Kernel-Size Lower Bounds: The Evidence from Complexity Theory

Andrew Drucker

IAS

Worker 2013, Warsaw

Part 1/3

These slides are taken (with minor revisions) from a 3-part tutorial given at the 2013 Workshop on Kernelization ("Worker") at the University of Warsaw. Thanks to the organizers for the opportunity to present!

Preparation of this teaching material was supported by the National Science Foundation under agreements Princeton University Prime Award No. CCF-0832797 and Sub-contract No. 00001583. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Main works discussed

- [BDFH'07] H. Bodlaender, R. Downey, M. Fellows, and D. Hermelin: On problems without polynomial kernels. ICALP 2008, JCSS 2009. (Preprint '07)
- [FS'08] L. Fortnow and R. Santhanam: Infeasibility of instance compression and succinct PCPs for NP. STOC 2008, JCSS 2011.
- [DvM'10] H. Dell and D. van Melkebeek: Satisfiability allows no nontrivial sparsification unless the polynomial-time hierarchy collapses. STOC 2010.
- [DM'12] H. Dell and D. Marx: Kernelization of packing problems. SODA 2012.
- [D'12] A. Drucker: New limits to classical and quantum instance compression. FOCS 2012.

- Part 1: introduction to the OR- and AND-conjectures and their use. Covers [BDFH'07], [DvM'10], [DM'12].
- Part 2: Evidence for the OR-conjecture [FS'08]
- Part 3: Evidence for the AND-conjecture (and OR-conjecture for probabilistic reductions) [D'12]

- P vs. NP: The central mystery of TCS.
- Can't understand this problem, but would like to use

 $\mathsf{P} \neq \mathsf{N}\mathsf{P}$

hypothesis to "explain" why many tasks are difficult.

- These talks: describe how (an extension of) $P \neq NP$ can explain hardness of kernelization tasks.
- Our focus: building the initial bridge between these two domains.
- [Many other papers]: clever reductions between kernelization problems, to show dozens of kernel lower bounds (LBs).

Introduction

- OR/AND-conjectures and their use
- Sevidence for the conjectures



- Input: Formula ψ .
 - Is ψ satisfiable?
- Parameters of interest:
 - total bitlength;
 - # clauses;
 - # variables;
 - can invent many more measures.

- Our view in these talks:
 - computational problems can have multiple interesting parameters.
 - won't define parameters formally, but always will be easily measureable.

 $x \longrightarrow k(x)$

• Insist: $k(x) \leq |x|$

• A parametrized problem *P* with associated parameter *k* is Fixed-Parameter Tractable (FPT) if some algorithm solves *P* in time

 $f(k(x)) \cdot poly(|x|)$.

- Self-reduction for problem P: a mapping R s.t.
 - x a "Yes"-instance of $P \iff R(x)$ a "Yes"-instance of P

- Goal: want R(x) to be smaller than x.
- This talk: only interested in poly-time self-reductions.
- (Will also discuss reductions between param'd problems...)

- Let *F* be a function.
- Poly-time self-reduction *R* is an *F*(*k*)-kernelization for *P* w.r.t. parameter *k*, if:

 $\forall x: \qquad |R(x)| \leq F(k(x))$

• Output ("kernel") size bounded by function of the parameter alone!

- *F*(*k*)-kernels for any (decidable) problem yields an FPT algorithm.
- Many natural FPT algorithms have this form.

Virtues of kernels

 If F(k) ≤ poly(k) and problem is in NP, we get an FPT alg. with runtime



• *F*(*k*) ≤ poly(*k*): "Polynomial kernelization"

- Kernelization lets us compress instances to store for the future.
- Also allows us to succinctly describe instances to a second, more powerful computer.

- Many great kernelization algs; won't survey here...
- Which problems fail to have small kernels?

