Beliefs and Plausibilities in Abstract Interpretation

Maja H. Kirkeby & Holger Axelsen

Roskilde University & Edlund A/S, Denmark

Contact Information:
Computer Science/ Dep. of People and Technology
Roskilde University,
Universitetsvej 1, 4000 Roskilde
Email: majaht@ruc.dk

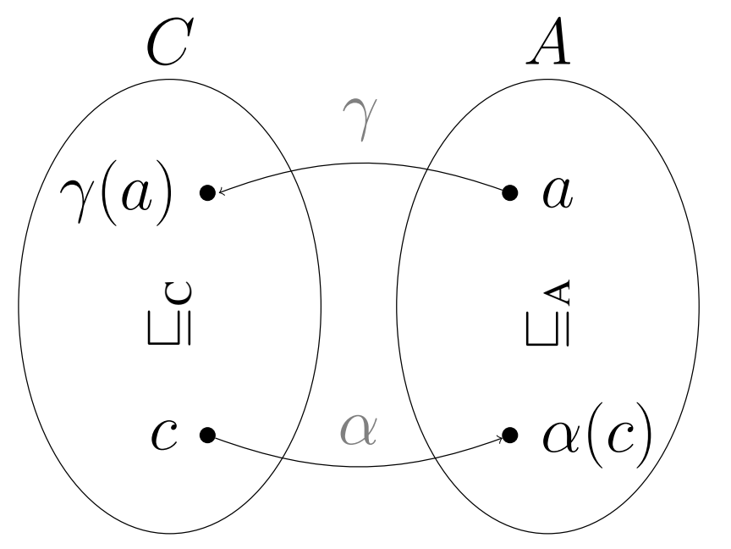
Introduction

Static Analysis of programs deduces properties of programs without executing them and can be expressed using Abstract Interpretation. A probabilistic analysis deduces program properties with respect to an input probability measure. We use Evidence theory to lift non-probabilistic analysis to probabilistic analysis of the same properties.

Abstract Interpretation

Two complete lattices (posets with well-defined least upper and greatest lower bounds) $(C, \sqsubseteq_\mathrm{C})$ and $(A, \sqsubseteq_\mathrm{A})$ are connected by a *Galois connection* $(C, \sqsubseteq_\mathrm{C}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \sqsubseteq_\mathrm{A})$ with an *abstraction* $\alpha\colon C \to A$ and *concretization* $\gamma\colon A \to C$ if $\alpha(c) \sqsubseteq_\mathrm{A} a \Leftrightarrow c \sqsubseteq_\mathrm{C} \gamma(a)$ whenever $a \in A$ and $c \in C$. The α uniquely determines γ and vice versa. A Galois connection is a *Galois insertion* if furthermore $\alpha \circ \gamma(a) = a$ holds.

Galois Connection:



$$c \sqsubseteq_\mathrm{C} \gamma(a) \Leftrightarrow \alpha(c) \sqsubseteq_\mathrm{A} a$$

Galois connection with transfer functions f and g:

$$\begin{tikzcd} A \arrow[r, "g"] & A' \arrow[d, "\gamma"] \\ C \arrow[u, "\alpha"] \arrow[r, "f"] & C' \arrow[u, phantom, "\sqsubseteq_\mathrm{C}"] \end{tikzcd}$$

A transfer function $f\colon \wp(C) \to \wp(C)$ is monotone and for a power domain $(\wp(C), \subseteq)$ it is distributive if written $f\colon C \to C$. For a Galois connection $(C, \sqsubseteq_\mathrm{C}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \sqsubseteq_\mathrm{A})$, an abstract transfer function $g\colon A \to A$ is an *upwards approximation* of the concrete transfer function $f\colon C \to C$, written $f \preceq_\sharp g$, iff

