Quantum Advantages for Approximate Combinatorial Optimization

Niklas Pirnay, Vincent Ulitzsch, Frederik Wilde, Jens Eisert, Jean-Pierre Seifert
2023-12-01

arXiv:2212.08678

frederikwil.de/hqcc2023

Combinatorial Optimization

- Combinatorial optimization is hard
- Incredibly successful heuristics (for approximation)
- Can quantum computers help?

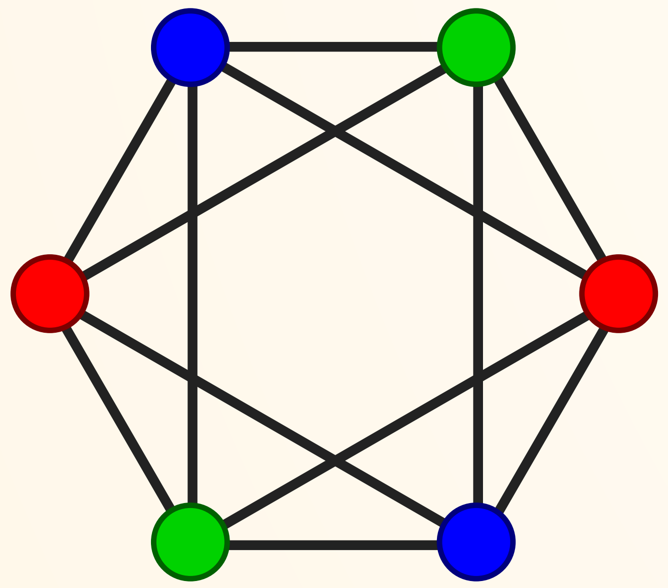
Operations Research Letters
Volume 37, Issue 1, January 2009, Pages 11-15

Certification of an optimal TSP tour through 85,900 cities

David L. Applegate [a], Robert E. Bixby [b], Vašek Chvátal [c], William Cook [d], Daniel G. Espinoza [e], Marcos Goycoolea [f], Keld Helsgaun [g]

APPROXIMATION HARDNESS

- MAX-CUT is APX-hard
- Unless P = NP, there exists no poly-time algorithm that computes a solution with more than $N = \frac{16}{17} N_{\text{opt}}$ cuts for any MAX-CUT instance [Håstad]



Chris Martin
wikimedia CC BY-SA

FORMULA COLORING

- Generalization of graph coloring
- $(z_1 \neq z_2) \wedge ((z_1 = z_3) \rightarrow (z_2 = z_4))$
- NP-complete
- Even hard to approximate! [Kearns]

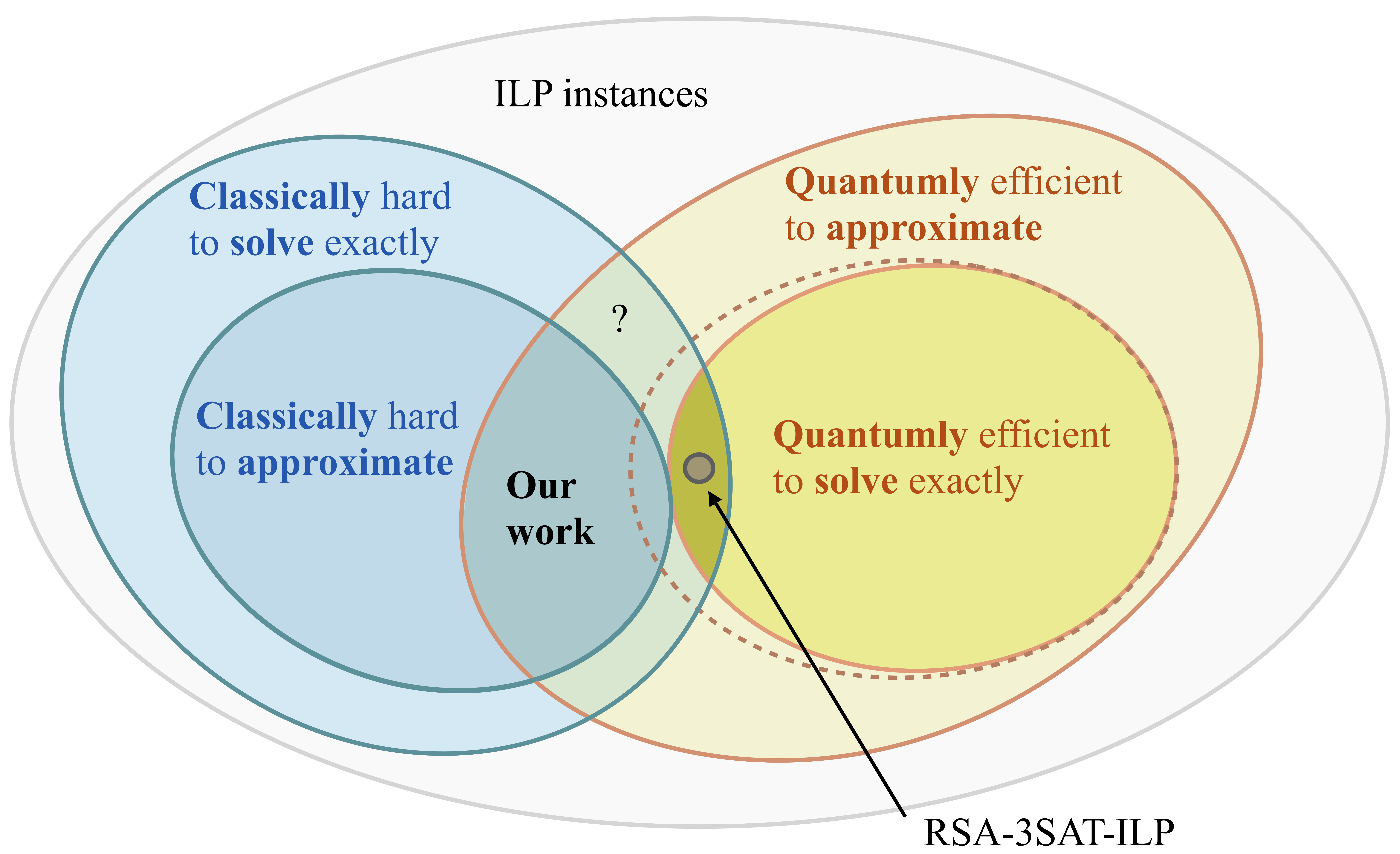
INTEGER LINEAR PROGRAM (ILP)

