

# Deciding knowledge in security protocols for monoidal equational theories

Véronique Cortier and Stéphanie Delaune

LORIA, CNRS & INRIA project Cassis, Nancy, France

July 8, 2007

# Context: cryptographic protocols

Messages are abstracted by terms ...

- encryption  $\{x\}_y$ ,
- pairing  $\langle x, y \rangle, \dots$

... together with an equational theory

- classical theory:

$$\text{proj}_1(\langle x, y \rangle) = x \quad \text{proj}_2(\langle x, y \rangle) = y \quad \text{dec}(\text{enc}(x, y), y) = x$$

- exclusive or (ACUN):

$$\begin{array}{ll} (x + y) + z = x + (y + z) & \text{(A)} \\ x + 0 = x & \text{(U)} \end{array} \quad \begin{array}{ll} x + y = y + x & \text{(C)} \\ x + x = 0 & \text{(N)} \end{array}$$

# Context: cryptographic protocols

Messages are abstracted by terms ...

- encryption  $\{x\}_y$ ,
- pairing  $\langle x, y \rangle$ , ...

... together with an equational theory

- classical theory:

$$\text{proj}_1(\langle x, y \rangle) = x \quad \text{proj}_2(\langle x, y \rangle) = y \quad \text{dec}(\text{enc}(x, y), y) = x$$

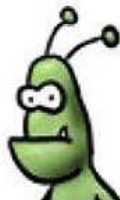
- exclusive or (ACUN):

$$\begin{array}{ll} (x + y) + z = x + (y + z) & \text{(A)} \\ x + 0 = x & \text{(U)} \end{array} \quad \begin{array}{ll} x + y = y + x & \text{(C)} \\ x + x = 0 & \text{(N)} \end{array}$$

Understanding security protocols often requires reasoning about **knowledge** of the attacker.

Two main kinds of knowledge

- deduction,
- static equivalence – indistinguishability



→ often used as **subroutines** in many decision procedures

# Deduction

$$\frac{}{T \vdash_E M} M \in T \qquad \frac{T \vdash_E M_1 \quad \dots \quad T \vdash_E M_k}{T \vdash_E f(M_1, \dots, M_k)} f \in \Sigma$$

$$\frac{T \vdash M}{T \vdash M'} M =_E M'$$

Example: Let  $E := \text{dec}(\text{enc}(x, y), y) = x$  and  $T = \{\text{enc}(\text{secret}, k), k\}$ .

$$\frac{\frac{}{T \vdash \text{enc}(\text{secret}, k)} \quad \frac{}{T \vdash k}}{T \vdash \text{dec}(\text{enc}(\text{secret}, k), k)} f \in \Sigma}{T \vdash \text{secret}} \text{dec}(\text{enc}(x, y), y) = x$$

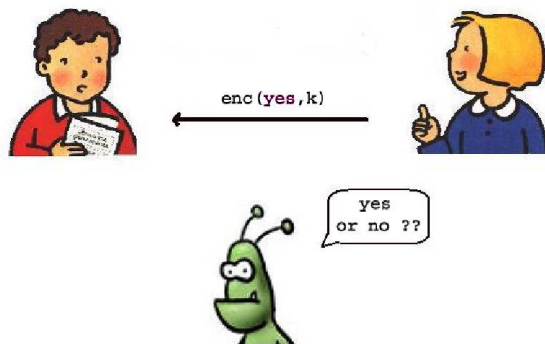
$$\frac{}{T \vdash_E M} M \in T \qquad \frac{T \vdash_E M_1 \quad \dots \quad T \vdash_E M_k}{T \vdash_E f(M_1, \dots, M_k)} f \in \Sigma$$

$$\frac{T \vdash M}{T \vdash M'} M =_E M'$$

**Example:** Let  $E := \text{dec}(\text{enc}(x, y), y) = x$  and  $T = \{\text{enc}(\text{secret}, k), k\}$ .

$$\frac{\frac{}{T \vdash \text{enc}(\text{secret}, k)} \quad \frac{}{T \vdash k}}{T \vdash \text{dec}(\text{enc}(\text{secret}, k), k)} f \in \Sigma}{T \vdash \text{secret}} \text{dec}(\text{enc}(x, y), y) = x$$

# Deduction is not always sufficient



→ The intruder **knows** the values **yes** and **no** !

