Formal kernel of ASM
1. Prologue
System specification

“systems specification” is about “algorithms”, affecting real world objects
( which may include implementable components.)

Is there anything mathematically interesting to say about such algorithms?
ASM: Yes!!
the math background: General Algebra

Algebraic Specifications:
“What can you say by help of a signature $\Sigma$, the ground terms $T_\Sigma$ and (quantified) general terms $T_\Sigma(X)$ about the $\Sigma$-structures?”

ASM:
“What can you say by help of a signature $\Sigma$, the ground terms $T_\Sigma$ and (quantified) general terms $T_\Sigma(X)$ about pairs of $\Sigma$-structures ("steps") ?”
Yuri’s theorem

... is 90% a theorem on General Algebra, and 10% on exploiting the 90% in a syntax.

... seems to be just one example in the so far unknown world of algorithms.
1. Prologue

the end
2. Tarski-Structures and Signatures
assumed:

1. notion set

2. For a set $U$, the notion of a function over $U$ of arity $n$ written $f: U^n \to U$.

From this we derive

**Def.:** (Tarski-)structure $S$:
the universe of $S$, frequently written $U_S$, finitely many functions $\varphi_i$ over $U_S$. 
Canonically: signature

**Def.**: (Tarski-)structure \( S \):
the *universe* of \( S \), frequently written \( U_S \),
finitely many functions \( \varphi_i \) over \( U_S \).

**Def.**: Signature \( \Sigma \): Finite set of symbols \( f_i \), each with its arity \( n_i \).

**Def.**: \( S \) is a \( \Sigma \)-structure iff \( \varphi_i \) has the arity \( n_i \) of \( f_i \).

**Observation.** The signature \( \Sigma \) of a structure is unique up to re-naming the symbols in \( \Sigma \).
Canonically: Molecules of $S$

**Def 4:** Let $S$ be a $\Sigma$-structure, let $f \in \Sigma$ with arity $n$, let $u_0, \ldots, u_n \in U_S$, $f_S(u_0, \ldots, u_{n-1}) = u_n$. Then $(f, u_0, \ldots, u_n)$ is a molecule of $S$.

**Lemma 2:** A structure $S$ can be re-gained from its molecules, provided $S$ has at least one function with arity $\geq 1$.

**In the sequel:** A structure $S$ is assumed to be given as a set of molecules.
Canonically: Ground Terms interpretation

for a signature $\Sigma$
the set $T_{\Sigma}$ of *ground terms over* $\Sigma$

For a $\Sigma$–structure $S$ and $t \in T_{\Sigma}$,
the element $t_S \in U_S$
Canonically: Generated molecules

**Def 7:** i. Let $S$ be a $\Sigma$ – structure, let $f \in \Sigma$ and let $t_0, \ldots, t_n \in T_{\Sigma}$.

The tuple $(f, t_0, \ldots, t_n)$

*generates the molecule* $(f, u_0, \ldots, u_n)$ in $S$

iff $t_iS = u_i$ (i = 0, ... ,n).

ii. For $T \subseteq T_{\Sigma}$, a set $M$ of molecules is *$T$-generated*

iff each molecule in $M$ is generated by terms in $T$.

[classically: term generated subalgebra]
Canonically: T - equality on structures

**Def:** Let S be a signature, let R, S be $\Sigma$-structures, let $T \subseteq T_S$.
Then $R =_T S$ iff $t_R = t_S$ for all $t \in T$. 
Canonically: T-Equivalence $\approx$ on structures

**Def 8:** Let $S$ be a signature, let $R$, $S$ be $\Sigma$-structures, let $T \subseteq T_S$.

$R \approx_T S$ iff for all $t, t' \in T$, $t_R = t'_R$ iff $t_S = t'_S$.

**Lemma 3.** Let $\Sigma$ be a signature, let $T \subseteq T_\Sigma$.

If $T$ is finite, $\approx_T$ has finitely many equivalence classes.

**Lemma 4.** Let $\Sigma$ be a signature, let $R =_T S$.

Then $R \approx_T S$. 
2. Tarski-Structures and Signatures

the end
3. Isomorphism
A new notion: Isomorphism

**Def 9:** Let $R, S$ be $\Sigma$ – structures

Let $h: U_R \rightarrow U_S$ be a bijection such that for all $f \in \Sigma$, $f$ n-ary,

and all $u_1, \ldots, u_n \in U_R$:

$h( f_R(u_1, \ldots, u_n)) = f_S(( h(u_1), \ldots, h(u_n)))$,

Then $h$ is an *isomorphism from $R$ to $S$*, written $h: R \rightarrow S$.