$$\min_{x \in \mathbb{Z}^n} \mathbf{c} \cdot \mathbf{x}$$

subject to linear constraints

A Provable Approximation Advantage

"A fault tolerant quantum computer can approximate certain combinatorial optimization problems super-polynomially more efficiently than a classical computer." [Pirnay]



Computational Problems and Models

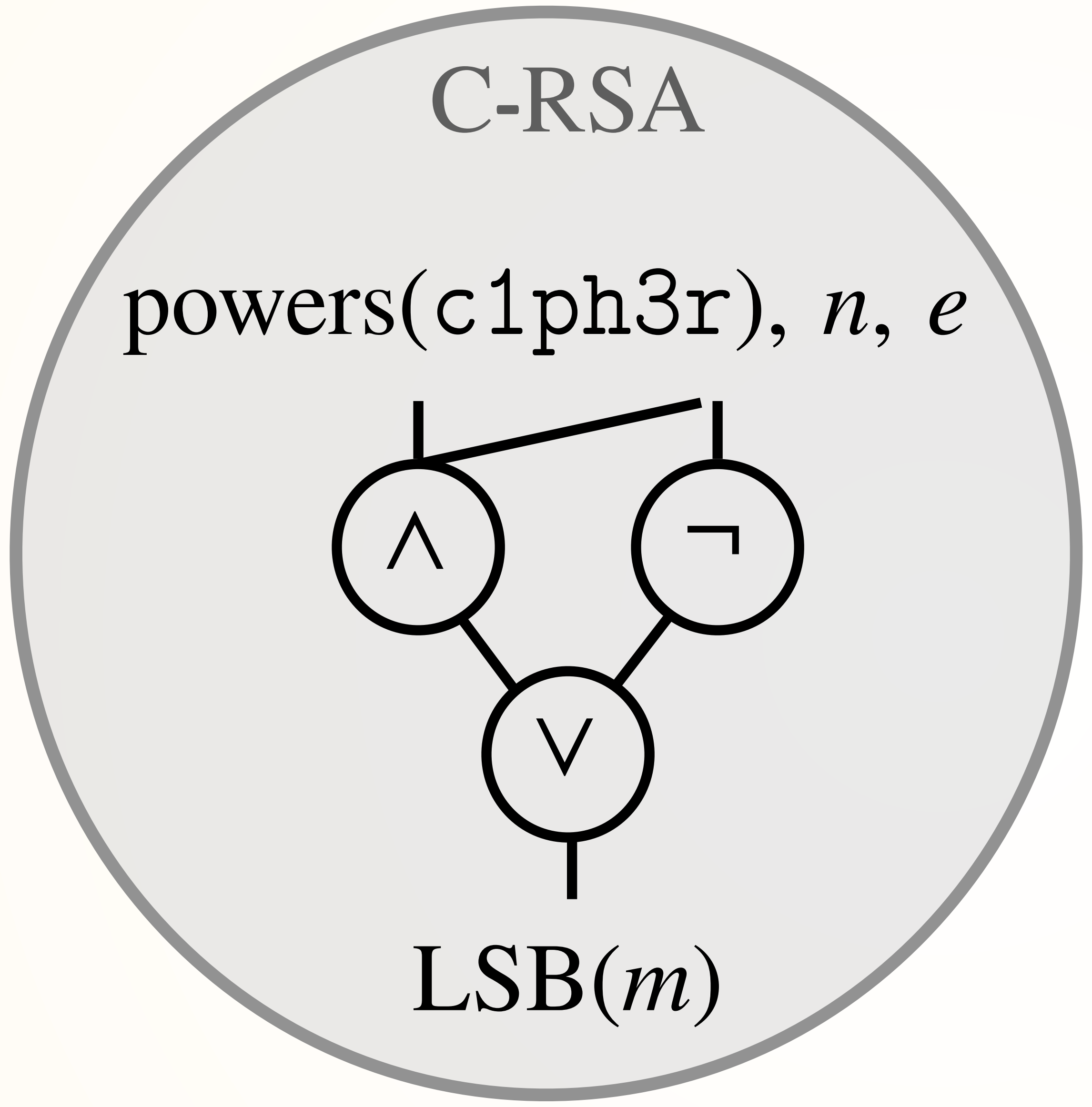
RSA

Public key

$$\texttt{c1ph3r} = m^e \bmod n$$

Private Key

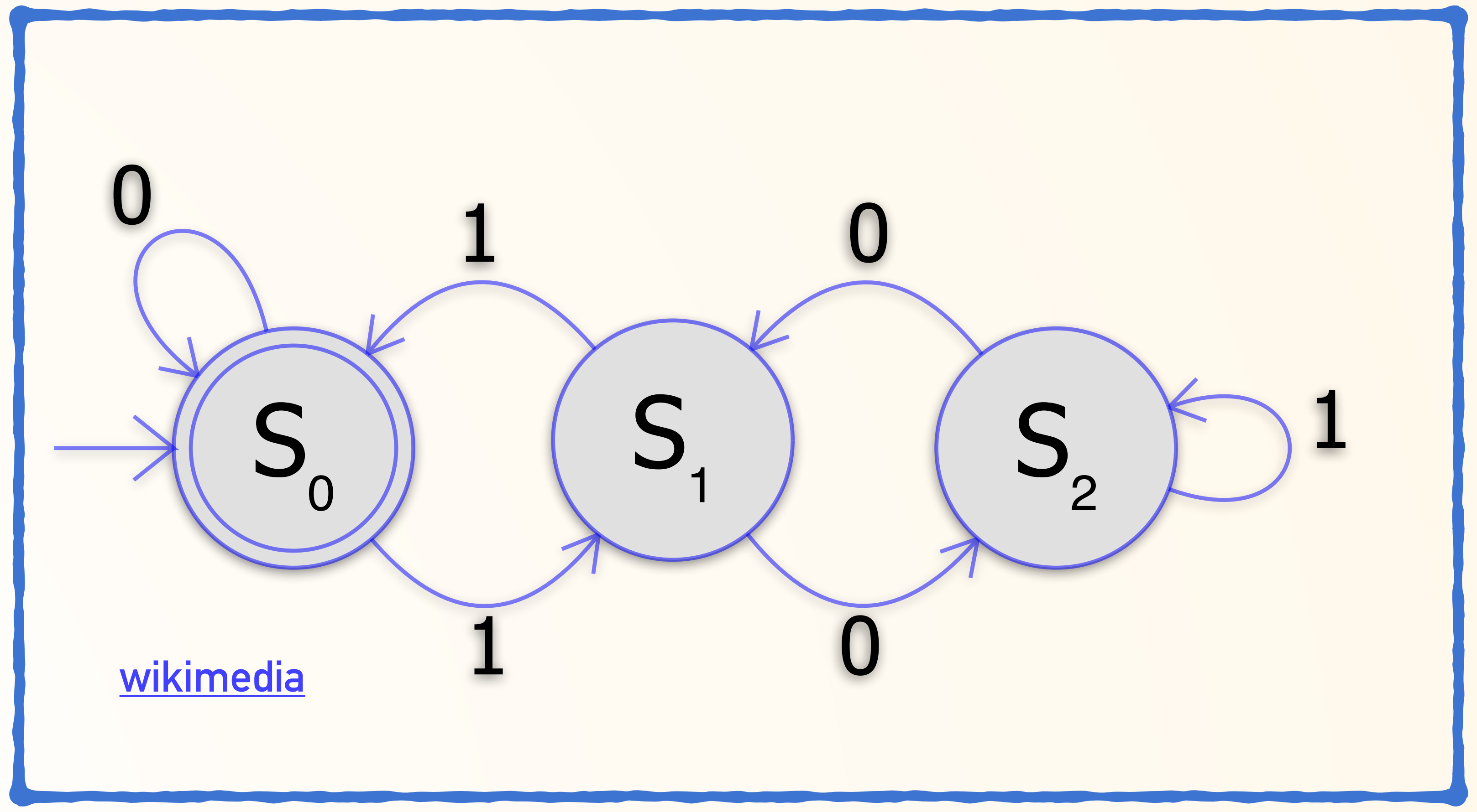
m



Class of log-depth, poly-size Boolean circuits computing $\mathrm{LSB}(m)$

Private key must be hard coded!