## The real question

Is the intruder able to tell whether Alice sends **yes** or **no**?

# Static equivalence

frame = set of **restricted names** + sequence of messages

$$\phi = \nu \tilde{n}. \{M_1/x_1, \dots, M_\ell/x_\ell\}$$

Examples:

- If the key  $k$  is not revealed, we have that

$$\phi_1 = \nu k. \{\text{enc}(\text{yes}, k)/x\} \quad \text{and} \quad \phi_2 = \nu k. \{\text{enc}(\text{no}, k)/x\}$$

- If the key  $k$  is revealed, we have that

$$\psi_1 = \nu k. \{k/x_1, \text{enc}(\text{yes}, k)/x_2\} \quad \text{and} \quad \psi_2 = \nu k. \{k/x_1, \text{enc}(\text{no}, k)/x_2\}$$

# Static equivalence

frame = set of **restricted names** + sequence of messages

$$\phi = \nu \tilde{n}. \{M_1/x_1, \dots, M_\ell/x_\ell\}$$

Examples:

- If the key  **$k$  is not revealed**, we have that

$$\phi_1 = \nu k. \{\text{enc}(\text{yes}, k)/x\} \quad \text{and} \quad \phi_2 = \nu k. \{\text{enc}(\text{no}, k)/x\}$$

- If the key  **$k$  is revealed**, we have that

$$\psi_1 = \nu k. \{k/x_1, \text{enc}(\text{yes}, k)/x_2\} \quad \text{and} \quad \psi_2 = \nu k. \{k/x_1, \text{enc}(\text{no}, k)/x_2\}$$

# Static equivalence

frame = set of **restricted names** + sequence of messages

$$\phi = \nu \tilde{n}. \{M_1/x_1, \dots, M_\ell/x_\ell\}$$

Examples:

- If the key  **$k$  is not revealed**, we have that

$$\phi_1 = \nu k. \{\text{enc}(\text{yes}, k)/x\} \quad \text{and} \quad \phi_2 = \nu k. \{\text{enc}(\text{no}, k)/x\}$$

- If the key  **$k$  is revealed**, we have that

$$\psi_1 = \nu k. \{k/x_1, \text{enc}(\text{yes}, k)/x_2\} \quad \text{and} \quad \psi_2 = \nu k. \{k/x_1, \text{enc}(\text{no}, k)/x_2\}$$

# Static equivalence

frame = set of **restricted names** + sequence of messages

$$\phi = \nu \tilde{n}. \{M_1/x_1, \dots, M_\ell/x_\ell\}$$

Examples:

- If the key  **$k$  is not revealed**, we have that

$$\phi_1 = \nu k. \{\text{enc}(\text{yes}, k)/x\} \quad \text{and} \quad \phi_2 = \nu k. \{\text{enc}(\text{no}, k)/x\}$$

→ indistinguishable

- If the key  **$k$  is revealed**, we have that

$$\psi_1 = \nu k. \{k/x_1, \text{enc}(\text{yes}, k)/x_2\} \quad \text{and} \quad \psi_2 = \nu k. \{k/x_1, \text{enc}(\text{no}, k)/x_2\}$$

→ distinguishable

# Goal of this paper

A **general approach** for deciding deduction and static equivalence

- to deal with the class of **monoidal theories**  
→ **AC-like equational theories** with homomorphism operators

$$h(x + y) = h(x) + h(y)$$

- based on an **algebraic characterization** (semiring)
- many **decidability** and **complexity** results with several **new ones**

# Outline of the talk

- 1 Monoidal theories / semirings
- 2 Deduction
- 3 Static equivalence
- 4 Applications

## Definition (Nutt'90)

A theory  $E$  over  $\Sigma$  is called **monoidal** if:

- $\Sigma$  contains  $+$  (binary),  $0$  (constant) and all other function symbols are unary,
- $+$  is AC symbol with unit  $0$ ,
- for every unary  $h \in \Sigma$ , we have  $h(x + y) = h(x) + h(y)$  and  $h(0) = 0$ .

Examples:

- 1 ACU: AC with unit  $0$ , *i.e.*  $0 + x = x$ ,
- 2 ACUI: ACU with idempotency  $x + x = x$ ,
- 3 ACUN (Exclusive Or): ACU with nilpotency  $x + x = 0$ ,
- 4 AG (Abelian groups): ACU with  $x + -(x) = 0$  (Inv),
- 5 ACUh, ACUIh, ACUNh, AGh, ...