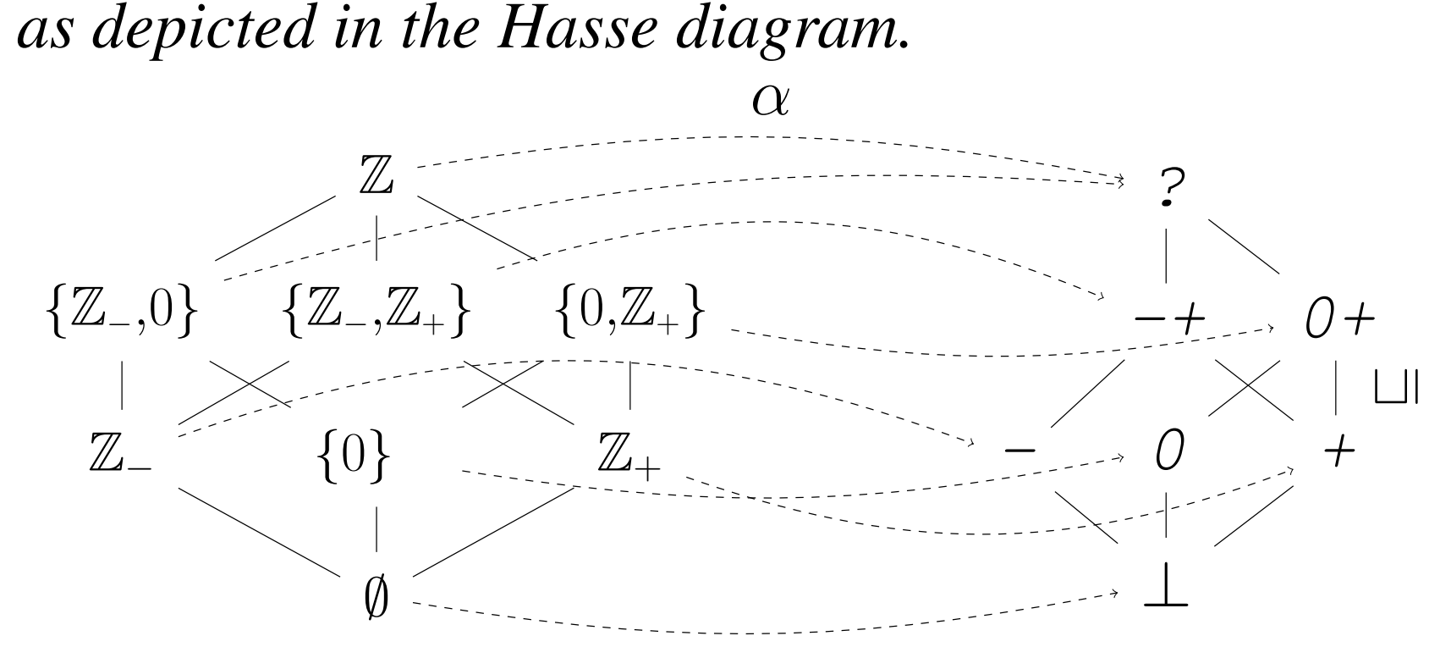
$$f \sqsubseteq_C \gamma \circ g \circ \alpha \qquad g \sqsupseteq_A \alpha \circ f \circ \gamma$$

and a *downwards* iff $g \sqsubseteq_A \alpha \circ f \circ \gamma$ and $f \sqsupseteq_C \gamma \circ g \circ \alpha$, written $f \preceq_\flat g$.

Example 1 (Intervals). *A classic example is abstracting sets of integers to intervals of integers using* $(\wp(\mathbb{Z}), \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (\mathcal{I}(\mathbb{Z}), \sqsubseteq_I)$. *where,* $\mathcal{I}(\mathbb{Z}) \triangleq \{[a,b] \mid a, b \in \mathbb{Z} \cup \{-\infty, \infty\}\colon a \leq b\}$ *and* $\sqsubseteq_I$ *is interval inclusion. The abstraction is defined for all non-empty sets* $\alpha(a) \triangleq [\min a, \max a]$ *where* $\min \mathbb{Z} \triangleq -\infty$ *and* $\max \mathbb{Z} \triangleq \infty$, *and the concretization* $\gamma([a,b]) \triangleq \{c \in \mathbb{Z} \mid a \leq c \leq b\}$.