Deterministic Finite Automaton (DFA)

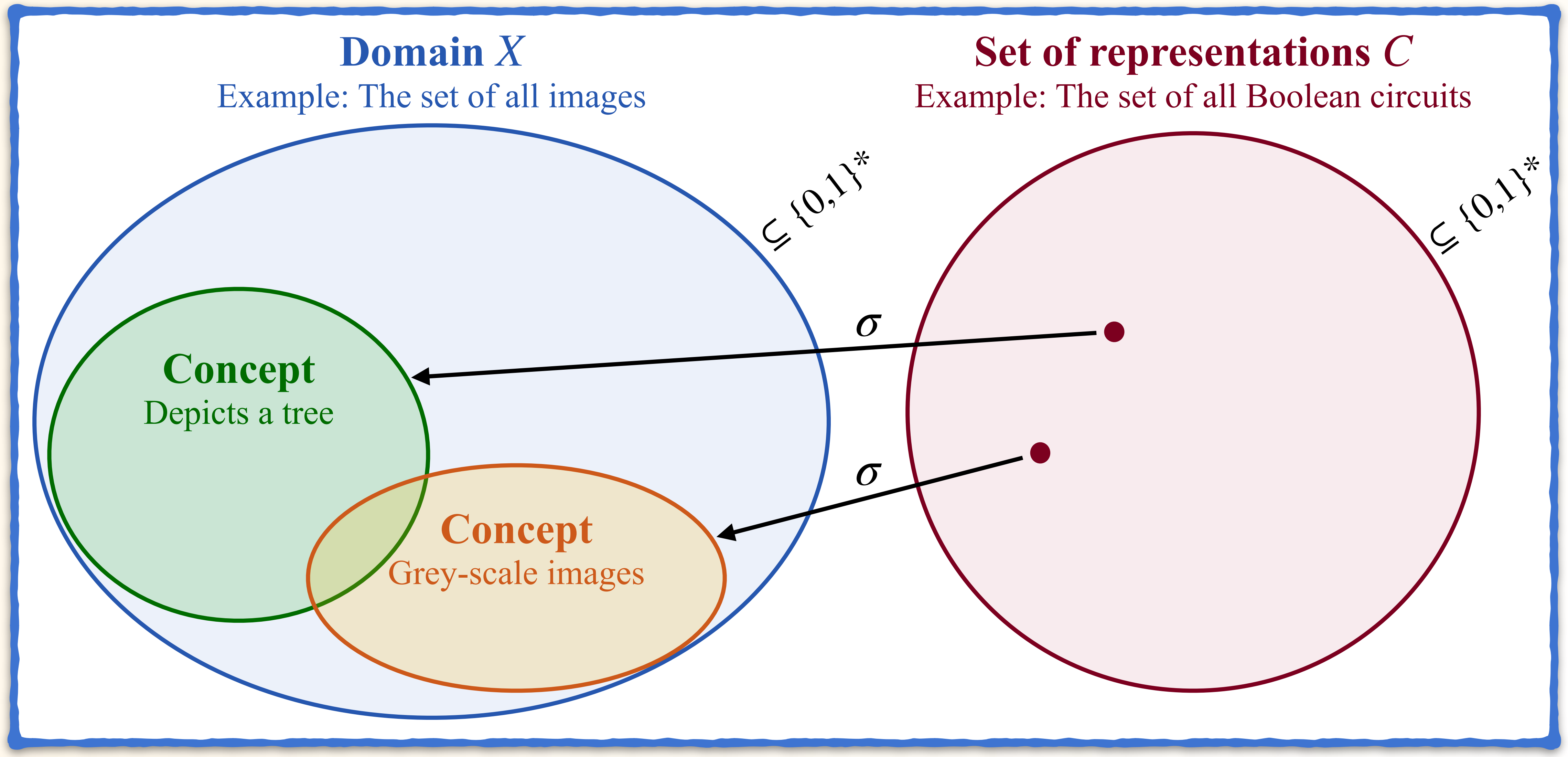


POLYNOMIAL REDUCTION

Computational Problems	A	$\leq_p$	B
Instances	$\mathscr{A}$	τ →	$\mathscr{B}$
Solutions	a	← g	b

A bit of learning theory

CONCEPT CLASS



CONSISTENCY PROBLEM

$\mathrm{Con}(C, H)$

Instance: A set of labeled examples $S = \{(x, c(x)) \mid x \in X\}$

Solution: Minimal-size $h \in H$ which is consistent with S

define: $\mathrm{opt}_{\mathrm{Con}}(S) := |h|$

OCCAM'S RAZOR

For a sample set S of size $|S| = \tilde{\mathcal{O}}\left(\frac{1}{\epsilon} + \left[\frac{n^\alpha}{\epsilon}\right]^{\frac{1}{1-\beta}}\right)$