## Definition (Nutt'90)

A theory  $E$  over  $\Sigma$  is called **monoidal** if:

- $\Sigma$  contains  $+$  (binary),  $0$  (constant) and all other function symbols are unary,
- $+$  is AC symbol with unit  $0$ ,
- for every unary  $h \in \Sigma$ , we have  $h(x + y) = h(x) + h(y)$  and  $h(0) = 0$ .

## Examples:

- 1 **ACU**: AC with unit  $0$ , *i.e.*  $0 + x = x$ ,
- 2 **ACUI**: ACU with idempotency  $x + x = x$ ,
- 3 **ACUN** (Exclusive Or): ACU with nilpotency  $x + x = 0$ ,
- 4 **AG** (Abelian groups): ACU with  $x + -(x) = 0$  (Inv),
- 5 **ACUh**, **ACUIh**, **ACUNh**, **AGh**, ...

# Monoidal theories defines semiring

[Nutt'90]

→ for any monoidal theory  $E$  there exists a corresponding semiring  $\mathcal{S}_E$

Examples:

- AG →  $(\mathbb{Z}, +, \cdot)$  – ring of integers,

$$\begin{aligned}t &= x + x + x \rightsquigarrow 3 \\u &= -(a + a) \rightsquigarrow -2 \\t[x \mapsto u] &\rightsquigarrow 3 \cdot (-2) = -6\end{aligned}$$

- ACU →  $(\mathbb{N}, +, \cdot)$  – semiring of natural numbers,
- ACUh →  $(\mathbb{N}[h], +, \cdot)$  – semiring of polynomials in one indeterminate with coefficient in  $\mathbb{N}$ ,

$$h(a) + h(h(a)) \rightsquigarrow h + h^2$$

# Monoidal theories defines semiring

[Nutt'90]

→ for any monoidal theory  $E$  there exists a corresponding semiring  $\mathcal{S}_E$

Examples:

- $AG \rightarrow (\mathbb{Z}, +, \cdot)$  – ring of integers,

$$\begin{aligned}t &= x + x + x \rightsquigarrow 3 \\u &= -(a + a) \rightsquigarrow -2 \\t[x \mapsto u] &\rightsquigarrow 3 \cdot (-2) = -6\end{aligned}$$

- $ACU \rightarrow (\mathbb{N}, +, \cdot)$  – semiring of natural numbers,
- $ACUh \rightarrow (\mathbb{N}[h], +, \cdot)$  – semiring of polynomials in one indeterminate with coefficient in  $\mathbb{N}$ ,

$$h(a) + h(h(a)) \rightsquigarrow h + h^2$$

# Representation of terms and frames

We generalize the previous construction.

Let  $\mathcal{B} = [b_1, \dots, b_m]$  be a base, *i.e.* a sequence of free symbols.

$$\psi_{\mathcal{B}} : \mathcal{T}(\Sigma, \{b_1, \dots, b_m\}) \rightarrow \mathcal{S}_{\mathcal{E}}^m$$

Example: theory ACU –  $\mathcal{B} = [n_1, n_2, n_3]$

• Term built on  $\mathcal{B}$      $M = 3n_1 + 2n_2 + 3n_3 \rightsquigarrow (3, 2, 3)$

• Frame built on  $\mathcal{B}$  and saturated w.r.t.  $\mathcal{B}$

Let  $\phi = \nu n_1, n_2, n_3. \{3n_1 + 2n_2 + 3n_3 / x_1, n_2 + 3n_3 / x_2, 3n_2 + n_3 / x_3, 3n_1 + n_2 + 4n_3 / x_4\}$

$$\phi \rightsquigarrow \begin{pmatrix} 3 & 2 & 3 \\ 0 & 1 & 3 \\ 0 & 3 & 1 \\ 3 & 1 & 4 \end{pmatrix} \quad \text{since}$$

- $\psi_{\mathcal{B}}(3n_1 + 2n_2 + 3n_3) = (3, 2, 3)$ ,
- $\psi_{\mathcal{B}}(n_2 + 3n_3) = (0, 1, 3)$ ,
- $\psi_{\mathcal{B}}(3n_2 + n_3) = (0, 3, 1)$ , and
- $\psi_{\mathcal{B}}(3n_1 + n_2 + 4n_3) = (3, 1, 4)$ .