Note that since the domains are infinite, the theory, presented here, does not cover the above example.

Example 2 (Sign). *The abstract domain may not be measurable. Let* $(\wp(\{\mathbb{Z}_-, 0, \mathbb{Z}_+\}), \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (\{\bot, -, 0, +, -0, -+, 0+, ?\}, \sqsubseteq)$ *with* $\sqsubseteq$ *and* α *as depicted in the Hasse diagram.*



Definition 1 (output probability measure). *Given a probability space* $(X, \mathcal{X}, \mu)$, *a measurable space* $(Y, \mathcal{Y})$, *and a measurable function* $f\colon X \to Y$ *then the* output probability measure $\mu_f\colon \mathcal{Y} \to [0,1]$ *of* f *is defined as*

$$\forall A \in \mathcal{Y}\colon\ \mu_f(A) = \mu(f^{-1}(A)).$$

A function f' *is a* probability-lifting of f *iff* $f'(\mu)(A) = \mu(f^{-1}(A))\colon \forall A \in \wp(X)$

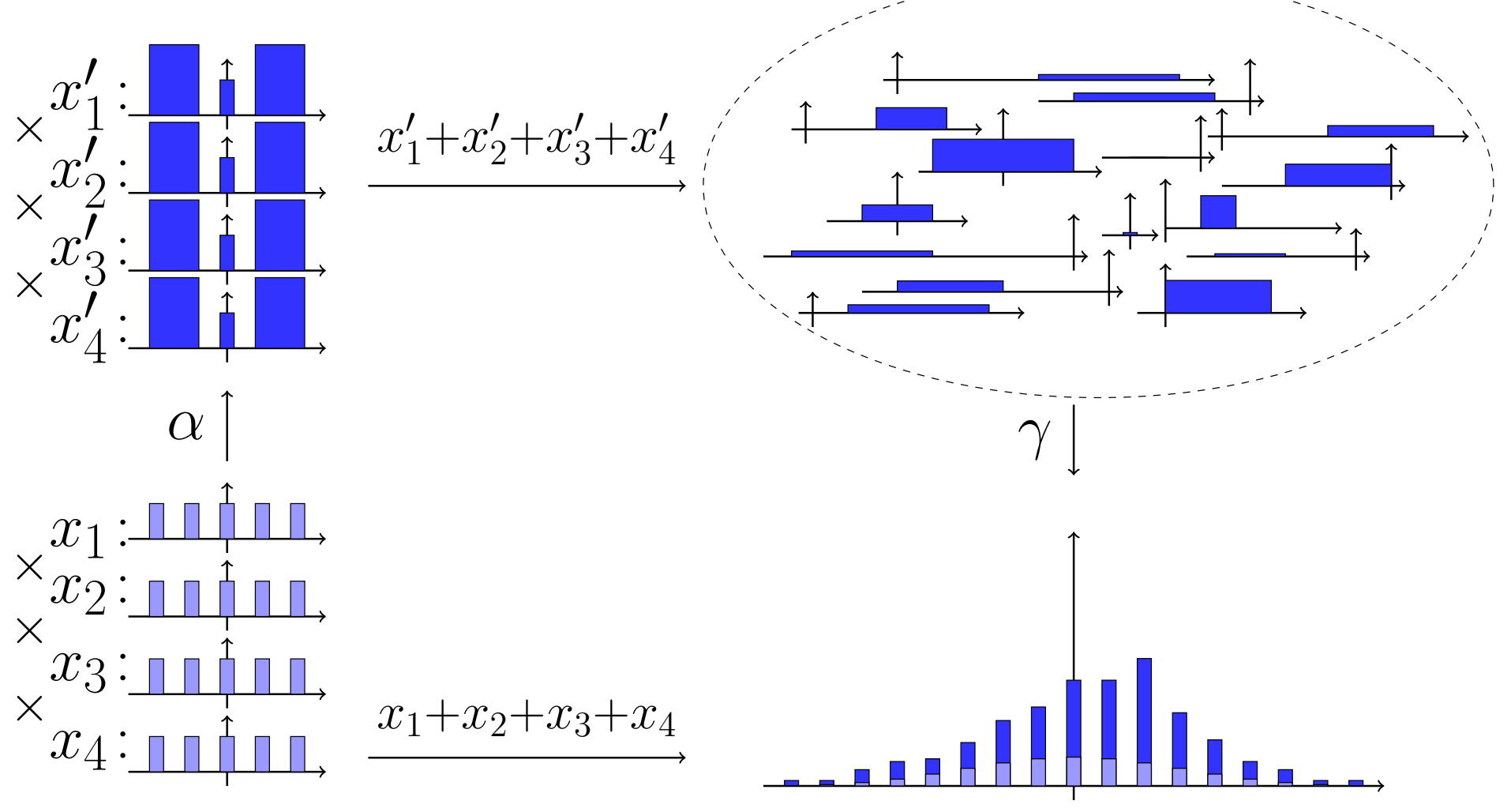
Definition 2. *Let* $(X, \mathcal{X}, \mu)$ *be a probability space and* $S \triangleq (\wp(C), \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \sqsubseteq)$ *be a Galois connection with transfer functions* $f\colon C \to C$ *and* $g\colon A \to A$, $f \preceq_\sharp g$. *Then a Galois connection* $(D, \sqsubseteq_D) \underset{\alpha'}{\overset{\gamma'}{\leftrightarrows}} (B, \sqsubseteq_B)$ *with transfer functions* f' *and* g' *is a* probability-lifted Galois of S *iff* f' *is probability-lifting of* f *and* $f' \preceq_\flat g'$ *or* $f' \preceq_\sharp g'$.