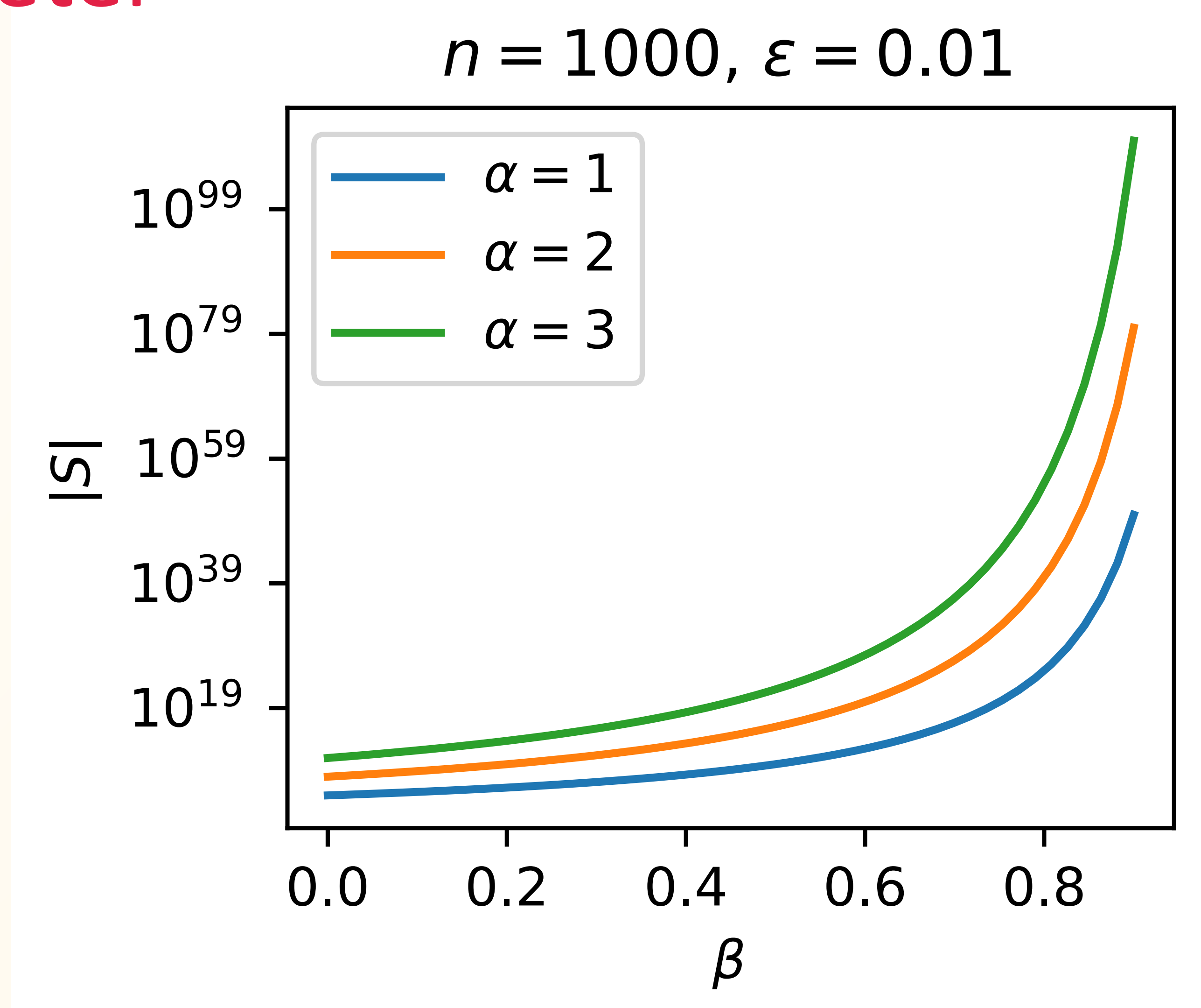
"approximation gap"

compression parameter

any $h \in H$ consistent with S which also satisfies $|h| \leq \mathrm{opt}_{\mathrm{Con}}(S)^\alpha \, |S|^\beta$ achieves $\mathrm{error}(h) := \mathbb{P}_x[h(x) \neq c(x)] \leq \epsilon$ with high probability.

Where $\alpha \geq 1$ and $0 \leq \beta < 1$

[Blumer]



