Exponential Separation Between AMP and MAP

Tom Gur, Yang P. Liu, Ron Rothblum

Merlin

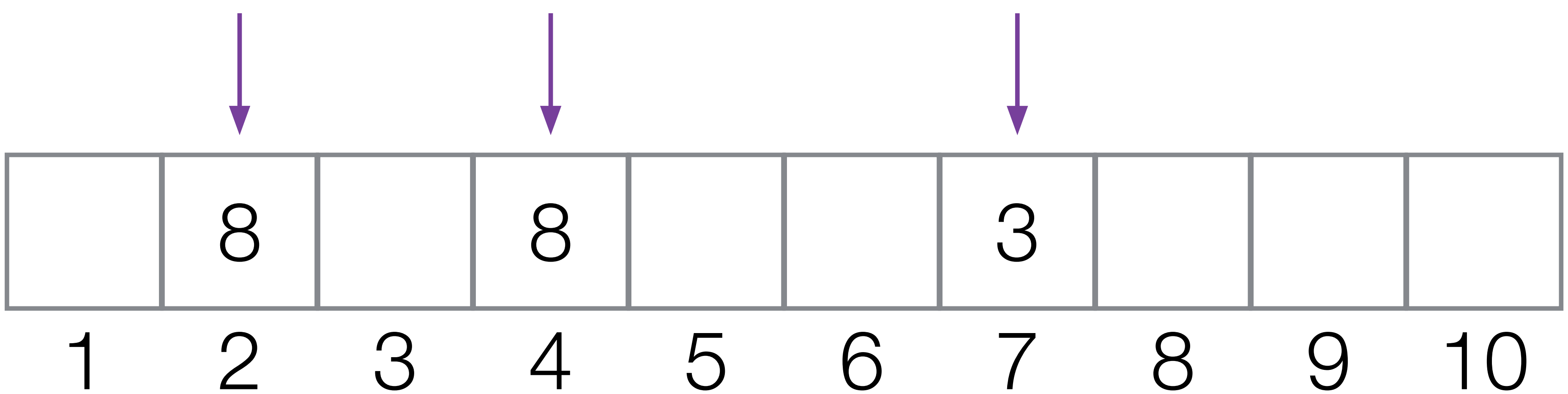
Arthur

Introduction: Property Testing

- A *property* Π_n is a subset of functions f: D_n -> $R_{n.}$
- Let F_n denote the family of *all* functions f: D_n -> R_n.
- Input is either in Π_n or ε-far from Π_n.
- Make q queries to f, then decide whether f in Π_n.

Property Testing: **Permutation** Property

f: {1, 2, …, 10} -> {1, 2, …, 10}



Not a permutation!

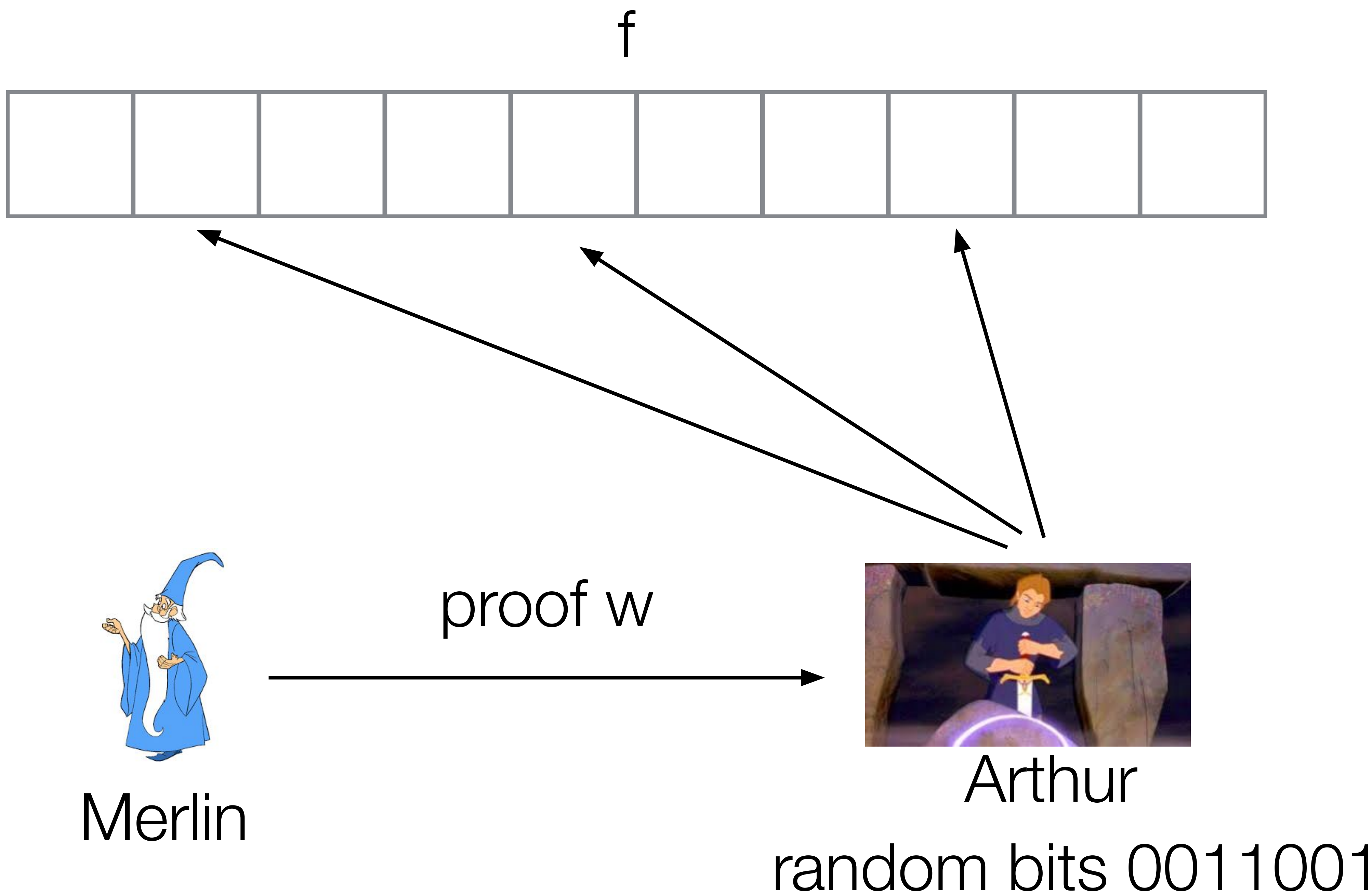
Property Testing: **Permutation** Property