Background and Objective

In the pioneering paper "Abstract Interpretation of probabilistic semantics" from 2001, Monniaux presented an abstract interpretation capable of probabilistic analysis of both deterministic programs and probabilistic programs. He lifted the concrete semantics to transform probability measures and lifted the transfer function to continuous linear transformations between measure spaces (of norm less than 1, using the Banach norm of total variation). This part of his work relates to Kozen's "Semantics of Probabilistic Programs" from 1979. Monniaux's abstract domain is a set of sub-measures defined using a finite partition of the concrete domain. He also uses the abstract transfer function to define the probabilistic version, and following his lifting-method for the concrete domain he lifts the abstract domain.

We present a more intuitive abstract domain that is directly related to the original analysis using beliefs, plausibilities, basic probability assignments and abstract versions thereof.

Example 3 (Output). *A more complex probabilistic output analysis was constructed by Monniaux based on interval analysis over reals; here, we present a simpler version. He analyze a program that adds four real variables produced by random generators, i.e., they are independent and uniformly distributed. Here, we show a reduced version where the variables comes as input, and each input follows the uniform distribution over* $\{-2,-1,0,1,2\}$. *The abstract interpretation domains are as mentioned above, and the concretization sums the sub-measures' values for the interval of interest and obtain the over-approximation (dark blue) of the concrete probability measure (light blue).*



Bel, Pl and BPA

Definition 3. *The pre-image* pre_Γ *and dual-pre-image* $\widetilde{pre}_\Gamma$ *of the set-function* Γ *are defined as:*

$$pre_\Gamma(A) \triangleq \{x \in X \mid \Gamma(x) \cap A \neq \emptyset\}$$
$$\widetilde{pre}_\Gamma(A) \triangleq \{x \in X \mid \Gamma(x) \subseteq A\}.$$

Definition 4. *A set-function* $\Gamma : X \to \wp(Y)$ *and a probability space* $(X, \wp(X), \mu)$ *induces a belief* Bel *and plausibility* Pl *on* $(Y, \wp(Y))$ *by*

$$Bel(A) \triangleq \mu(\widetilde{pre}_\Gamma(A))$$
$$Pl(A) \triangleq \mu(pre_\Gamma(A))$$