A Provable Approximation Advantage

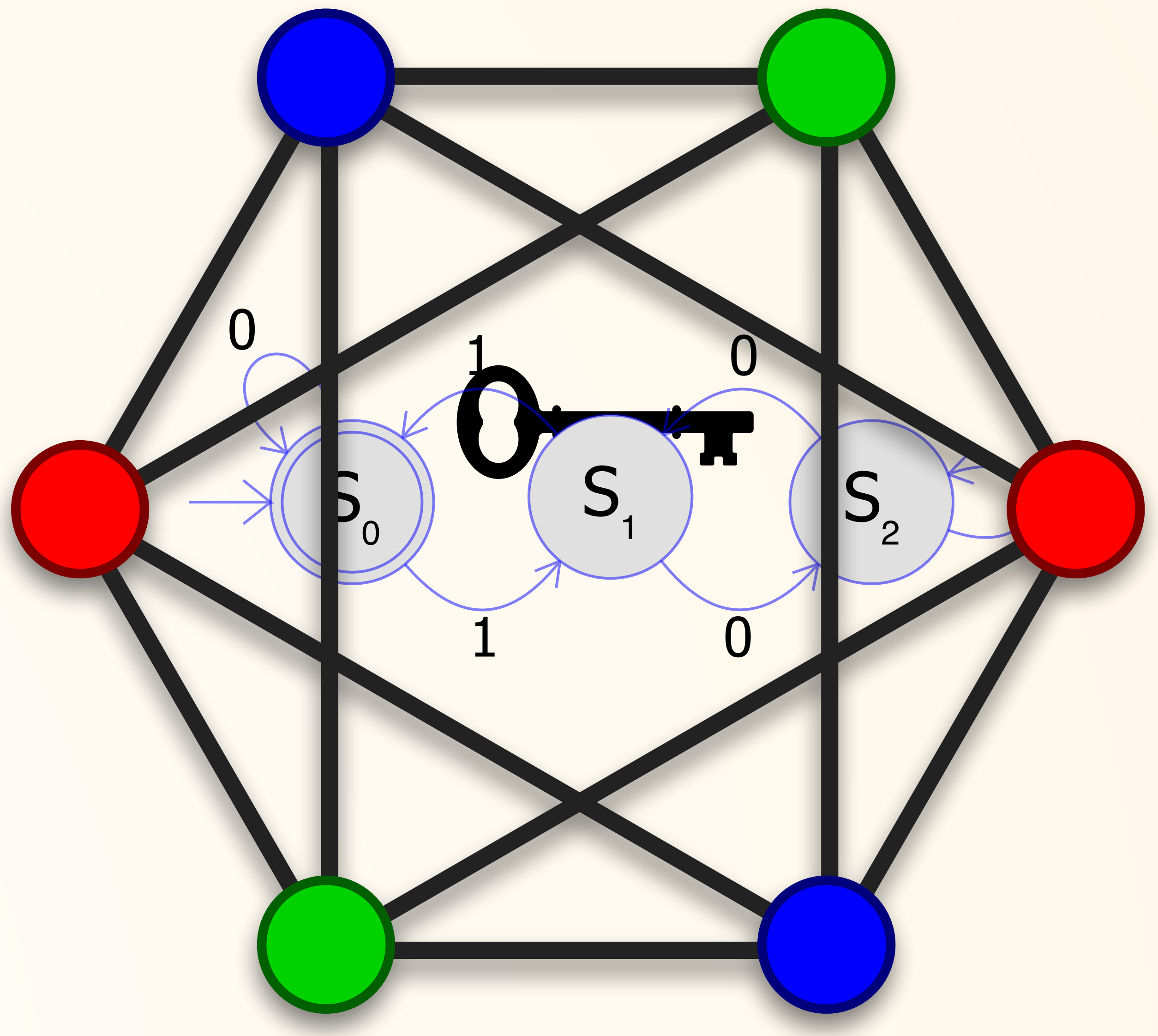
STRATEGY

- Classical hardness of inverting RSA
- Hardness of approximation for Con(C-RSA, H) via Occam's razor
- Approximation preserving reduction to Con(DFA-RSA, DFA) and then FC-RSA [Kearns]
- approximation-preserving reduction to ILP-RSA [Pirnay]
- Efficient quantum algorithm for approximating ILP-RSA [Pirnay]

With sample size $|S| = \mathrm{poly}(n, \epsilon^{-1})$ any $h \in H$ that is consistent with S, s.t. $|h| \le \mathrm{opt}_{\mathrm{Con}}(S)^{\alpha}\, |S|^{\beta}$ achieves error $\le \epsilon$.

- Learning C-RSA by H can be seen as an *approximation task*: Approximate $\mathrm{opt}_{\mathrm{Con}}(S)$
- Approximately learning a C-RSA circuit enables one to break RSA ! [Alexi]

