CoRNG

Martin Vassor

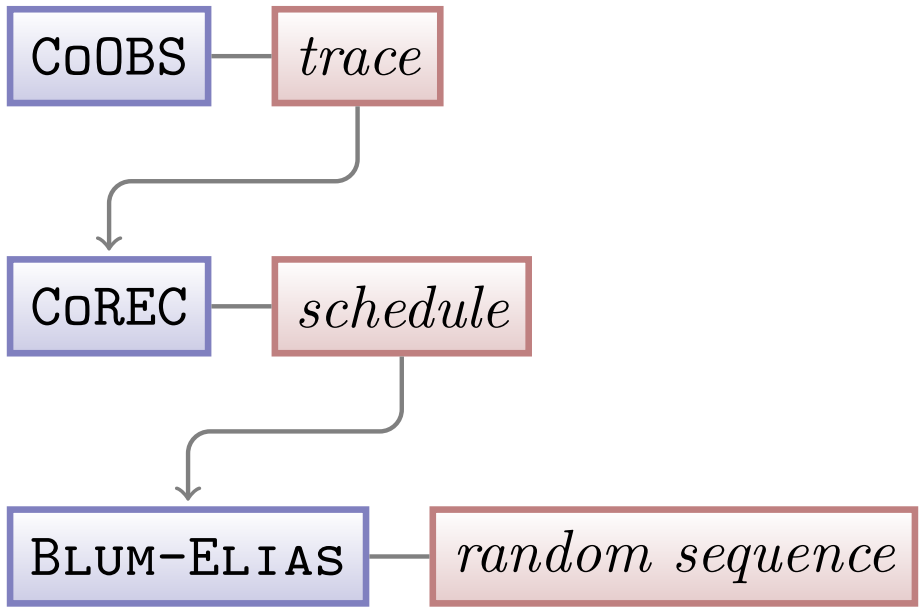
EPFL

November 10, 2016

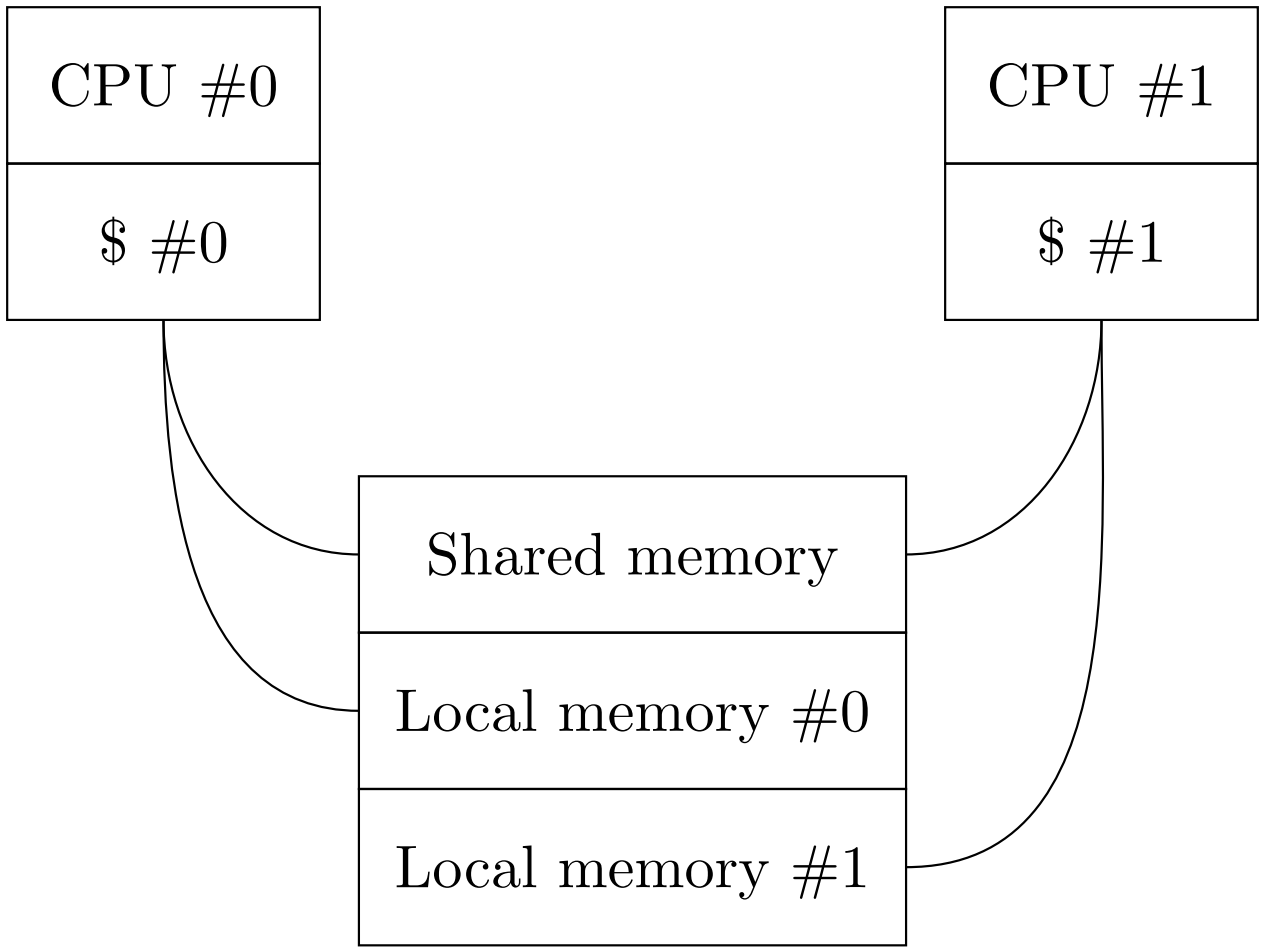
Introduction

- K. Antoniadis, P. Blanchard, R. Guerraoui and J. Stainer (lpd – epfl), 2016
- Benefits from lack of locality ?