Definition 5. *An upper (resp. lower) pre-image* $pre^\sharp_f$ *(resp.* $pre^\flat_f$*) of* f *is a function satisfying*

$$pre^\flat_f \subseteq \widetilde{pre}_f \subseteq pre_f \subseteq pre^\sharp_f.$$

Definition 6. *A* Basic Probability Assignment *(BPA) is a set function* $m\colon \wp(\mathcal{D}) \to [0,1]$ *iff (i)* $m(\emptyset) = 0$ *(ii)* $\sum_{A \in \wp(\mathcal{D})} m(A) = 1$ *(iii)* $\{A \in \wp(\mathcal{D}) \mid M(A) > 0\}$ *is finite.*

Results

Theorem 1 (Evidence Theory). *Given a probability space* $(X, \wp(X), \mu)$ *and Galois connection* $(\wp(X), \alpha, \gamma, S)$ *with transfer functions* $f\colon X \to X$ *and* $g\colon S \to S$ *where* $f \preceq_\sharp g$. *Then* $\mu^\sharp_f \triangleq \mu(pre^\sharp_f)$ *is a belief function and* $\mu^\flat_f(A) \triangleq \mu(\widetilde{pre}^\flat_f(A))$ *is a plausibility function that satisfy*

$$\mu^\flat_f \leq \mu_f \leq \mu^\sharp_f \qquad \text{and} \qquad \mu^\sharp_f(A) = 1 - \mu^\flat_f(A^\complement).$$

Lemma 1. *Let* X *be finite,* $\mathbf{Bel}_{\wp(\mathbf{X})}$ *be the set of all belief functions over* $\wp(X)$ *with function order* $\leq$ *and* $\mathbf{m}_{\wp(\mathbf{X})}$*be the set of all BPA over* $\wp(X)$ *with order* $m \sqsubseteq_m m' \triangleq \sum_{B \subseteq A} m(B) \leq \sum_{B \subseteq A} m'(B) \quad : \forall A \in \wp(X)$ *then*

$$(\mathbf{Bel}_{\wp(\mathbf{X})}, \leq) \underset{\alpha_b}{\overset{\gamma_b}{\leftrightarrows}} (\mathbf{m}_\mathbf{X}, \sqsubseteq_m)$$

is a Galois connection when

$$\alpha_b(Bel)(A) \triangleq \textstyle\sum_{B \subseteq A} (-1)^{|A-B|} Bel(B)$$
$$\gamma_b(m)(A) \triangleq \textstyle\sum_{B \subseteq A} m(B)$$

Definition 7 (Abstract BPA). *Given a lattice* S *with least element* $\bot$, *a function* $M\colon S \to [0,1]$ *is an* Abstract BPA *(Abstract BPA) iff (i)* $M(\bot) = 0$, *(ii)* $\sum_{s \in S} M(s) = 1$, *and (iii)* $\{s \in S \mid M(s) > 0\}$ *is finite.*

Lemma 2. *Let* $(\wp(X), \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (S, \sqsubseteq)$ *be a Galois insertion for which it holds that* $\gamma(\bot) = \emptyset$, *and let* $(\mathbf{M}_\mathbf{S}, \sqsubseteq_M)$ *be the set of all Abstract BPAs with order* $\sqsubseteq_M$: $M \sqsubseteq_M M' \triangleq \sum_{B \sqsubseteq A} M(B) \leq \sum_{B \sqsubseteq A} M'(B)$. *Then*

$$(\mathbf{m}_\mathbf{X}, \sqsubseteq_m) \underset{\alpha_m}{\overset{\gamma_m}{\leftrightarrows}} (\mathbf{M}_\mathbf{S}, \sqsubseteq_M)$$

is a Galois connection when α_m *and* γ_m *are defined by*

$$\alpha_m(m)(s) \triangleq \textstyle\sum_{A \in \alpha^{-1}(s)} m(A)$$
$$\gamma_m(M)(A) \triangleq \begin{cases} M(\alpha(A)) & \text{if } A = \gamma(\alpha(A)) \\ 0 & \text{otherwise} \end{cases}$$

