Better Circuits For Boolean Functions

René Peralta
National Institute of Standards and Technology

Cybersecurity Innovation Forum

September 2015

Circuits

- Binary operands $\{0, 1\}$.
- Binary operations , e.g.

$$1 + 1 = 0$$

- ’+’ gates in **yellow**

  ’X’ gates in **red**

Circuits

$$\mathbf{Majority(a, b, c) = ab + ac + bc}$$

Circuits

$$\mathbf{Majority(a, b, c) = ab + ac + bc}$$

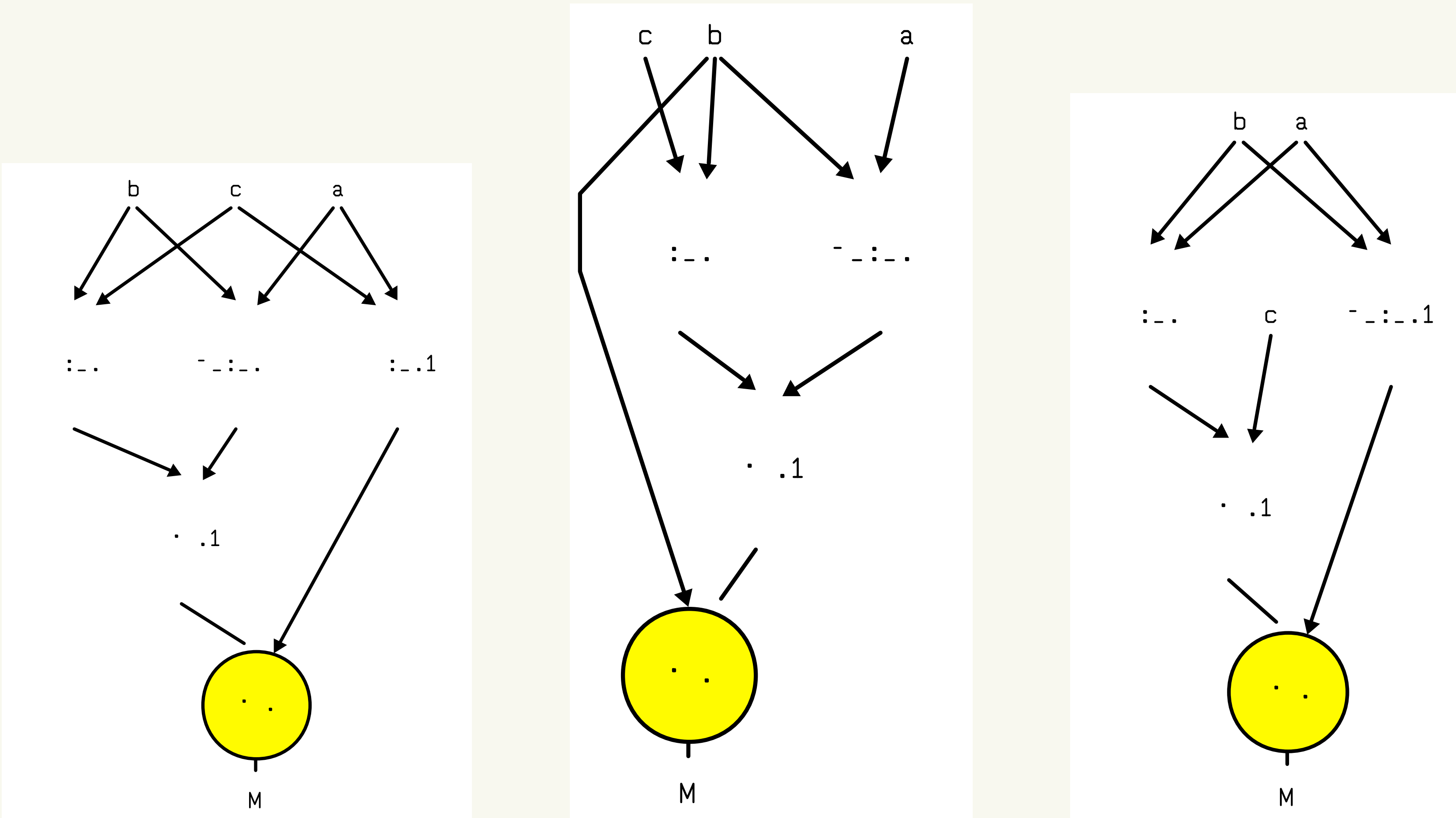

Figure 1: Equivalent circuits over **GF(2)**.

Metrics

- Number of gates;
- Depth;
- Number of multiplication gates (ANDS).

Optimality is out of reach

- Finding optimal circuits is NP-Hard or worse.

Optimality is out of reach

- Finding optimal circuits is NP-Hard or worse.
- We are interested in practical applications.

Optimality is out of reach

- Finding optimal circuits is NP-Hard or worse.
- We are interested in practical applications.
- Hence we are looking into the *concrete complexity* of circuit optimization problems.