- For fixed ε, testing for the **Permutation** property takes time $\Theta(n^{1/2})$.

Introduction: MAP and AMP

- MAP = Merlin-Arthur proof of proximity
- AMP = Arthur-Merlin proof of proximity
- MAP and AMP both denote property testing with a *proof system*.
- MAPs are the analog of MA.
- AMPs are the analog of AM.

Definition: MAP



Definitions: MAP

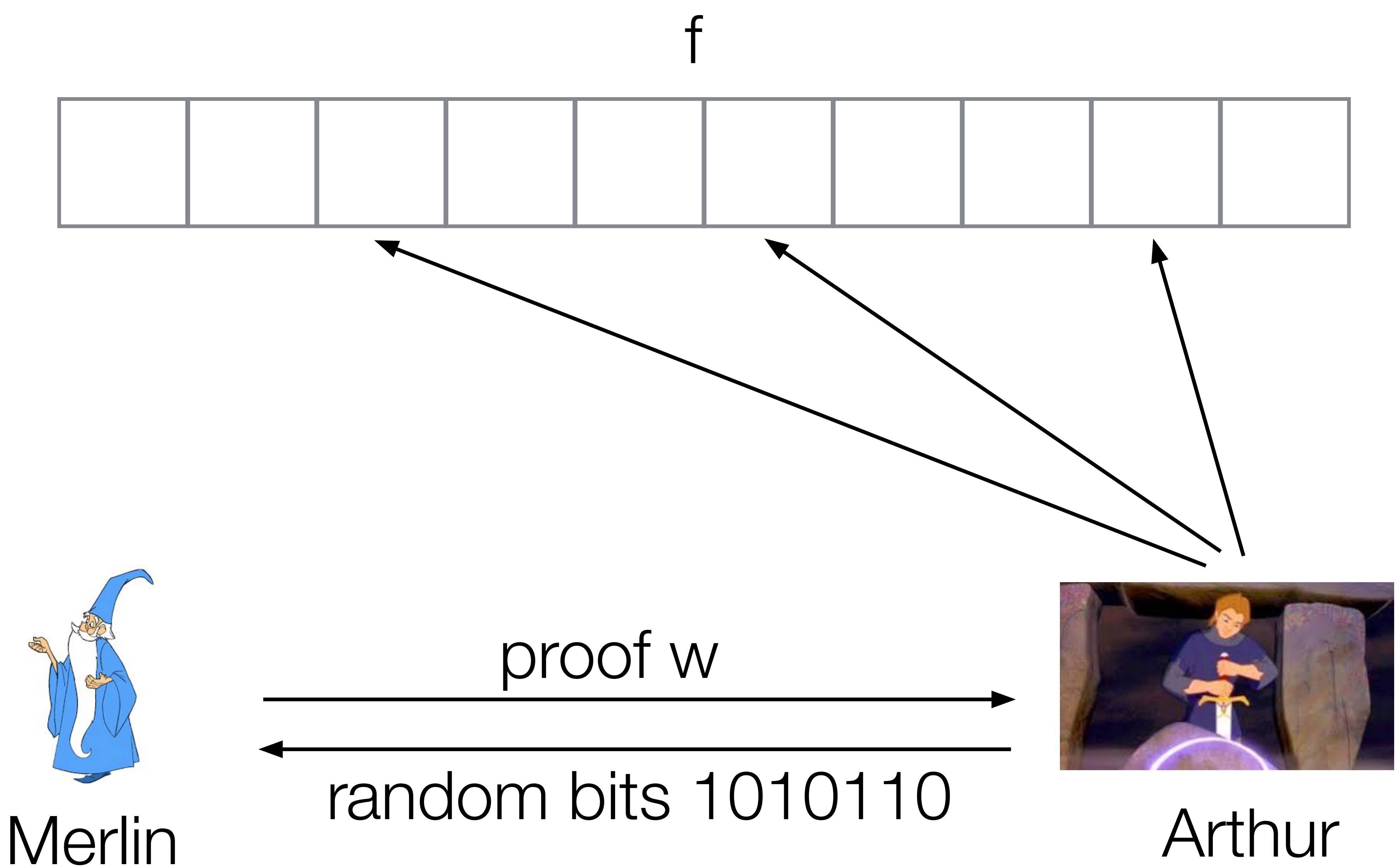
- Completeness: for any f in Π_n we have