Theorem 2. *Let* $(X, \wp(X), \mu)$ *be a probability space and* $(\wp(X), \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (S, \sqsubseteq)$ *be a Galois insertion with transfer functions* f *and* g *such that* f *is distributive and* $f \preceq_\sharp g$. *Let* $(\mathbf{Bel}_{\wp(\mathbf{X})}, \leq) \underset{\alpha_b}{\overset{\gamma_b}{\leftrightarrows}} (\mathbf{m}_\mathbf{X}, \sqsubseteq_m)$ *and* $(\mathbf{m}_\mathbf{X}, \sqsubseteq_m) \underset{\alpha_m}{\overset{\gamma_m}{\leftrightarrows}} (\mathbf{M}_\mathbf{S}, \sqsubseteq_M)$ *be Galois connections, as above. Then* $f_b =_\flat f_m$ *and* $f_m \preceq_\flat g_m$ *holds for transfer functions* $f_b(Bel)'(A) \triangleq Bel(\bigcup f^{-1}(A))$, $f_m(m)(A) \triangleq \sum_{B \in f^{-1}(A)} m(B)$, *and* $g_m(M) \triangleq \sum_{s' \in g^{-1}(s)} M(s')$.

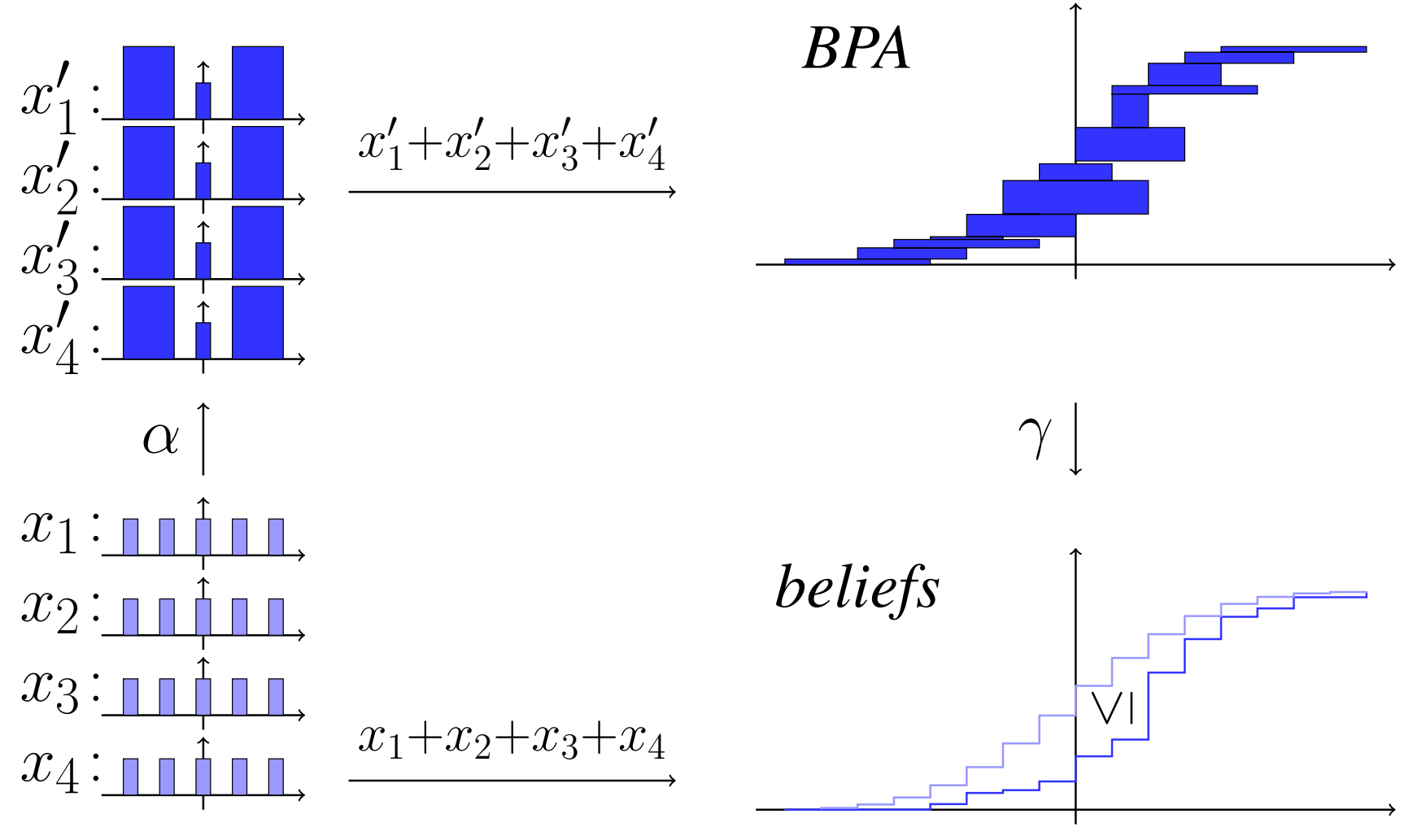
Theorem 3. *Let* $\mathcal{G} \triangleq (\wp(X), \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (S, \sqsubseteq)$ *be a Galois insertion for which it holds that* $\gamma(\bot) = \emptyset$, X *is finite, and* $f\colon X \to X$ *and* $g\colon S \to S$ *transfer functions so that* $f \preceq_\sharp g$ *then the Galois connection*