- $|h| \mapsto$ #(partitions)
- $S \mapsto$ FC-graph



approximation preserving reduction

$$\min_{x \in \mathbb{Z}^n} \mathbf{c} \cdot \mathbf{x}$$
subject to constraints

A Provable Approximation Advantage

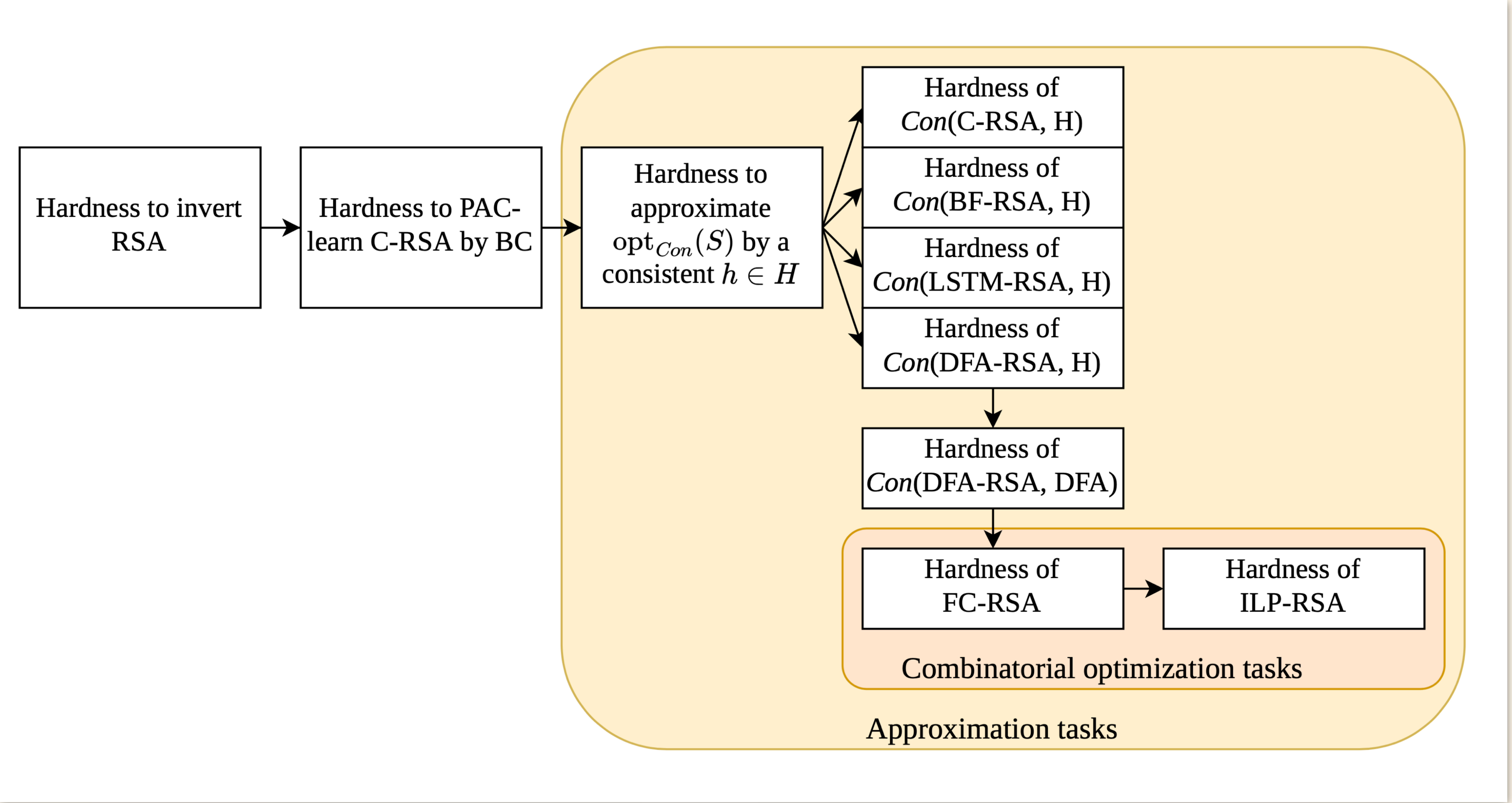


Figure 5 in [Pirnay]

ILP-RSA

By our construction, we get the *integer linear programming* problem ILP_F

$$\text{minimize} \sum_{1 \le i \le M} w_i \tag{22}$$

indicator variable (color i is being used)

indicator variable ($z_u \in P_i$)

subject to the following constraints,

for all $u, i \in \{1, \ldots, M\}$,
$$(x_{u,i} = 1) \iff (\hat{z}_u = i), \tag{23}$$

for all $u \in \{1, \ldots, M\}$, only one color per variable:
$$\sum_{i=1}^{M} x_{u,i} = 1, \tag{24}$$

for all $u, i \in \{1, \ldots, M\}$, count colors:
$$x_{u,i} \le w_i, \tag{25}$$

for all Q clauses $(z_u \neq z_v)$ and all $i \in \{1, \ldots, M\}$,
$$x_{u,i} + x_{v,i} \le 1, \tag{26}$$

for all R clauses $((z_u \neq z_v) \vee (z_k = z_l))$ with $j \in \{1, \ldots, R\}$,
$$(a_j = 1) \iff (\hat{z}_k = \hat{z}_l), \tag{27}$$
$$(b_j = 1) \iff (\hat{z}_u \neq \hat{z}_v), \tag{28}$$
$$s_j = (a_j \vee b_j), \tag{29}$$
$$s_j \ge 1, \tag{30}$$

and $w_i, x_{u,i}, a_j, b_j, s_j \in \{0, 1\}$ and $1 \le \hat{z}_u, \hat{z}_v, \hat{z}_k, \hat{z}_l \le M$. (31)

Classical Hardness of Approximation

Theorem V.12 (Classical hardness of approximation for *integer linear programming*). *Assuming the hardness of inverting the RSA function, there exists no classical probabilistic polynomial-time algorithm that on input an instance* ILP_F *of* ILP-RSA *finds an assignment of the variables in* ILP_F *which satisfies all constraints and approximates the size* $opt_{\mathrm{ILP}}(\mathrm{ILP}_F)$ *of the optimal solution by*

$$\sum_{1 \le i \le M} w_i \le opt_{\mathrm{ILP}}(\mathrm{ILP}_F)^{\alpha} |\,\mathrm{ILP}_F\,|^{\beta} \tag{46}$$

for any $\alpha \ge 1$ *and* $0 \le \beta < 1/4$.

An Efficient Quantum Algorithm

Algorithm 1: Approximate the solution of $Con(\text{C-RSA}, \text{BC})$

Input : A labeled sample S of C-RSA
Output : The description of a Boolean circuit consistent with S

Pick any example $s \in S$ and read e, N from it;
Run *Shor's algorithm* [1] to factor N and retrieve p and q;
Run the extended Euclidean algorithm to compute d, such that $d \times e = 1 \bmod (p-1)(q-1)$;

```
// Note that at this point, d is the secret RSA exponent.
```

Output the description of a Boolean circuit that, on input binary $(\text{powers}_N(\text{RSA}(x, N, e)), N, e)$, multiplies the 2^i'th powers together for which the bit $d_i = 1$ (thereby hard-wiring d into the circuit), using the iterated products technique [33] and outputs the LSB of the result.

