\, \mathbf{J}\, \rangle \subseteq \{\, t \mid t \in \sigma \,\}$.

Assume $\sigma = t_1\, t_2\, t_3 \ldots$ and $M_0 \xrightarrow{t_1} M_1 \xrightarrow{t_2} M_2 \xrightarrow{t_3} \ldots$

By boundedness: $[\, M_0 \,\rangle$ is finite.

By the pigeonhole principle, there are $0 \leq i < j$ s.t. $M_i = M_j$
Let $\sigma' = t_{i+1} \ldots t_j$. Then $M_i \xrightarrow{\sigma'} M_j = M_i$

By the marking equation lemma: $\vec{\sigma'}$ is a T-invariant. (fund. prop. of T-inv.)
It is semi-positive, because σ' is not empty $(i < j)$.
Clearly, $\langle\, \mathbf{J}\, \rangle$ only includes transitions in σ.

Boundedness, liveness and positive T-invariant

Theorem: If a bounded system is live, then it has a positive T-invariant

By boundedness: $[\, M_0 \,\rangle$ is finite and we let $k = |[\, M_0 \,\rangle|$.

By liveness: $M_0 \xrightarrow{\sigma_1} M_1$ with $\vec{\sigma_1}(t) > 0$ for any $t \in T$
Similarly: $M_1 \xrightarrow{\sigma_2} M_2$ with $\vec{\sigma_2}(t) > 0$ for any $t \in T$
Similarly: $M_0 \xrightarrow{\sigma_1} M_1 \xrightarrow{\sigma_2} M_2 ... \xrightarrow{\sigma_k} M_k$

By the pigeonhole principle, there are $0 \leq i < j \leq k$ s.t. $M_i = M_j$
Let $\sigma = \sigma_{i+1} ... \sigma_j$. Then $M_i \xrightarrow{\sigma} M_j = M_i$

By the marking equation lemma: $\vec{\sigma}$ is a T-invariant. (fund. prop. of T-inv.)
It is positive, because $\vec{\sigma}(t) \geq \vec{\sigma_j}(t) > 0$ for any $t \in T$.

Corollary of previous theorem

Every live and bounded system has:

a reachable marking M and
an occurrence sequence $M \stackrel{\sigma}{\longrightarrow} M$

such that <u>all transitions of N occur in σ.</u>

T-invariants: recap

Boundedness + liveness => positive T-invariant

No positive T-invariant => non (live + bounded)
No positive T-invariant => non-live OR unbounded
No positive T-invariant + liveness => unbounded
No positive T-invariant + boundedness => non-live
No positive T-inv. + positive S-inv. => non-live

Exercises

Exhibit a system that has a positive T-invariant
but is not
live and bounded

Exhibit a live system that has a positive T-invariant
but is not bounded