Kernelization limits

- For decidable problems:
 - F(k)-kernels implies FPT, so...
 - NOT FPT implies no F(k)-kernels for any F!
- E.g., k-Clique is W[1]-complete, so is not FPT or
 F(k)-kernelizable, unless

 $\mathsf{FPT}=\mathsf{W}[1]$

Leaves possibility that all "natural" problems in FPT have poly(k)-kernels!

- A few kernel size LBs based on $P \neq NP...$
- "Dual parameter" technique [Chen, Fernau, Kanj, Xia '05] shows that k-Planar Vertex Cover has no 1.332k-kernels* unless P = NP.

* (only applies to reductions that don't increase k)

- A few kernel size LBs based on $P \neq NP...$
- Similar results for kernels of restricted form, based on NP-hardness of approximation [Guo, Niedermeier '07].
- These bounds are all $\Theta(k)$.

- Lower bound tools were limited, until a paper of [Bodlaender, Downey, Fellows, Hermelin '07].
- Introduced "OR-" and "AND-conjectures," showed that these would rule out poly(k)-kernels for many problems.
- Related, independent work in crypto: [Harnik, Naor '06]

- Many follow-up works showed the usefulness, versatility of the OR-conjecture for kernel LBs.
- We'll describe one important example: [Dell, Van Melkebeek '10] (and follow-up by [Dell, Marx '12])

• [Fortnow, Santhanam '08] and [D. '12] showed the OR, AND-conjectures follow from a "standard" assumption in complexity, namely

 $\mathsf{NP} \nsubseteq \mathsf{coNP}/\mathsf{poly}$.

• (We'll discuss this assumption...)

• We now have strong kernel-size LBs for most problems that resisted kernels. E.g.: unless NP \subset coNP/poly:

• k-Path does not have poly(k)-kernels;

- 2 Same for k-Treewidth;
- N-Clique (param. N = # vertices), which has a trivial N² kernel, does not have have kernels of size N^{2-ε}.

(For *d*-uniform hypergraphs, we have the tight threshold N^d .)

• Before telling this story...

Whats the real significance of these negative results?

"Kernelizations are assumed to be deterministic. That's too limited."

Agreed.

- In practice, <u>almost</u> all kernelizations we know are deterministic. But for meaningful lower bounds, we need to understand randomized ones as well.
- But—since [D.'12], our kernel LBs also apply to randomized algorithms.

"Kernelizations are assumed to map problem instances to instances of the same problem. That's also too limited."

- But all known kernel LBs for NP problems are insensitive to the target problem.
- They apply to "cross-kernelization" as well.

"Some applications of kernelization could be achieved under a broader definition. You're just ruling out one path to those goals."

Agreed.

- In particular, self-reductions which output <u>many smaller</u> <u>instances</u> (whose solutions yield a solution to the original instance) could be nearly as useful for FPT algs. [Guo, Fellows]
- We don't understand full power of these "Turing kernels" (yet!)
- Question explored by [Hermelin, Kratsch, Soltys, Wahlstrom, Wu '10].

- Kernelization also useful to succinctly transmit hard problems to a powerful helper. ⇒ Natural to allow 2-way interaction.
- [Dell, Van Melkebeek '10]: boost our kernel LBs to communication LBs. (More general!)
- OPEN: extend to probabilistic communication.

"Ultimately, kernelization is just one approach to fast algorithms. Many of the LBs are for problems which already have good FPT algs."

...but this criticism also applies to kernel upper-bound research! Many papers give kernels where good FPT results were already known. Kernelization is a natural, rich algorithmic paradigm.

It's worthwhile and interesting to understand its strengths \underline{and} limitations.

Introduction

OR/AND-conjectures and their use

- [Bodlaender, Downey, Fellows, Hermelin '07] got this project rolling.
- What core idea lies behind their work?

"Many param'd problems can express an OR of a large number of subproblems, without a blowup in the parameter.

"Those problems should resist small kernels... for a shared reason."