**Lemma 5:** Let $R, S$ be $\Sigma$ – structures,

let $t \in T_\Sigma$,

let $h: R \rightarrow S$ be an isomorphism,

Then $h(t_R) = t_S$.
Implications

**Lemma 6:** Let $R$ and $S$ be isomorphic.
Then for each $T \subseteq T_\Sigma$:
$R \approx_T S$

**Lemma 7:** Let $h: R \rightarrow S$ be an isomorphism.
Then $(f, u_0, \ldots, u_n)$ is a molecule of $R$ iff
$(f, h(u_0), \ldots, h(u_n))$ is a molecule of $S$.

**Lemma 8:** Replacing some $u \in U_S$ by some new element $v \notin U_S$
yields a structure $R$, isomorphic to $S$,
with $U_R = U_S \setminus \{u\} \cup \{v\}$.
Lemma 9. Let $R, S$ be $\Sigma$-structures, let $T \subseteq T_\Sigma$, let $R \approx_T S$. Then there exists some $Q$ isomorphic to $R$ with $Q =_T S$.

short hand: If $R \approx_T S$ then $R \rightarrow Q =_T S$.

Proof.
The RQS construction, graphically

**Lemma 9.** Let $R, S$ be $\Sigma$-structures, let $T \subseteq T_\Sigma$, let $R \approx_T S$.

For each $t \in T$
then holds

$$Q^{t_Q} = t_{\approx S}$$
The RQS construction, graphically

**Lemma 9.** Let $R, S$ be $\Sigma$-structures, let $T \subseteq T_\Sigma$, let $R \cong_T S$.

**Proof.**

For each $u \in U_R \cap U_S$ replace:

$$R \xrightarrow{u \text{ by } v \notin U_R \cup U_S} P$$

iso \quad (triv.)

For each $t \in T$ replace:

$$P \xrightarrow{t_P \text{ by } t_S} Q$$

iso

then holds:

$$t_Q = t_{SS}$$

iso by $P \cong_T S$
3. Isomorphism

the end
4. Steps
**A new notion: steps**

**Def 10:** A *step* is a pair \((S,S')\) of structures \(S\) and \(S'\), where
\[
S \text{ and } S' \text{ have the same signature and the same universe.}
\]

**Def 11:** For a step \((S, S')\), let \(\Delta(S,S') =_{\text{def}} S\setminus S\).

**Def 12:** A set \(\Xi\) of steps is *isomorphism closed* iff for each \((R,R') \in \Xi\)
and each isomorphism \(h: R \to S\) holds:
\[(S,S') \in \Xi, \text{ with } S' = h(R').\]
Lemma 10. Let \((R, R')\) and \((S, S')\) be steps, let \(h: R \rightarrow S\) and \(h: R' \rightarrow S'\) be an isomorphism, let \(T \subseteq T_\Sigma\). Then \(T\) generates \(\Delta(R, R')\) iff \(T\) generates \(\Delta(S, S')\).

Proof.
\((f, u_0, \ldots, u_n)\) is generated by \((f, t_0, \ldots, t_n)\) in \(R\) (in \(R'\), resp.) iff
\((f, h(u_0), \ldots, h(u_n))\) is generated by \((f, t_0, \ldots, t_n)\) in \(S\) (in \(S'\), resp)
(by Lemma 7).
Then \((f, u_0, \ldots, u_n) \in R\setminus R = \Delta(R, R')\) iff
\((f, h(u_0), \ldots, h(u_n)) \in S\setminus S = \Delta(S, S')\).
Hence, \(\{t_0, \ldots, t_n\}\) generates \(\Delta(R, R')\) iff
4. Steps
5. Witnesses [Discriminators]
A new notion: Witness of a set of steps

idea of witness $T$:
If $\Delta(R, R') \neq \Delta(S, S')$ then $t_R \neq t_S$ for some $t \in T$.

Def 14: Let $\Xi$ be a set of steps.
A set $T \subseteq T_\Sigma$ of terms is a witness for $\Xi$ iff for each two steps $(R, R')$ and $(S, S') \in \Xi$ $R \implies_T S$ implies $\Delta(R, R') = \Delta(S, S')$.