$$(\mathbf{Bel}_{\wp(\mathbf{X})}, \leq) \underset{\alpha_m \circ \alpha_b}{\overset{\gamma_b \circ \gamma_m}{\leftrightarrows}} (\mathbf{M}_\mathbf{S}, \sqsubseteq_M)$$

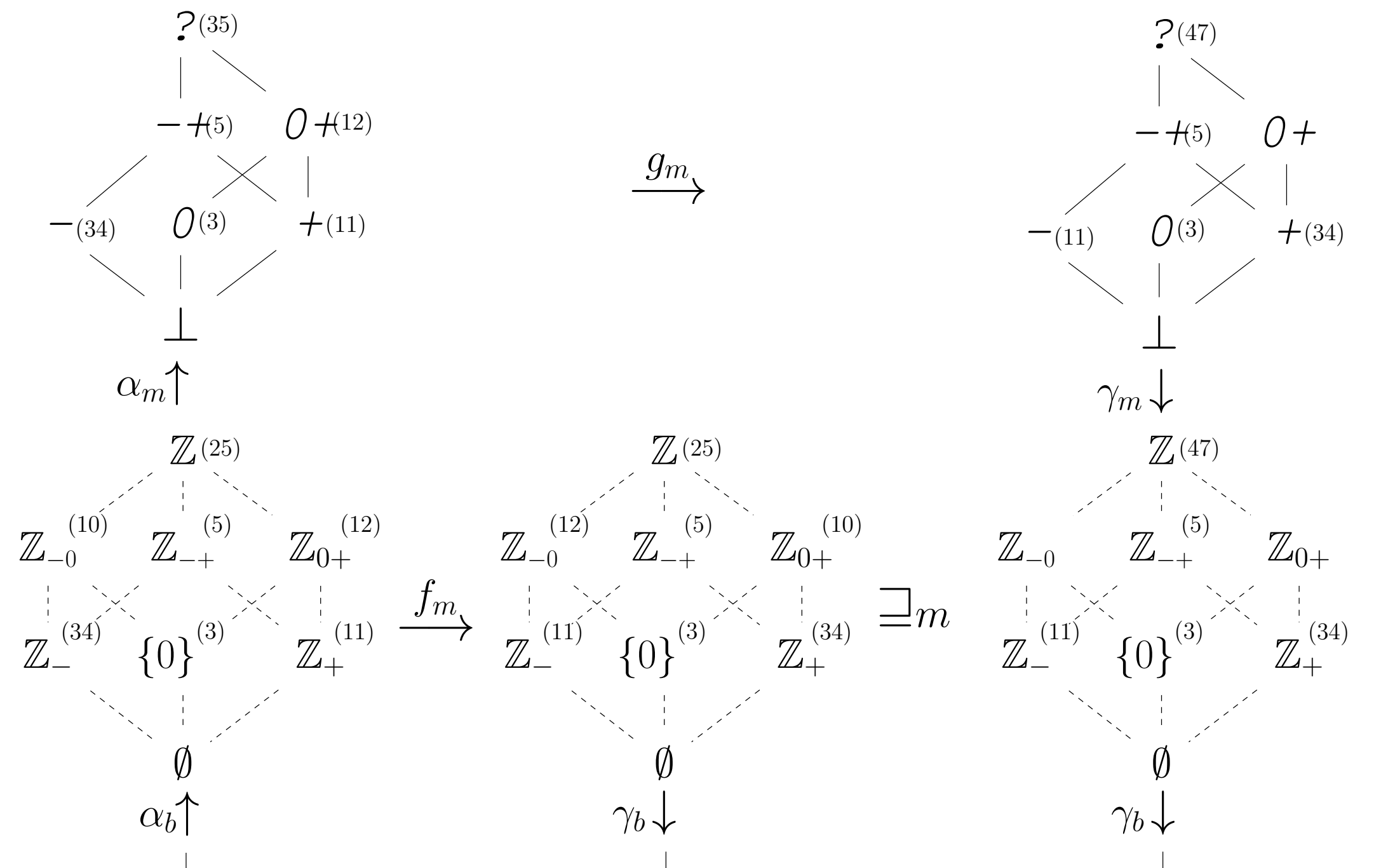
with transfer functions f_b *and* g_m *(as in Theorem 2) is a* probability-lifted Galois of $\mathcal{G}$ *with* $f_b \preceq_\flat g_m$.