Move along the chain of reductions...

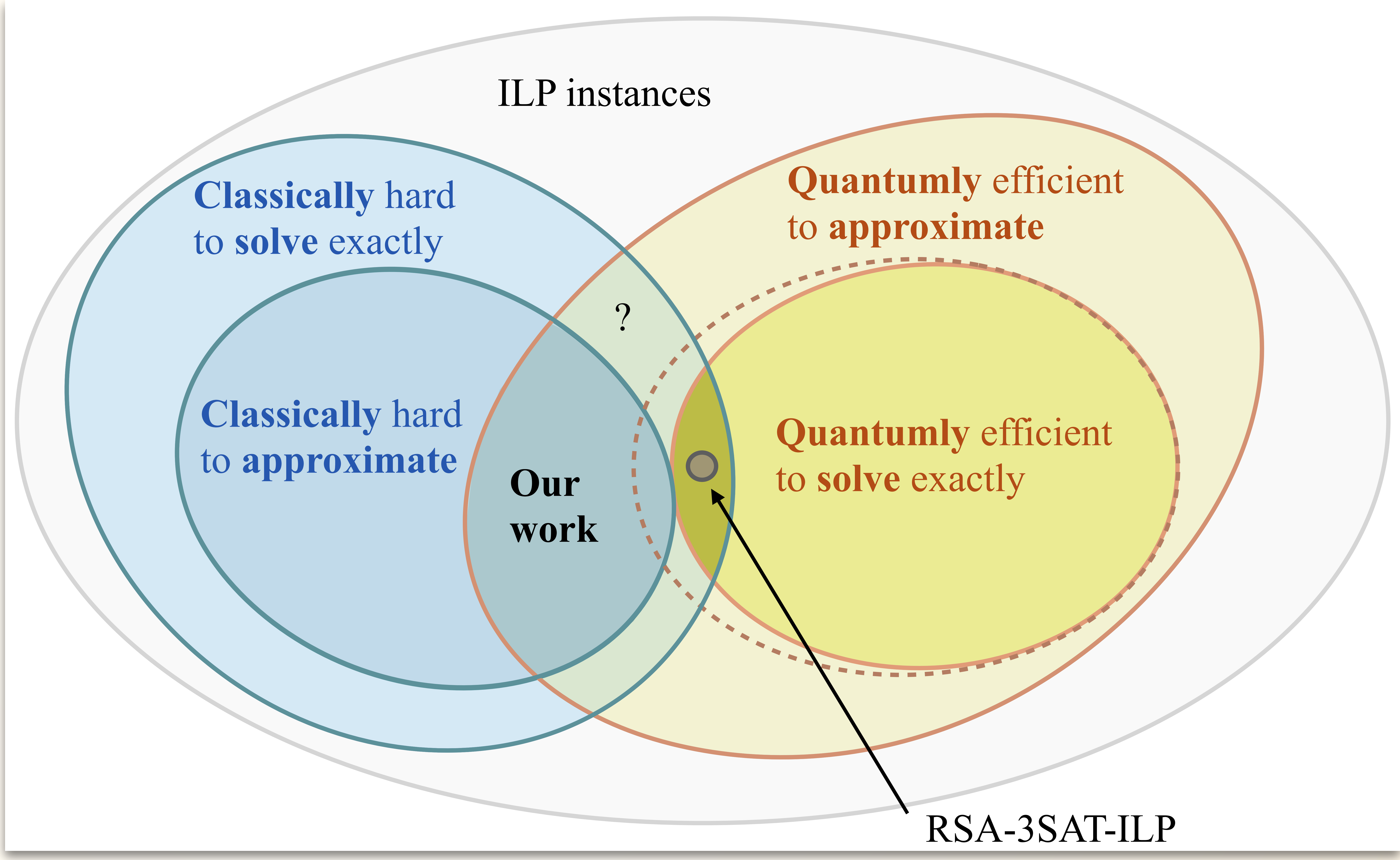
Theorem V.16 (Quantum efficiency for ILP-RSA). *There exists a polynomial-time quantum algorithm that, on input an instance* ILP_{F_S} *of* ILP-RSA, *finds a variable assignment A that satisfies all constraints and for which the objective function is bounded as*

$$\sum_{1 \leq i \leq M} w_i \leq opt_{\text{ILP}}(\text{ILP}_{F_S})^{\alpha}$$

for all ILP_{F_S} *and for some* $\alpha \geq 1$.

Conclusion

- Constructive quantum advantage for approximate optimization
- Opens up new problems to study with actual quantum optimization algorithms (QAOA)
- Alternative proofs via the PCP theorem possible [Szegedy]
- Opens up the path towards more practical *advantage-bearing* instances



Slides at: frederikwil.de/hqcc2023