OR(L)

Let $L \subseteq \{0,1\}^*$. Define the problem OR(L) by:

- Input: a list $\langle x^1, \ldots, x^t
 angle$ of binary strings.
- Decide: is some $x^j \in L$?
- Parameter: $k := \max_{i} |x^{j}|$.

To ease discussion, let $OR_{=}(L)$ be the special case where we require that

$$|x^i| = |x^j| = k \quad \forall i, j .$$

(even this special case resists small kernels.)
AND(L)

Define the problem $AND_{=}(L)$ by:

- Input: a list $\langle x^1, \ldots, x^t \rangle$ of binary strings.
- Decide: is every $x^j \in L$?
- Parameter: $k := |x^i| = |x^j|, \quad j = 1, 2, ..., t.$

One approach to kernelization: sparsification



May try to identify instances that are "logically least-likely" to lie in L, remove them.

One approach to kernelization: sparsification



May try to identify instances that are "logically least-likely" to lie in L, remove them.

One approach to kernelization: sparsification

- Reasonable idea, but no nontrivial kernel size bounds known for OR₌(L), AND₌(L)...
- No equivalence between the two tasks either!

Let *L* be any NP-complete language.

- OR-conjecture: The problem OR₌(*L*) does <u>not</u> have poly(*k*)-kernels.
- AND-conjecture: The problem $AND_{=}(L)$ does not either.

Slightly "massaged" forms of the conjectures. [BDFH'07]: equivalent to respective conjectures for OR(SAT), AND(SAT) (but we won't need this) [BDFH'07]: The OR-conjecture \implies none of these problems have poly(k)-kernels:

- k-Path, k-Cycle, k-Exact Cycle and k-Short Cheap Tour,
- k-Graph Minor Order Test and k-Bounded Treewidth Subgraph Test,
- *k*-Planar Graph Subgraph Test and *k*-Planar Graph Induced Subgraph Test,
- (*k*, *σ*)-

Short Nondeterministic Turing Machine Computation,

• *w*-Independent Set, *w*-Clique and *w*-Dominating Set.

Dozens more in later works.

[BDFH'07]: The AND-conjecture \implies none of these problems have poly(k)-kernels:

- k-Cutwidth, k-Modified Cutwidth, and k-Search Number,
- k-Pathwidth, k-Treewidth, and k-Branchwidth,
- k-Gate Matrix Layout and k-Front Size,
- w-3-Coloring and w-3-Domatic Number,

- OR, AND-conjectures connect to <u>specific</u> parametrized problems through various technical lemmas and reductions.
- Here we explain one of the <u>simplest such connections.</u>¹ Still quite powerful.

¹Related to definitions in [Harnik-Naor '06], [BDFH'07], [Bodlaender, Jansen, Kratsch '11]

Claim

Let L be NP-complete, P a parametrized problem, and suppose there is a poly-time reduction R from an instance \overline{x} to $OR_{=}(L)$ to an equivalent instance of P, with

 $k(R(\overline{x})) \leq \operatorname{poly}(k(\overline{x}))$.

Then, if P has some poly(k)-kernelization A, so does $OR_{=}(L)$ (and the OR-conjecture fails).

Proof.

To kernelize an instance \overline{x} of $OR_{=}(L)$:

$$\overline{x} \rightarrow R(\overline{x}) \rightarrow A(R(\overline{x})) \rightarrow$$
 (reduce to L).

Claim

Let L be NP-complete, P a parametrized problem, and suppose there is a poly-time reduction R from an instance \overline{x} to AND₌(L) to an equivalent instance of P, with

 $k(R(\overline{x})) \leq \operatorname{poly}(k(\overline{x}))$.

Then, if P has some poly(k)-kernelization A, so does $AND_{=}(L)$ (and the AND-conjecture fails).

Proof.

To kernelize an instance \overline{x} of AND₌(*L*):

$$\overline{x} \rightarrow R(\overline{x}) \rightarrow A(R(\overline{x})) \rightarrow (\text{reduce to } L) \;.$$

Let's see some (easy) examples.