This is basic metrology

- Platonic view: these objects are not "created" but discovered.

This is basic metrology

- Platonic view: these objects are not “created” but discovered.
  Find , measure ...

This is basic metrology

- Platonic view: these objects are not "created" but discovered.
  Find , measure ...

- Modern tool is the computer.

This is basic metrology

- Platonic view: these objects are not "created" but discovered.
  Find , measure ...

- Modern tool is the computer.

- Not using our great computational power for this is like not using microscopes to determine the structure of living cells.

example: binary multiplication

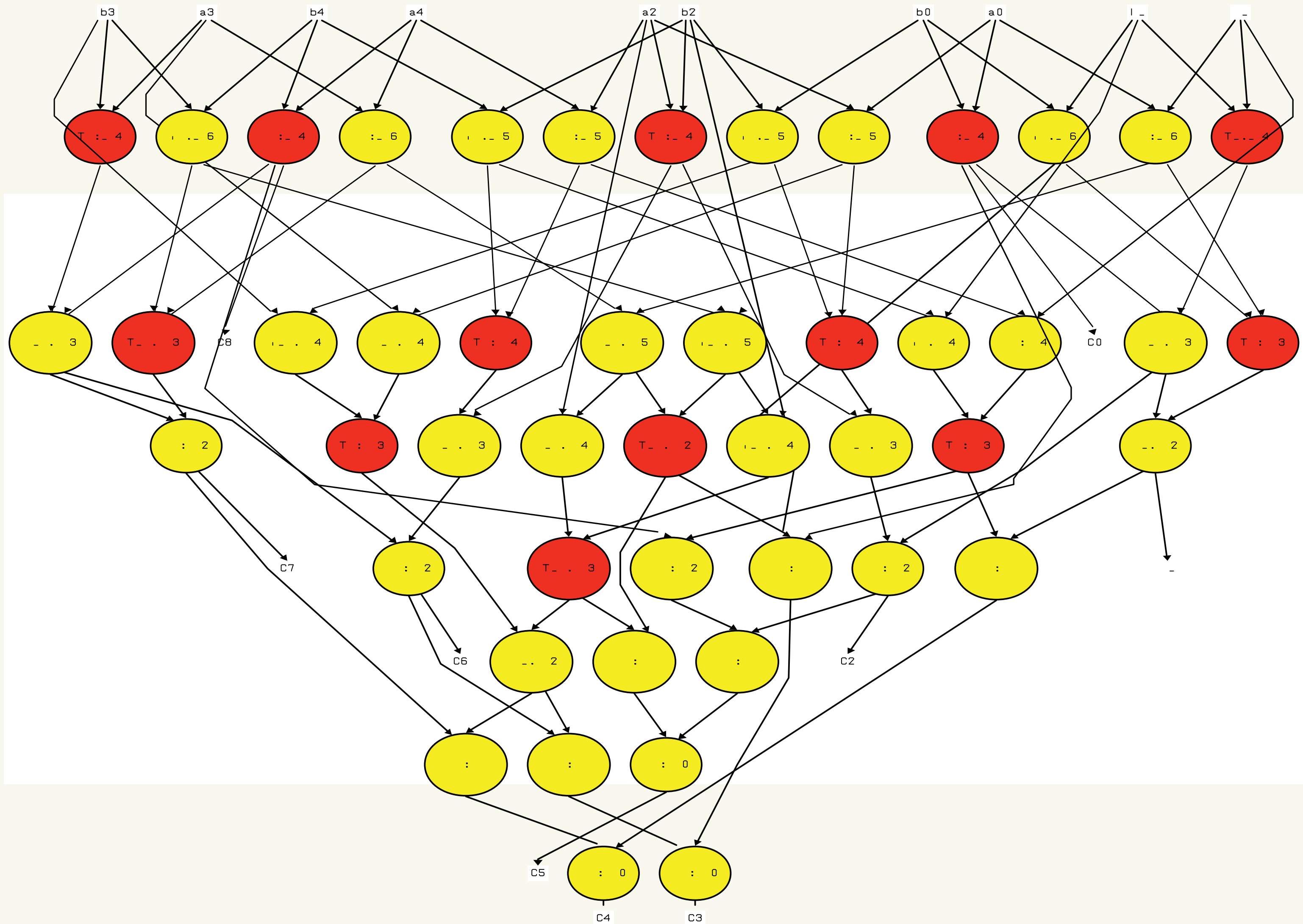

Figure 2: 5 x 5 multiplication with optimal number of AND gates

Applications

- Homomorphic Encryption
- Cryptanalysis
- Multiparty Computation
- Lightweight Crypto
- Privacy Preserving Proofs

Applications

Homomorphic Encryption

Cryptanalysis

Multiparty Computation

Lightweight Crypto

Privacy Preserving Proofs

THANKS