Soundness of the Analysis

We establish a Galois insertion between the domain of signals and the abstraction to logs considered in the paper. More precisely, we show that any encoding of signals results in an over-approximation, in particular any M-out-of-N encoding. For details on the logging procedure and the terminology, we refer to the submission.

Let m be the length of the trace cycle. A *signal* is a map $S : [1..m] \to \{0, 1\}$, where a change in the i-th clock cycle is indicated by $S(i) = 1$. Let Sig denote the set of all signals. The domain we abstract from is the powerset lattice over signals, $\mathcal{P}(Sig)$.

The abstraction is defined relative to an *encoding* of signals. An encoding is an injective map $TS : [1..m] \to \mathbb{F}_2^b$, which assigns each clock cycle a unique timestamp.

Our logging procedure uses the encoding to abstract signals to pairs consisting of a timeprint $TP \in \mathbb{F}_2^b$ and a number of changes k with $k \leq m$. We call such a pair a *log*. We collect all logs in the set $Log = \mathbb{F}_2^b \times [1..m]$. Then, the abstract domain is the powerset lattice over all logs, $\mathcal{P}(Log)$.

We now construct a Galois insertion between $\mathcal{P}(Sig)$ and $\mathcal{P}(Log)$. For the abstraction function, note that our logging procedure implements the function $\tilde{\alpha}_{TS} : Sig \to Log$ defined as follows. Given a signal S, it returns $\tilde{\alpha}_{TS}(S) = (TP, k)$ with

$$TP = \sum_{i\,:\,S(i)=1} TS(i) \qquad \text{and} \qquad k = |\{i \mid S(i) = 1\}|.$$

This is a log. The timeprint TP is the sum over the timestamps where the signal changes. These changes sum-up to k. The abstraction function $\alpha_{TS} : \mathcal{P}(Sig) \to \mathcal{P}(Log)$ in the Galois insertion is the lifting of $\tilde{\alpha}_{TS}$ to sets of signals $F \in \mathcal{P}(Sig)$. The lifting is defined by taking the union over the signals in the set, $\alpha_{TS}(F) = \bigcup_{S \in F} \{\tilde{\alpha}_{TS}(S)\}$.

For the concretization function $\gamma_{TS} : \mathcal{P}(Log) \to \mathcal{P}(Sig)$ of the Galois insertion, we define the auxiliary function $\tilde{\gamma}_{TS} : Log \to \mathcal{P}(Sig)$ by

$$\tilde{\gamma}_{TS}(TP, k) = \{S \in Sig \mid \sum_{i\,:\,S(i)=1} TS(i) = TP \text{ and } |\{i \mid S(i) = 1\}| = k\}.$$

Note that $\tilde{\gamma}_{TS}(TP, k) = \tilde{\alpha}_{TS}^{-1}(TP, k)$. Then γ_{TS} is the lifting of $\tilde{\gamma}_{TS}$ to sets of logs, again defined by taking a union. Both α_{TS} and γ_{TS} are monotonic by definition.

Lemma 1 (Galois insertion)**.** *Let TS be an encoding. We have* $id_{\mathcal{P}(Sig)} \leq \gamma_{TS} \circ \alpha_{TS}$*, which means* $F \subseteq \gamma_{TS}(\alpha_{TS}(F))$ *for all* $F \in \mathcal{P}(Sig)$*. Moreover,* $id_{\mathcal{P}(Log)} = \alpha_{TS} \circ \gamma_{TS}$*.*

The proof relies on the fact that $\tilde{\gamma}_{TS}$ yields the preimage of $\tilde{\alpha}_{TS}$.

The trace reconstruction problem is also interesting from a complexity-theoretic point of view. We refer the interested reader to [1].

References

[1] P. Chini, R. Massoud, R. Meyer, and P. Saivasan. Fast witness counting. *CoRR*, http://arxiv.org/abs/1807.05777, 2018.