# Representation of terms and frames

We generalize the previous construction.

Let  $\mathcal{B} = [b_1, \dots, b_m]$  be a base, *i.e.* a sequence of free symbols.

$$\psi_{\mathcal{B}} : \mathcal{T}(\Sigma, \{b_1, \dots, b_m\}) \rightarrow \mathcal{S}_{\mathcal{E}}^m$$

**Example:** theory ACU –  $\mathcal{B} = [n_1, n_2, n_3]$

- Term built on  $\mathcal{B}$      $M = 3n_1 + 2n_2 + 3n_3 \rightsquigarrow (3, 2, 3)$

- Frame built on  $\mathcal{B}$  and saturated w.r.t.  $\mathcal{B}$

Let  $\phi = \nu n_1, n_2, n_3. \{3n_1+2n_2+3n_3/x_1, n_2+3n_3/x_2, 3n_2+n_3/x_3, 3n_1+n_2+4n_3/x_4\}$

$$\phi \rightsquigarrow \begin{pmatrix} 3 & 2 & 3 \\ 0 & 1 & 3 \\ 0 & 3 & 1 \\ 3 & 1 & 4 \end{pmatrix} \quad \text{since}$$

- $\psi_{\mathcal{B}}(3n_1 + 2n_2 + 3n_3) = (3, 2, 3)$ ,
- $\psi_{\mathcal{B}}(n_2 + 3n_3) = (0, 1, 3)$ ,
- $\psi_{\mathcal{B}}(3n_2 + n_3) = (0, 3, 1)$ , and
- $\psi_{\mathcal{B}}(3n_1 + n_2 + 4n_3) = (3, 1, 4)$ .

# Representation of terms and frames

We generalize the previous construction.

Let  $\mathcal{B} = [b_1, \dots, b_m]$  be a base, *i.e.* a sequence of free symbols.

$$\psi_{\mathcal{B}} : \mathcal{T}(\Sigma, \{b_1, \dots, b_m\}) \rightarrow \mathcal{S}_E^m$$

**Example:** theory ACU –  $\mathcal{B} = [n_1, n_2, n_3]$

• Term built on  $\mathcal{B}$      $M = 3n_1 + 2n_2 + 3n_3 \rightsquigarrow (3, 2, 3)$

• Frame built on  $\mathcal{B}$  and saturated w.r.t.  $\mathcal{B}$

Let  $\phi = \nu n_1, n_2, n_3. \{ 3n_1 + 2n_2 + 3n_3 /_{x_1}, n_2 + 3n_3 /_{x_2}, 3n_2 + n_3 /_{x_3}, 3n_1 + n_2 + 4n_3 /_{x_4} \}$

$$\phi \rightsquigarrow \begin{pmatrix} 3 & 2 & 3 \\ 0 & 1 & 3 \\ 0 & 3 & 1 \\ 3 & 1 & 4 \end{pmatrix} \quad \text{since}$$

- $\psi_{\mathcal{B}}(3n_1 + 2n_2 + 3n_3) = (3, 2, 3)$ ,
- $\psi_{\mathcal{B}}(n_2 + 3n_3) = (0, 1, 3)$ ,
- $\psi_{\mathcal{B}}(3n_2 + n_3) = (0, 3, 1)$ , and
- $\psi_{\mathcal{B}}(3n_1 + n_2 + 4n_3) = (3, 1, 4)$ .

## Lemma

Let  $\phi = \nu \tilde{n} . \sigma$  be a frame and  $\zeta$  be a term in  $\mathcal{T}(\Sigma, \text{dom}(\phi))$ . Let  $\mathcal{B}$  be a base of names in which we can decompose  $\phi$ . We have that

$$\psi_{\mathcal{B}}(\zeta\sigma) = \psi_{\text{dom}(\phi)}(\zeta) \cdot \psi_{\mathcal{B}}(\phi).$$

→ applying a frame to a term is equivalent to **multiplying** the **vector** representing the term with the **matrice** representing the frame

# Outline of the talk

- 1 Monoidal theories / semirings
- 2 Deduction
- 3 Static equivalence
- 4 Applications

## Lemma (characterization of deduction)

Let  $M$  be a ground term and  $\nu\tilde{n}.\sigma$  be a frame. Then  $\nu\tilde{n}.\sigma \vdash_E M$  if and only if there exists  $\zeta \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$  such that  $\text{fn}(\zeta) \cap \tilde{n} = \emptyset$  and  $\zeta\sigma =_E M$ . Such a term  $\zeta$  is a **recipe** of the term  $M$ .