$$\exists w \text{ such that } \Pr\left[V(f,w)=1\right] \geq \frac{2}{3}$$

- Soundness: for any f that is ε-far from Π_n

$$\forall w \text{ we have that } \Pr\left[V(f,w)=1\right] \leq \frac{1}{3}$$

Definition: AMP



Definitions: AMP

- Completeness: for any f in Π_n we have

$$\Pr_r\left[\exists w \text{ such that } V(f,w,r)=1\right] \geq \frac{2}{3}$$

- Soundness: for any f that is ε-far from Π_n

$$\Pr_r\left[\exists w \text{ such that } V(f,w,r)=1\right] \leq \frac{1}{3}$$

Definition: MAP and AMP

- In both models, we define the *complexity* of the MAP/AMP to be the sum of the:
  - proof length in the worst case
  - number of queries needed in the worst case.

Background

- **maybe put something here?**

Exponential Separation

- There is an AMP for the **Permutation** property that takes complexity $O(\log n)$.
- Every MAP for the **Permutation** property requires time $\Omega(n^{1/4})$.
- Corollary: there is an exponential separation between the classes MAP and AMP.

Proof: AMP Protocol

- Lemma: $|\mathrm{Im}(f)| \leq n(1-\varepsilon)$ if f is ε-far from a permutation
- Fix $k = O(1/\varepsilon)$.
- Arthur randomly generates $x_1, x_2, \ldots, x_k$ in $[n]$.
- Ask Merlin for $s_1, s_2, \ldots, s_k$ such that $f(s_i) = x_i$
- Query f to check $f(s_i) = x_i$

MAP Lower Bound

- Goal: Every MAP for the **Permutation** property requires time $\Omega(n^{1/4})$.
- Question: What properties of **Permutation** allow us to show MAP lower bounds on it?

Independence

- Property Π_n of functions f: D_n -> R_n.
- Π_n is *k-wise independent* if for all distinct indices i_1, i_2, …, i_k in D_n:
- the k-tuple $(f(i_1), f(i_2), \ldots, f(i_k))$ is uniform over $(R_n)^k$ over functions f in Π_n.

Independence

- Theorem: a k-wise independent property requires complexity k for property testing.

- [FGL14]: a k-wise independent property requires MAPs of complexity $k^{1/2}$.

Relaxed Independence

- Π_n is *relaxed k-wise independent* if for all distinct indices $i_1, i_2, \ldots, i_k$ in D_n and all k-tuples of values $t_1, t_2, \ldots, t_k$ in R_n:

- the probability that $f(i_1) = t_1, \ldots, f(i_k) = t_k$ is at most $C/|R_n|^k$ for some constant C

Relaxed Independence

- Theorem: A relaxed k-wise independent requires complexity $\Omega(k)$

Relation to **Permutation**

- **Permutation** is not k-wise independent for any $k > 1$.
- **Permutation** is relaxed $n^{1/2}/10$-wise independent
- **Permutation** requires property testers of complexity $\Omega(n^{1/2})$.

Sparsity

- The property of all functions is easily testable despite being independent.
- Need some measure of non-degeneracy.
- Say that a property Π_n of F_n (all functions f: D_n -> R_n) is *sparse* if exponentially few functions f in F_n are ε-close to Π_n.

Main Theorem

- Theorem: If a property is relaxed k-wise independent and sparse, then it requires MAP complexity $\Omega(k^{1/2})$.
- Corollary: **Permutation** requires MAP complexity $\Omega(n^{1/4})$.

Discussion

- Question: Does every k-wise independent property requires MAPs of size $\Omega(k)$?
- Question: Does **permutation** requires MAPs of size $\Omega(n^{1/2})$?