Define *k*-Path:

• Input: $\langle G, k \rangle$.

• Decide: does G have a simple path of length k?

k-Path is FPT, runtime $2^{O(k)} \operatorname{poly}(n)$ [Alon, Yuster, Zwick '95]. But no $\operatorname{poly}(k)$ -kernel known.

- Apply our Claim to show that *k*-Path is hard to kernelize.
- How to express an OR of many NP instances of size s, as a single instance of k-Path, with k ≈ s?
- Which *L* to choose?





- Take L = HAMILTONIAN PATH.
- Use graph encoding where length-k² input encodes a graph on k vertices.
- On the input $\langle G_1, \ldots, G_t \rangle$ to $OR_{=}(L)$ (where $|\langle G_i \rangle| = k^2$), output

$$\left\langle H := \bigcup^{\cdot} G_j, k \right\rangle$$
.

• *H* has a simple *k*-path \iff some *G_i* has a Ham path.

Define *k*-Treewidth:

- Input: $\langle G, k \rangle$.
- Decide: does G have treewidth^{*} ≤ k?
 *(tw = a monotone measure of graph "fatness")

Treewidth an important graph complexity measure for FPT alg. design.

k-Treewidth FPT, but treewidth is NP-hard to compute exactly.

• Given graphs G_1, \ldots, G_t , if

$$H := \bigcup G_j$$

then

$$\operatorname{tw}(H) := \max_{i} (\operatorname{tw}(G_i)) ,$$

so

$$\operatorname{tw}(H) \leq k \iff \bigwedge_{i} [\operatorname{tw}(G_{i}) \leq k].$$

 Basis of proof that (AND-Conjecture) ⇒ k-Treewidth has no poly(k)-kernels. We take

$$L := \{\langle G \rangle : \operatorname{tw}(G) \leq |V(G)|/2 \}$$

- In k-Treewidth, k-Path examples, choice of NP-complete language L was "obvious," closely related to param'd problem.
- Time has shown: sometimes "best" choice of *L* is not obvious, makes reductions easier.

(We'll see an example...)

- We've seen a strong framework for ruling out poly(k) kernels (modulo the AND-/OR-conjectures).
- Shortly after [BDFH'07], Fortnow and Santhanam showed OR-conjecture is true (for deterministic algorithms) if NP ⊈ coNP/poly. (We'll come back to this...)
- Dell and Van Melkebeek built on [BDFH'07,FS'08] ideas to give tight kernel LBs for problems that do have poly(k)-kernels.
- How??

- First step: studied [FS'08] carefully!
- [FS'08] implicitly shows something <u>much stronger</u> than the OR-conjecture.
- Important to know this...

• Recall $OR_{=}(L)$: given x^1, \ldots, x^t each of length k, compute

 $\bigvee_{i\in[t]} [x^i \in L] \; .$

- Let t(k) be a function, and let OR₌(L)^{t(·)} be the same problem where we further restrict t = t(k).
- Focus on "reasonable" $t(\cdot)$: easily computable, and satisfy

 $t(k) \leq \operatorname{poly}(k)$.

Theorem

[FS'08, implicit]: Assume NP $\not\subseteq$ coNP/poly. If L is NP-complete and $t(k) \leq \text{poly}(k)$, no poly-time reduction R from $OR_{=}(L)^{t(\cdot)}$ to any other problem can achieve output size

 $|R(\overline{x})| \leq O(t \log t) ,$

where t = t(k), $k = k(\overline{x})$.

- E.g., take $t(k) := k^{100}$.
- Then input (x¹,..., x^{t(k)}) to OR₌(L)^{t(·)}, of size k · k¹⁰⁰, cannot be reduced to a kernel of size < k¹⁰⁰!
- Here, OR₌(L)^{t(·)} trivially has a k¹⁰¹-kernel, and by [FS'08] it is nearly optimal!