Example:

Consider  $\Sigma = \{+, 0\}$  and the equational theory ACUN (Exclusive Or).

$$\phi = \nu n_1, n_2, n_3. \{n_1+n_2+n_3/x_1, n_1+n_2/x_2, n_2+n_3/x_3\}.$$

We have that  $\phi \vdash_{\text{ACUN}} n_2 + n_4$ .

$$\begin{aligned} & (x_1 + x_2 + x_3 + n_4)\phi \\ = & (n_1 + n_2 + n_3) + (n_1 + n_2) + (n_2 + n_3) + n_4 \\ =_{\text{ACUN}} & n_2 + n_4 \end{aligned}$$

## Lemma (characterization of deduction)

Let  $M$  be a ground term and  $\nu\tilde{n}.\sigma$  be a frame. Then  $\nu\tilde{n}.\sigma \vdash_E M$  if and only if there exists  $\zeta \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$  such that  $\text{fn}(\zeta) \cap \tilde{n} = \emptyset$  and  $\zeta\sigma =_E M$ . Such a term  $\zeta$  is a *recipe* of the term  $M$ .

### Example:

Consider  $\Sigma = \{+, 0\}$  and the equational theory **ACUN** (Exclusive Or).

$$\phi = \nu n_1, n_2, n_3. \{n_1+n_2+n_3/x_1, n_1+n_2/x_2, n_2+n_3/x_3\}.$$

We have that  $\phi \vdash_{\text{ACUN}} n_2 + n_4$ .

$$\begin{aligned} & (x_1 + x_2 + x_3 + n_4)\phi \\ = & (n_1 + n_2 + n_3) + (n_1 + n_2) + (n_2 + n_3) + n_4 \\ =_{\text{ACUN}} & n_2 + n_4 \end{aligned}$$

# Deciding deduction

Let  $E$  be a monoidal theory and  $S_E$  be its associated semiring.

Deduction problem for the equational theory  $E$  built over  $\Sigma$ .

*Entries:* A frame  $\phi$  and a term  $M$  (both built over  $\Sigma$ )

*Question:*  $\phi \vdash_E M$ ?

## Theorem

*Deduction in  $E$  is reducible in **polynomial time** to the following problem:*

*Entries:* A matrix  $A$  over  $S_E$  of size  $\ell \times m$  and a vector  $b$  over  $S_E$  of size  $\ell$

*Question:* Does there exist  $X$  (a vector over  $S_E$  of size  $\ell$ ) such that  $X \cdot A = b$ ?

→ when  $S_E$  is commutative, that is whether  $b^T$  is in the image of  $A^T$  where  $M^T$  is the transpose of  $M$ .

# Reduction on an Example

Consider the theory **ACUNh** and the term  $M = n_1 + h(h(n_1))$ . Let

$$\phi = \nu n_1, n_2. \{ n_1 + h(n_1) + h(h(n_1)) /_{x_1}, n_2 + h(h(n_1)) /_{x_2}, h(n_2) + h(h(n_1)) /_{x_3} \}.$$

We have:

$$A = \begin{pmatrix} 1 + h + h^2 & h^2 & h^2 \\ 0 & 1 & h \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 + h^2 \\ 0 \end{pmatrix}$$

The equation  $X \cdot A = b$  has a solution over  $\mathbb{Z}/2\mathbb{Z}[h] : (1 + h, h, 1)$ . The term  $M$  is deducible from  $\phi$  by using the recipe  $x_1 + h(x_1) + h(x_2) + x_3$ .

