Formal Methods above the Code

specifying a non-computer

Martin Ames Harrison

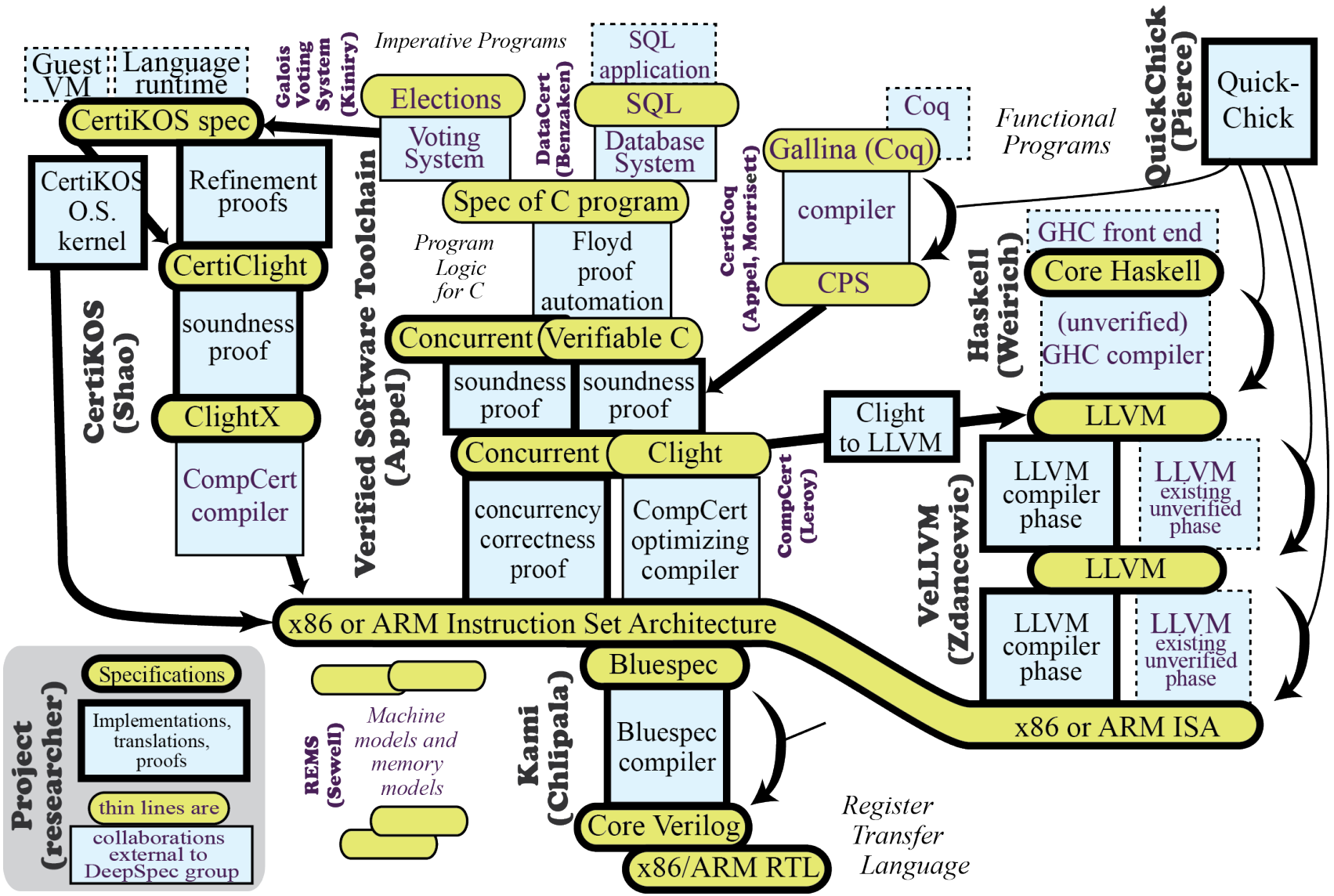
RTX BBN Interview
February 15, 2024

Some Background

About DeepSpec

- NSF *Expedition in Computing* focused on "the specification and verification of full functional correctness of software and hardware"
- vision: build systems with end-to-end formal verification of specs
- tools include Coq/Gallina among many others (next slide)

