Pragmatic Formal Verification of Sequential Error Detection and Correction Codes (ECCs) used in Safety-Critical Design

Aman Kumar

Infineon Technologies, Dresden, Germany

accellera SYSTEMS INITIATIVE

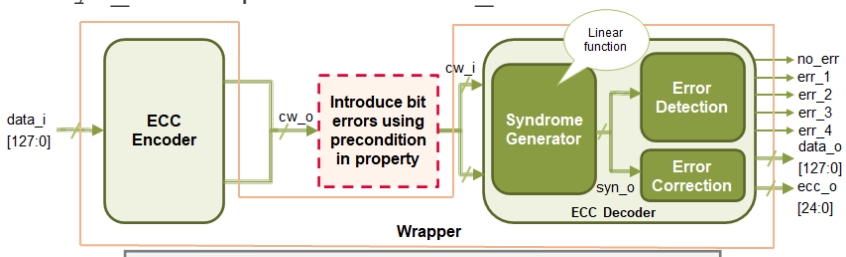
2023 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES
SAN JOSE, CA, USA
FEBRUARY 27-MARCH 2, 2023

INTRODUCTION

- Error Detection and Correction Codes (ECC) are often used in digital designs to protect data integrity
- Soft errors in memories can occur due to radiation errors, electrical glitches or magnetic interferences
- An ECC of 128 data bits with a possibility to detect up to four-bit errors, the combination of bit errors is given by 128C1 + 128C2 + 128C3 + 128C4 ≈ 1.1 * 10^7
- To overcome such problems and sign-off the design with confidence within reasonable proof time, we present a pragmatic formal verification approach of complex ECC cores with several complexity reduction techniques and know-how that were learnt during the course of verification

LINEARITY APPROACH

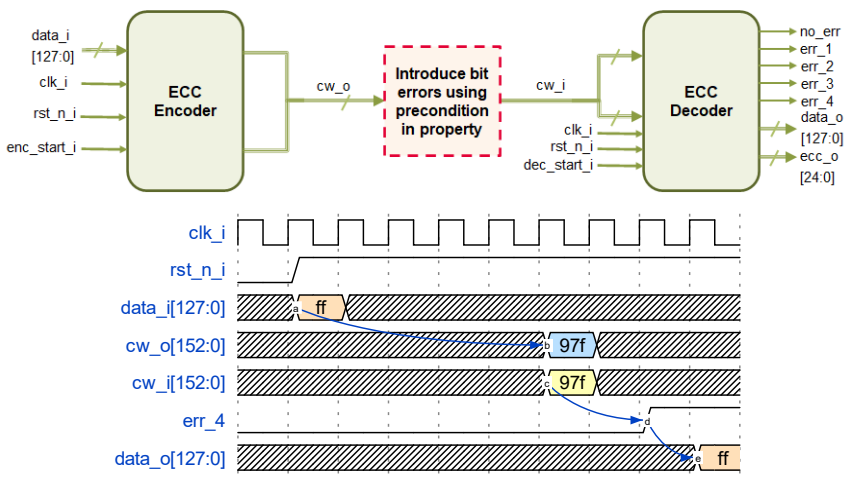
- Syndrome generator is a linear function
- `syn_o` is independent od `data_i`




```
property MBERR_detection;
    data_i == 128'hcaba79a638aca501 //random
    && $countones(cw_o ^ cw_i) == 4
  |->
    err_4 && !err_1 && !err_2 && !err_3 &&
    !no_err;
endproperty
```

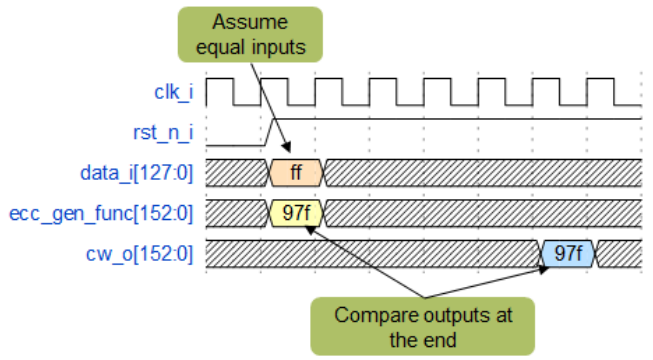
SEQUENTIAL ECC VERSION

- Sequentially pipelined encoding and decoding stages



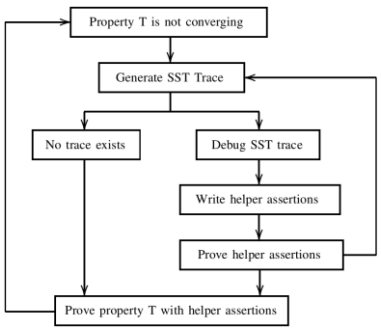
REDUCED LATENCY MODEL

- Encoder has longer latency
- A cycle inaccurate model of the Encoder was prepared that calculates ECC in same clock cycle



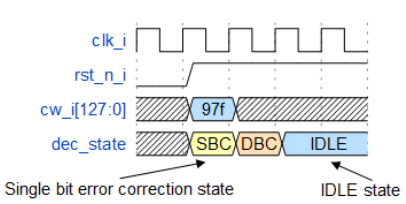
INDUCTION-BASED PROOF

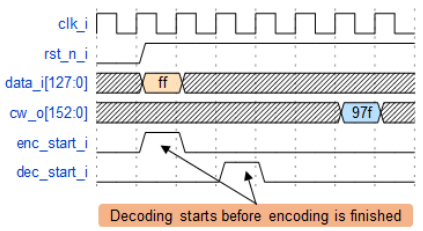
- Induction is a method to check if the design is in a random good state whether it will be in a good state at the next cycle
- SST trace from JasperGold gives hints for helper assertion to converge the target property faster



INDUCTION-BASED PROOF

- SST trace shows two missing constraints





- Adding these two missing constraints helped to prove the properties within 24 hours