Indeed,

$$\begin{aligned} & (x_1 + h(x_1) + h(x_2) + x_3)\phi \\ = & n_1 + h(n_1) + h^2(n_1) + h(n_1 + h(n_1) + h^2(n_1)) \\ & + h(n_2 + h^2(n_1)) + h(n_2) + h^2(n_1) \\ =_{\text{ACUNh}} & n_1 + h^2(n_1) \end{aligned}$$

# Reduction on an Example

Consider the theory **ACUNh** and the term  $M = n_1 + h(h(n_1))$ . Let

$$\phi = \nu n_1, n_2. \{ n_1 + h(n_1) + h(h(n_1)) /_{x_1}, n_2 + h(h(n_1)) /_{x_2}, h(n_2) + h(h(n_1)) /_{x_3} \}.$$

We have:

$$A = \begin{pmatrix} 1 + h + h^2 & h^2 & h^2 \\ 0 & 1 & h \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 + h^2 \\ 0 \end{pmatrix}$$

The equation  $X \cdot A = b$  has a solution over  $\mathbb{Z}/2\mathbb{Z}[h] : (1 + h, h, 1)$ . The term  $M$  is deducible from  $\phi$  by using the recipe  $x_1 + h(x_1) + h(x_2) + x_3$ .

Indeed,

$$\begin{aligned} & (x_1 + h(x_1) + h(x_2) + x_3)\phi \\ = & n_1 + h(n_1) + h^2(n_1) + h(n_1 + h(n_1) + h^2(n_1)) \\ & + h(n_2 + h^2(n_1)) + h(n_2) + h^2(n_1) \\ =_{\text{ACUNh}} & n_1 + h^2(n_1) \end{aligned}$$

# Outline of the talk

- 1 Monoidal theories / semirings
- 2 Deduction
- 3 Static equivalence**
- 4 Applications

# Static equivalence

## Definition (static equivalence)

$\phi_1 \approx \phi_2$  iff  $\text{dom}(\phi_1) = \text{dom}(\phi_2)$  and for every couple of terms  $(M, N)$

$$(M =_{\mathbf{E}} N)\phi_1 \Leftrightarrow (M =_{\mathbf{E}} N)\phi_2$$

Example:

Consider the equational theory ACU and

$$\phi = \nu n_1, n_2, n_3. \{ 3n_1 + 2n_2 + 3n_3 /_{x_1}, n_2 + 3n_3 /_{x_2}, 3n_2 + n_3 /_{x_3}, 3n_1 + n_2 + 4n_3 /_{x_4} \}.$$

Let  $M = 2x_1 + x_2$  and  $N = x_3 + 2x_4$ . We have that  $(M =_{\mathbf{E}} N)\phi$ .

$M\phi$

$N\phi$

$$= (2x_1 + x_2)\phi$$

$$= (x_3 + 2x_4)\phi$$

$$= 2(3n_1 + 2n_2 + 3n_3) + (n_2 + 3n_3)$$

$$= (3n_2 + n_3) + 2(3n_1 + n_2 + 4n_3)$$

$$= 6n_1 + 5n_2 + 9n_3$$

$$= 6n_1 + 5n_2 + 9n_3$$

## Definition (static equivalence)

$\phi_1 \approx \phi_2$  iff  $\text{dom}(\phi_1) = \text{dom}(\phi_2)$  and for every couple of terms  $(M, N)$

$$(M =_{\mathbf{E}} N)\phi_1 \Leftrightarrow (M =_{\mathbf{E}} N)\phi_2$$

### Example:

Consider the equational theory **ACU** and

$$\phi = \nu n_1, n_2, n_3. \{3n_1 + 2n_2 + 3n_3 /_{x_1}, n_2 + 3n_3 /_{x_2}, 3n_2 + n_3 /_{x_3}, 3n_1 + n_2 + 4n_3 /_{x_4}\}.$$

Let  $M = 2x_1 + x_2$  and  $N = x_3 + 2x_4$ . We have that  $(M =_{\mathbf{E}} N)\phi$ .

$M\phi$	$N\phi$
$= (2x_1 + x_2)\phi$	$= (x_3 + 2x_4)\phi$
$= 2(3n_1 + 2n_2 + 3n_3) + (n_2 + 3n_3)$	$= (3n_2 + n_3) + 2(3n_1 + n_2 + 4n_3)$
$= 6n_1 + 5n_2 + 9n_3$	$= 6n_1 + 5n_2 + 9n_3$

# Deciding static equivalence

Let  $E$  be a monoidal theory and  $\mathcal{S}_E$  be its associated semiring.

Static equivalence problem for the theory  $E$  built over  $\Sigma$ .

*Entries:* Two frames  $\phi_1$  and  $\phi_2$  (both built over  $\Sigma$ )

*Question:*  $\phi_1 \approx_E \phi_2$ ?