Lemma 11. If $T$ is a witness for $\Xi$ and $T' \supseteq T$, then $T'$ is a witness for $\Xi$, too.
Lemma 13. Let $\Xi$ be an isomorphism closed set of steps
let $T$ be a witness for $\Xi$,
let $(R,R'), (S,S') \in \Xi$, $R \approx_T S$.
Let $T$ generate $\Delta(R,R')$.
Then $T$ generates $\Delta(S,S')$

Proof. There exists a structure $Q$ isomorphic to $R$ with $Q =_T R$ (Lemma 9).
Then $T$ generates $\Delta(Q,Q')$ (Lemma 10)
Then $T$ generates $\Delta(S,S')$ (Lemma 12)
Structures without witness

**Lemma 14.** Let \((S, S')\) be a step
where \(\Delta(S,S')\) is not \(T_\Sigma\)-generated.
Then there exists a step \((R, R')\) isomorphic to \((S, S')\)
such that \(S\) and \(R\) have no witness.

**Proof.** The Lemma’s assumption implies a molecule
\((f, u_0, \ldots, u_n) \in \Delta(S,S')\) and some index \(0 \leq k \leq n\)
with \(u_k \neq t_S\) for all \(t \in T_\Sigma\).
Let \(v\) be any element, \(v \notin U_S\).
In \(S\), replace each occurrence of \(u_k\) by \(v\).
This yields a structure \(R\), isomorphic to \(S\) (by Lemma 8).
As \(u_k \neq t_S\) for all \(t \in T_\Sigma\), it holds \(t_R = t_S\) for all \(t \in T_\Sigma\).
Hence, \(R\) and \(S\) have no witness (by Def. 13).
Term generation of $\Delta(S, S')$

**Lemma 15.** Let $\Xi$ be a set of isomorphism closed steps, let $T$ be a witness of $\Xi$. Then for each step $(S, S') \in \Xi$, $\Delta(S, S')$ is $T$-generated.

**Proof.** By contradiction, assume $\Delta(S, S')$ is not $T$-generated. Construct $R$ according to the proof of Lemma 13. Then $(R, R') \in \Xi$ and $\Delta(R, R') \neq \Delta(S, S')$, and $S$ and $R$ have no witness by construction. Hence, $\Xi$ has no witness (by Def. 14).
5. Witnesses
6. Construction of an ASM
the ingredients: Given

- a signature $\Sigma$, 

- a set $\Xi$ of steps $(S,S')$ with $\Sigma$-structures $S$, $S'$, deterministic (i.e. for each $\Sigma$-structure $S$ exactly one $(S, S')$) and isomorphism closed, (i.e. for each $(R,R') \in \Xi$ and each $h: R \to S$, $(S, h(R')) \in \Xi$). 

- a finite witness $T \subseteq T_{\Sigma}$ for $\Xi$. 


What to cook: Construct

1. for each \( \approx_T \) -equivalence class \( A \)

   - a set \( M \) of \( \langle f, t_0, \ldots, t_n \rangle \), generating \( \Delta(R, R') \),
     for some \( (R, R') \in \Xi \) with \( R \in A \)

   - the set \( \text{ass}(A) = \text{def} \{ f(t_0, \ldots, t_{n-1}) := t_n \mid (f, t_0, \ldots, t_n) \in M \} \)

   - the set \( \text{eq}(A) = \text{def} \{ t = t' \mid t, t' \in T \text{ and } t_S = t'_S \text{ for some } S \in A \} \)
     \( \cup \{ t \neq t' \mid t, t' \in T \text{ and } t_S \neq t'_S \text{ for some } S \in A \} \)

   - the ASM- rule \( \text{rule}(A) = \text{def} \{ \text{eq}(A) \rightarrow \text{ass}(A) \} \)
The equivalence $\approx_T$ graphically

all $\Sigma$ - structures the $\approx_T$ equivalence classes
all steps
from $A$
go to $A'$
a step from $A$ to $A'$
a step is a set of updates
an update yields an ass. statement

$A$
$A'$

$S$
$h(S)$
$h(S')$

$S'$

$A$ to $A'$

all isomorphic updates are described by one assignment statement.

isom. str. are 

an update yields ass. statem. describes all steps from $A$ to $A'$

$a$ finite set of ass. statem.
The equivalence $\approx_T$ graphically

all $\Sigma$ - structures the $\approx_T$ equivalence classes

all steps from $A$ go to $A'$

Construct all equations that hold and all equations that don't hold in $A$

$\land$ - them as a guard for the ass. statement

$A$

$S$

$A'$

$h(S)$

$h(S')$

$\approx_T$ equivalence class

A step is a set of updates

an update yields an ass. statement

a finite set of updates, statem.

an update

updates all steps from $A$ to $A'$

Do that for each $\approx_T$ equivalence class

and combine

isom. str. are equivalent.
6. Construction of an ASM

the end