- Corollary: the *k*-Path problem on k^{100} -vertex graphs does not have kernels of size k^{100} .
- So [DvM'10] not really the first ones to prove good fixed-poly kernel LBs. Their achievement:
 - Express OR₌(L) instances very efficiently within a parametrized problem instance, minimizing parameter blowup;
 - Find a way to "boost" the [FS'08] bound and get truly tight results.

Define the *N*-Clique problem as:

- Input: $\langle G, s \rangle$.
 - (G a graph on N vertices; $s \leq N$)
- Decide: Does G have a clique of size s?
- Parameter: N.
- Natural input size: up to N².
 Can we compress?

- For kernel LBs, goal is to efficiently express an OR of NP instances within an *N*-Clique instance.
- Can easily express an OR of NP instances by $\bigcup \ \ldots$
- <u>Problem</u>: blows up the parameter *N* linearly!
 Wasteful, since most potential edges are not used...

- Idea: "Pack" many CLIQUE instances into one graph, in a way that creates no large "unwanted" cliques.
- Main effort: Find special "host" graph to contain these instances.

Edge-disjoint clique packing: example



Lemma (Packing Lemma for graphs, DvM '10)

For any s, t > 0 there is a graph G^* on

 $s \cdot (s + t^{.5+o(1)})$

vertices. $E(G^*)$ is union of t edge-disjoint cliques K_1, \ldots, K_t of size s, and has no other ("unwanted") s-cliques. G^* can be constructed in time poly(s + t).

With this lemma we can "embed" t instances of an appropriate problem into K₁,..., K_t respectively.

(Details...)

Lemma

For any s, t > 0 there is a graph G^* on

 $s \cdot (s + t^{.5+o(1)})$

vertices. $E(G^*)$ is union of t edge-disjoint cliques K_1, \ldots, K_t of size s, and has no other ("unwanted") s-cliques.

- Cliques K_i, K_j can intersect in at most one vertex.
- Suggests we consider them as lines in a (finite) plane...

- Fix any prime p > s.
- We'll build a graph *G* with *sp* vertices, and see how large we can take *t*...
- Vertex set: LP = $\mathbb{F}_{p} \times \{0, 1, \dots, s-1\}$. ("left-plane")

The "left-plane"



• line in LP:

$$\ell_{[a,b]} = \{(x,y) \in \mathsf{LP} : y = ax + b\} \qquad (a,b \in \mathbb{F}_p, a \neq 0)$$

• For each line ℓ define

$$\mathcal{K}_{\ell} \;=\; \left\{ \left((x,y) \;,\; (x',y')
ight) \;:\; (x,y), (x',y') \in \ell
ight\}$$

Lines and line-cliques



Lines and line-cliques



- K_l, K_l are <u>edge-disjoint</u> as needed. (two points contained in unique line)
- Each K_l is a clique of size s! (so sp cliques placed in total.)
- Problem: many other *s*-cliques...

- Inspired idea: restrict the slope of lines we use.
- Choose "special" $A \subset \mathbb{F}_p^*$, and take

$$E(G^*) = \bigcup_{\mathrm{slope}(\ell) \in A} K_\ell \; .$$

• $A = \text{large set without length-3 arithmetic progressions}}$ (3-APs).
- Key claim: The only s-cliques in G^* are the K_{ℓ} 's we included.
 - Why true?
 - What does it get us?

• In our construction, we packed $p \cdot |A|$ cliques of size s into G^* .



- So to pack t cliques, we may take $p \le s + t^{.5+o(1)}$.
- Number of verts. $N = sp \le s(s + t^{.5+o(1)})$, as needed!

- First, no "vertical" edges ((x, y), (x, y')) in G^* .
- Thus any s-clique must have one element from each "column"

$$\operatorname{col}_j = \mathbb{F}_p \times [j]$$
.