DeepSpec in a Picture

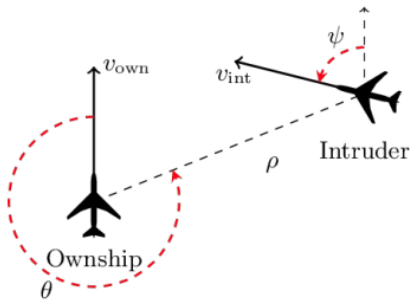


Verified Missile Toolchain?

- Can we mimic this in MDA's software IV&V operation?
- IV&V = Independent Verification & Validation
  - contractor delivers code to customer
  - independent entity evaluates code, reports findings
  - repeat till final delivery
- **idea**: let's use Coq to develop in parallel, producing corrected and verified versions of contractors' code drops
- **plan**: hire a dozen STEM types and put them to work studying *Software Foundations* in IV&V lab
- **result**: skepticism, chairs thrown and a **new task**!

A Different Approach

- begin formal methods practice at the outset of a project, at the *system design level*
- NASA used PVS for collision-avoidance algorithms
- Lamport's TLA+ used in RTOS design
- TLA+ used also by Elasticsearch in developing their data replication algorithm



Katz

elasticsearch

On TLA+ and Model Checking

- describes system as a finite state machine
- allowed transitions (**actions**) are specified together with initial state
- has **constants**, knobs to adjust model scale
- the TLC model checker searches breadth-first the reachable states of the system, checking **state** predicates and **behavior** properties
- feature of interest: TLA+ supports **refinement** or **implementation**; checking or proving that one spec is a higher resolution picture of another

On Refinement

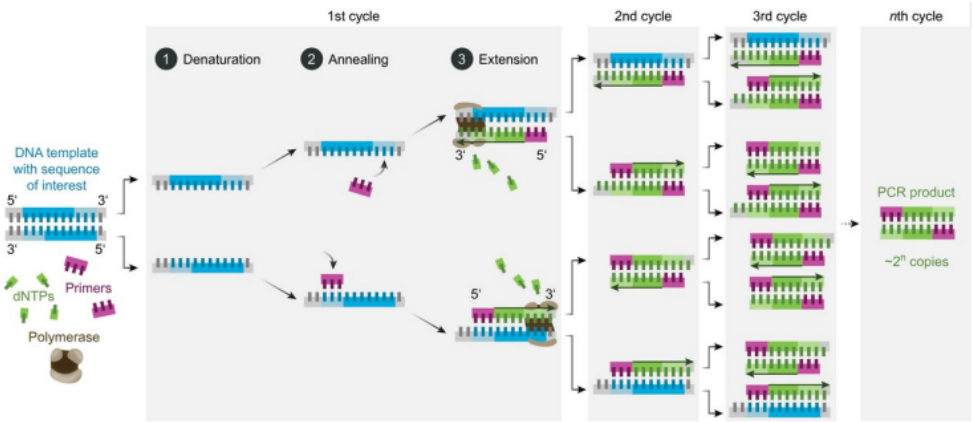
What is refinement,exactly? We need some terms:

- an **action** is a predicate on (state, next state) pairs
- a **behavior** is a sequence of states
- a spec is a set of valid behaviors
- spec B **refines** spec A if there is a map from B's state into A's state such that all valid behaviors of B map to valid behaviors of A