Examples

Example 4. *(Example 3 cont.) In our framework we lift The program:* `add4`$(\mathtt{x_1}, \mathtt{x_2}, \mathtt{x_3}, \mathtt{x_4}) = \mathtt{x_1} + \mathtt{x_2} + \mathtt{x_3} + \mathtt{x_4}$.



Example 5 (Sign). *(Example 2 cont.) We analyse a simple integer program:* `prg(x) = x*(-1)` *using a standard Detection of Sign analysis. We can (a bit simplistic) represent the concrete transformation carried out by the program as* $f(x) = -x$ *and the associated abstract transformation as* $g(?) = ?, g(-+) = -+, g(0+) = ?, g(-) = +, g(0) = 0, g(+) = -, g(\bot) = \bot$. *Note especially the transformation of* $g(0+) = ?$ *which will also push the belief masses of the transformed Abstract BPA when compared to the transformed BPA.*



	Bel		Bel
$\emptyset$	0	$\mathbb{Z}_{-0}$	47
$\{0\}$	3	$\mathbb{Z}_{-+}$	50
$\mathbb{Z}_-$	34	$\mathbb{Z}_{0+}$	26
$\mathbb{Z}_+$	11	$\mathbb{Z}$	100

$\xrightarrow{f_b}$

	Bel'		Bel'
$\emptyset$	0	$\mathbb{Z}_{-0}$	26
$\{0\}$	3	$\mathbb{Z}_{-+}$	50
$\mathbb{Z}_-$	11	$\mathbb{Z}_{0+}$	47
$\mathbb{Z}_+$	34	$\mathbb{Z}$	100

$\geq$

	Bel''		Bel''
$\emptyset$	0	$\mathbb{Z}_{-0}$	14
$\{0\}$	3	$\mathbb{Z}_{-+}$	50
$\mathbb{Z}_-$	11	$\mathbb{Z}_{0+}$	37
$\mathbb{Z}_+$	34	$\mathbb{Z}$	100

Acknowledgements The research leading to these results has been supported by EU FP7 project 318337, ENTRA - Whole-Systems Energy Transparency.