 If K_{bad} is an s-clique in G* not equal to some K_ℓ, then ∃ some three adjacent columns like so:









Claim: $a_1 + a_3 = 2a_2$



Claim: $a_1 + a_3 = 2a_2$



 $y_2 - y_1 = a_3$



$$y_2 - y_1 = a_3$$





Conclude: $a_1 + a_3 = 2a_2$



This contradicts (*A* is 3-AP-free).

The upshot

Theorem (DvM'10)

Fix any $t(k) \leq \text{poly}(k)$. There is an NP-complete language L, and a poly-time reduction from $OR_{=}(L)^{t(k)}$ to N-Clique, whose output instance $\langle G, s \rangle$ satisfies

$$N = |V(G)| \leq O(k^2 + k \cdot t^{.5+o(1)})$$

- Now suppose N-Clique had a kernelization R' with output size bound N^{2-ε}.
- Let t(k) := k^C, for some C ≫ 1/ε. Apply R to the output of DvM reduction. Maps OR₌(L)^{t(k)} instance to an N-Clique instance of size

$$O\left(\left[k^{2}+k\cdot k^{.5C+o(1)}\right]^{2-\varepsilon}\right) = o\left(k^{C-1}\right)$$

 But L is NP-complete, so [FS'08] tells us: can't compress OR₌(L)^{k^C} instances even to size O(k^C log k)

(of <u>any</u> target problem)...

- <u>unless</u> NP \subset coNP/poly.
- Similar proof: N-Clique on d-hypergraphs does not have N^{d-ε}-kernels. Same for N-Vertex Cover, others.

- [Dell, Marx '12]: simpler proofs of these and related results.
- Basic idea: to efficiently compress OR₌(*L*) instances into *N*-Clique, choose *L* as an NP-complete language with "special structure"

(making instances easier to combine in a shared graph)

Define L = FUSSY-CLIQUE:

• Input: A graph G on $2s^2$ vertices, presented as

 $V(G) = X_1 \cup \ldots \cup X_s \cup Y_1 \cup \ldots \cup Y_s .$

Require:

- each $X_i(Y_i)$ is an independent set of size s;
- each pair (X_i, X_j) is a complete bipartite graph (i ≠ j). Same for (Y_i, Y_j).
- Decide: does G have a clique of size 2s?
- NP-complete ([Dell, Marx '12], essentially)

Structure of "fussy" graphs





Structure of "fussy" graphs



The "fussy clique" problem

• Easy to compress *OR*₌(FUSSY-CLIQUE) instance into an *N*-Clique instance.

Given: t FUSSY-CLIQUE instances

 $\{G_{p,q}\}_{p,q \leq \sqrt{t}}$.

• Create graph G^* on $\sqrt{t} \times 2s^2$ vertices, in *s*-vertex parts $X_{p,i}$, $Y_{p,i}$ $i \le s, \ p \le \sqrt{t}$.

• For $p,q \leq \sqrt{t}$, place copy of $G_{p,q}$ on vertex-set

$$\overline{X}_{p} := X_{p,1}, \ldots, X_{p,s} \quad \cup \quad \overline{Y}_{q} := Y_{q,1}, \ldots, Y_{q,s} \; .$$

The "fussy clique" problem



The "fussy clique" problem



- Analysis: First: if some $G_{p,q}$ has an 2s-clique, so does G^* .
- Now suppose G^* has an 2*s*-clique *C*. Can intersect only <u>one</u> \overline{X}_p , and <u>one</u> \overline{Y}_q .
- Every $G_{p,q'}$ using \overline{X}_p adds the same edges within \overline{X}_p . Similarly for \overline{Y}_q .
- Thus, C must be a clique in $G_{p,q}$!
- Have reduced OR₌(FUSSY-CLIQUE)^t to an N-Clique instance ⟨G^{*}, 2s⟩ with N = |V(G^{*})| ≤ O(s²√t).
- Here $|\langle G_{p,q} \rangle| \approx s^4$, so reduction is good enough to infer the same kernel-size lower bounds we got from [DvM'10].