CoRNG overview



CoOBS

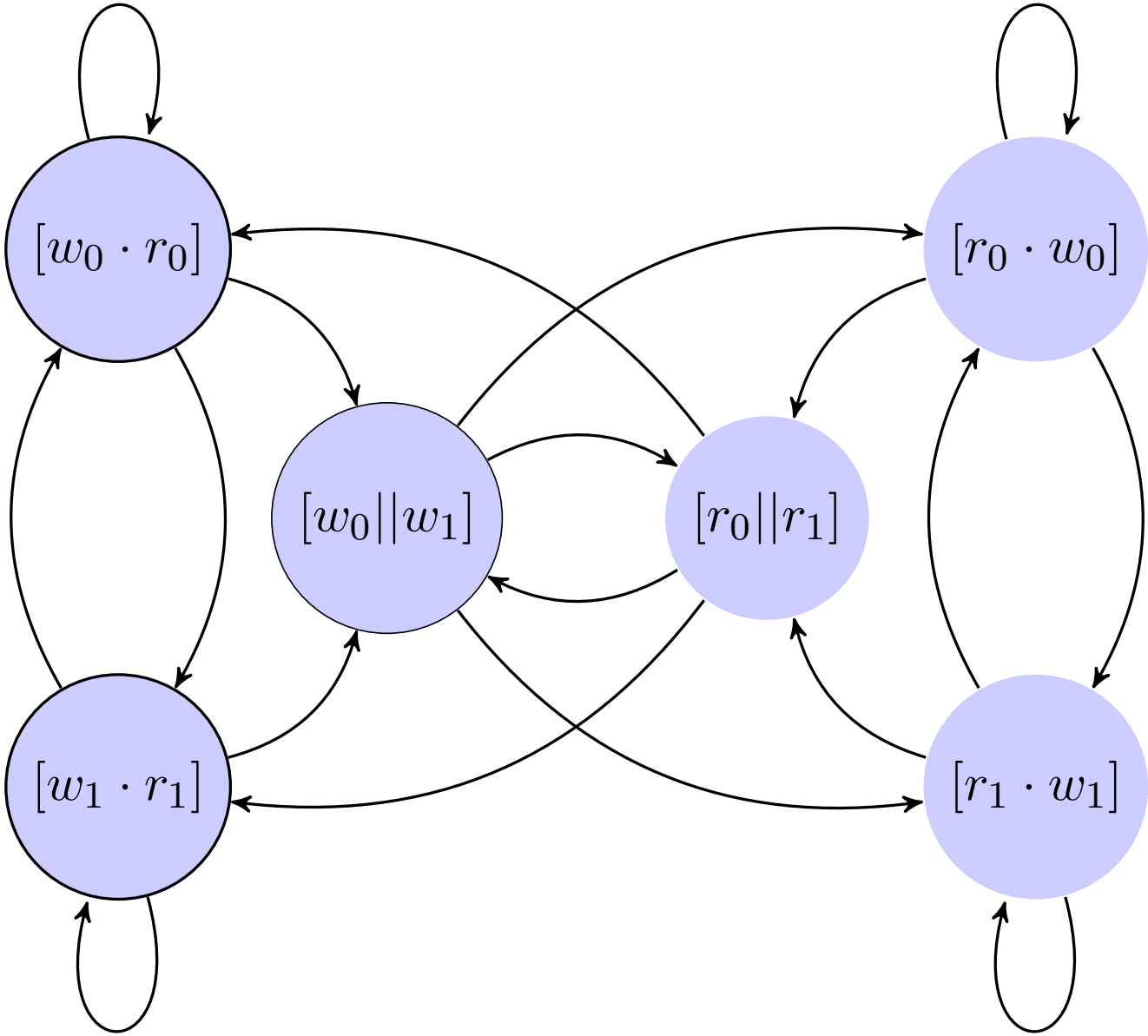


CoREC and Blum-Elias

CoREC: Rebuild schedule from local memories.

Blum-Elias: Generate unbiased random from schedule.

From schedule to unbiased randomness



Conclusion

- Requires data races.
- Uses order of atomic accesses.
- Better if more interleaving.
- Orders of magnitude faster[1].

[1] than current `/dev/random` for same quality

References

- Submitted to *Distributed Computing* journal


Manuel Blum.
Independent unbiased coin flips from a correlated biased source—A finite state markov chain.
Combinatorica, 6(2):97–108, 1986.


John Von Neumann.
13. Various Techniques Used in Connection With Random Digits.
Monte Carlo Method:36:38, 1951.