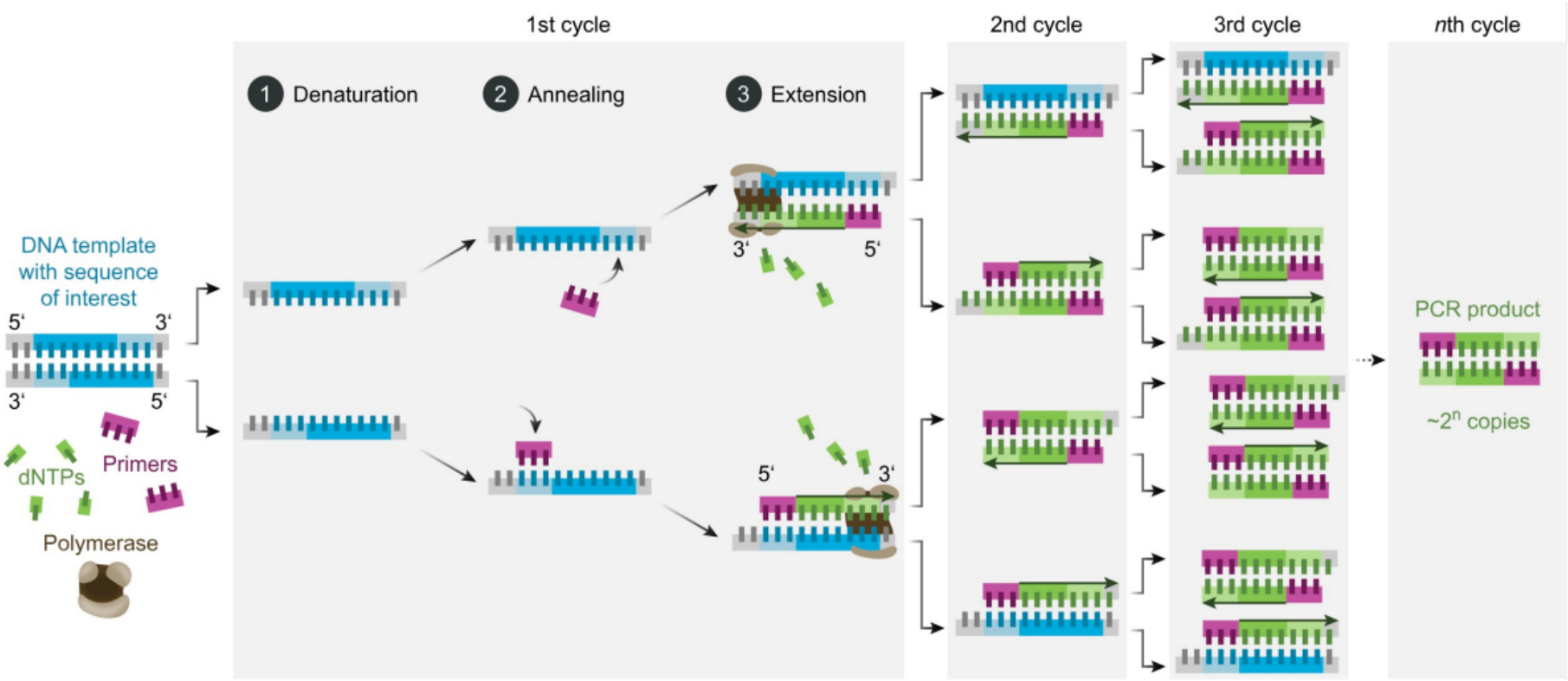
Let's look at an example!

Polymerase Chain Reaction

- invented by Kary Mullis in 1983; won Nobel
- amplifies desired snippet of DNA (called *amplion*)
- requires *thermal cycling*, *primers* and a special type of *polymerase*



Closer Look at PCR



PCR Specification

What is the plan, exactly?

- describe the process in broad, low-resolution terms
- check basic properties, discuss **safety** and **liveness**
- refine spec by introducing two new variables
- refine spec further with **refinement mapping**
- check one last property *not expressible* in the first two specs (which are implemented by final spec)

Let's look at the code!

But Why?

- specs can be refined and checked at each new level of detail
- refine it enough and you wind up with pseudocode (PlusCal)
- the process of specification improves our understanding of the system
- preempt flaws before coding starts