## Theorem

Static equivalence in  $E$  is reducible in **PTIME** to the following problem:

*Entries:* Two matrices  $A_1$  and  $A_2$  over  $\mathcal{S}_E$  of size  $\ell \times m$

*Question:* Does the following equality holds?

$$\{(X, Y) \in \mathcal{S}_E^\ell \times \mathcal{S}_E^\ell \mid X \cdot A_1 = Y \cdot A_1\} = \{(X, Y) \in \mathcal{S}_E^\ell \times \mathcal{S}_E^\ell \mid X \cdot A_2 = Y \cdot A_2\}$$

→ When  $\mathcal{S}_E$  is a commutative ring (or can be extended in such a way), it is equivalent to deciding whether  $\text{Ker}(A_1) = \text{Ker}(A_2)$ .

# Outline of the talk

- 1 Monoidal theories / semirings
- 2 Deduction
- 3 Static equivalence
- 4 Applications

# Applications

This framework allows us

- to retrieve a lot of results,
- to obtain some new decidability and complexity results.

Theory E	$\mathcal{S}_E$	Deduction	Static Equivalence
ACU	$\mathbb{N}$	NP-complete	decidable, PTIME
ACUI	$\mathbb{B}$	decidable	decidable
ACUN	$\mathbb{Z}/2\mathbb{Z}$	PTIME	decidable, PTIME
AG	$\mathbb{Z}$	PTIME	PTIME
ACUh	$\mathbb{N}[h]$	NP-complete	decidable
ACUIh	$\mathbb{B}[h]$	decidable	?
ACUNh	$\mathbb{Z}/2\mathbb{Z}[h]$	PTIME	decidable
AGh	$\mathbb{Z}[h]$	PTIME	decidable

Is deduction harder than knowledge?

- **ACU**: deduction is NP-complete whereas static equivalence is PTIME
- [Abadi & Cortier'06]  
deduction can be reduced in **PTIME** to static equivalence  
 $\hookrightarrow$  the reduction required the presence of a free function symbol

Combination [Cortier & Delaune'07]

Any of these decidability results can be combined with any existing ones provided the signatures of the equational theories are **disjoints**.

Example: Deduction and static equivalence are decidable for the equational theories  $E_{\text{enc}} \cup \text{ACU}$ ,  $E_{\text{enc}} \cup \text{AG}$ , ...

$$E_{\text{enc}} := \text{dec}(\text{enc}(x, y), y) = x, \text{proj}_1(\langle x, y \rangle) = x \text{ and } \text{proj}_2(\langle x, y \rangle) = y.$$

Is deduction harder than knowledge?

- **ACU**: deduction is NP-complete whereas static equivalence is PTIME
- [Abadi & Cortier'06]  
deduction can be reduced in **PTIME** to static equivalence  
 $\hookrightarrow$  the reduction required the presence of a free function symbol

Combination [Cortier & Delaune'07]

Any of these decidability results can be combined with any existing ones provided the signatures of the equational theories are **disjoints**.

**Example**: Deduction and static equivalence are decidable for the equational theories  $E_{\text{enc}} \cup \text{ACU}$ ,  $E_{\text{enc}} \cup \text{AG}$ , ...

$$E_{\text{enc}} := \text{dec}(\text{enc}(x, y), y) = x, \quad \text{proj}_1(\langle x, y \rangle) = x \quad \text{and} \quad \text{proj}_2(\langle x, y \rangle) = y.$$

## Conclusion

- a **methodology** that can potentially be extended to a number of different theories
- numerous results, several new ones

## Further work

- implementation by using existing tool manipulating matrices (e.g. PARI/GP developed at Bordeaux - France)
- extension to active attacker
  - for deduction  
already done in a rather similar setting [Delaune *et al.*]
  - static equivalence  
useful to decide guessing attacks for new equational theories involving AC operators.

## Conclusion

- a **methodology** that can potentially be extended to a number of different theories
- numerous results, several new ones

## Further work

- **implementation** by using existing tool manipulating matrices (*e.g.* PARI/GP developed at Bordeaux - France)
- extension to **active attacker**
  - **for deduction**  
already done in a rather similar setting [Delaune *et al.*]
  - **static equivalence**  
useful to decide guessing attacks for new equational theories involving **AC** operators.