Consistency of circuit evaluation, extended resolution and total NP search problems

Jan Krajíček

Faculty of Mathematics and Physics
Charles University in Prague*

Abstract

We consider sets $\Gamma(n,s,k)$ of narrow clauses expressing that no definition of a size s circuit with n inputs is refutable in resolution R in k steps. We show that every CNF with a short refutation in Extended R, ER, can be easily reduced to an instance of $\Gamma(0,s,k)$ (with s,k depending on the size of the ER-refutation) and, in particular, that $\Gamma(0,s,k)$ when interpreted as a relativized NP search problem is complete among all such problems provably total in bounded arithmetic theory V_1^1.

We use the ideas of implicit proofs from [9, 10] to define from $\Gamma(0,s,k)$ a non-relativized NP search problem $i\Gamma$ and we show that it is complete among all such problems provably total in bounded arithmetic theory V_2^1. The reductions are definable in S_2^1.

We indicate how similar results can be proved for some other propositional proof systems and bounded arithmetic theories and how the construction can be used to define specific random unsatisfiable formulas, and we formulate two open problems about them.

Let C be a size s circuit with n Boolean inputs $\mathbf{x} = x_1, \ldots, x_n$ over the basis $0, 1, \neg, \vee, \wedge$. It is defined by s instructions how to compute Boolean values $\mathbf{y} = y_1, \ldots, y_s$, all of which have one of the following forms:

- $y_i := x_u$ for some $u \leq n$,
- $y_i := 0$ or $y_i := 1$,
- $y_i := \neg y_j$ for some $j < i$,
- $y_i := y_j \vee y_k$ or $y_i := y_j \wedge y_k$ for some $j, k < i$.

The value of y_s is the output value of C and is denoted also as $C(\mathbf{x})$. Let $\mathrm{Def}_C^{n,s}(\mathbf{x}, \mathbf{y})$ be the canonical 3CNF formula expressing the conjunction of all instructions. For example, the instruction $y_i := 0$ is represented by one clause

*MSC 2010: Primary 03F20, Secondary 68Q15.

$\{y_i^0\}$, $y_i := \neg y_j$ by 2 clauses $\{y_i, y_j\}, \{y_i^0, y_j^0\}$ and the instruction $y_i := y_j \vee y_k$ is represented by three clauses

$$\{y_j^0, y_i^1\}\ ,\ \{y_k^0, y_i^1\}\ ,\ \{y_i^0, y_j^1, y_k^1\}$$

where for a literal ℓ we let $\ell^1 := \ell$ and $\ell^0 := \neg\ell$. $\mathrm{Def}_C^{n,s}(\mathbf{x}, \mathbf{y})$ has at most $3s$ clauses.

It is easy to prove in the propositional resolution proof system R that the computation of C is unique: in $O(i)$ steps derive from $\mathrm{Def}_C^{n,s}(\mathbf{x}, \mathbf{y}) \cup \mathrm{Def}_C^{n,s}(\mathbf{x}, \mathbf{z})$ clauses $\{y_i^1, z_i^0\}, \{y_i^0, z_i^1\}$ expressing that $y_i \equiv z_i$. The whole proof of $y_s \equiv z_s$ has $O(s)$ clauses and its structure is quite close to that of C.

But can we prove equally easily that a computation of C on $\mathbf{x}$ exists? This question is in propositional logic represented by the question of whether $\mathrm{Def}_C^{n,s}(\mathbf{x}, \mathbf{y})$ is consistent, i.e. not refutable, and we take as our refutation system R (more precisely, its slight technical variant R^w defined in Section 1). Given $n \geq 0, s, k \geq 1$ we shall define a set $\Gamma(n, s, k)$ of narrow clauses such that satisfying assignments for $\Gamma(n, s, k)$ would be precisely k step R^w-refutations of sets $\mathrm{Def}_C^{n,s}(\mathbf{x}, \mathbf{y})$. Our question can be then phrased as follows: How hard it is to refute $\Gamma(n, s, k)$?

We will, in fact, concentrate on the case $n = 0$ in which the sets $\Gamma(0, s, k)$ talk about refutations of $\mathrm{Def}_C^{0,s}(\mathbf{y})$, sets of clauses defining a straight-line program C computing Boolean constants (i.e. C has no inputs $\mathbf{x}$). Using standard techniques of proof complexity we show that sets $\Gamma(0, s, k)$ express the reflection principle for Tseitin's [13] Extended resolution ER, and hence any proof system that refutes these sets by polynomial size proofs has at most polynomial slowdown over ER (it simulates it in the standard terminology). In fact, due to the combinatorial transparency of $\Gamma(0, s, k)$ we use rather only the idea how reflection principles work rather than any "technique" surrounding them. Further, the simulation yields straightforwardly a reduction of unsatisfiable CNFs Δ to $\Gamma(0, s, k)$ where k depends on the size of an ER-refutation of Δ, if we interpret them as relativized total NP search problems with oracles representing truth assignments.

We will also show, using the idea of implicit proofs from [9, 10], how to define ordinary (i.e. non-relativized) total NP search problems $i\Gamma$ and show that these are complete among all NP search problems provably total in theory V_2^1 of Buss [3]. The reductions are definable in S_2^1. Another total NP search problems with this property have been defined earlier by Kolodziejczyk, Nguyen and Thapen [6] and recently by Beckmann and Buss [2].

We shall conclude with remarks on how to modify the construction for some other proof systems and how to use it to define random unsatisfiable formulas, and we formulate two open problems.

The reader is assumed to have knowledge of standard results in proof complexity, such as can be found in [8]. Only Section 3 presupposes knowledge of specific material from [9, 10]; we explain there the underlying ideas and give precise references but we shall not repeat that material here.

1 Formalization: sets $\Gamma(n,s,k)$

We shall first augment R a bit to make it technically more convenient. First, we shall allow also constant 1 in clauses and allow as new initial clauses all C containing 1 (we shall call these new initial clauses *1-axioms*). We also allow that both a variable and its negation occur in a clause. Second, we add *the weakening rule*:

$$\frac{C}{D}\ ,\quad \text{if}\ \ C \subseteq D\ .$$

Denote this augmented resolution system R^w. The reason for the modifications is that one can substitute constants for variables in an R^w-proof and it remains an R^w-proof (delete all literals evaluated to 0 and replace resolution inferences on variables substituted for by weakenings). An additional reason for the weakening rule is that otherwise it is a bit cumbersome to talk about a derivation of D from $C \subseteq D$: as R is a refutation system one has to talk instead of refuting the set of clauses

$$\{C\} \cup \{\{\ell^0\} \mid \ell \in D\}$$

and such derivations is even more cumbersome to concatenate (recall from the introduction that $\ell^0 := \neg\ell$).

Fix $n \geq 0$ and $s,k \geq 1$. Formula $\Gamma(n,s,k)$ talks about a potential k-step R^w-refutation of $\mathrm{Def}_C^{n,s}$ for an unspecified C (it is coded by atoms of $\Gamma(n,s,k)$). There are $\mathbf{q}$ and $\mathbf{p}$ variables; the former describe a sequence of clauses in a refutation and the latter encode the inference structure of the refutation. For the purpose of the following discussion call the steps in the refutation $D_1,\ldots,D_k$.

Clauses D_i may contain constant 1 or literals corresponding to $\mathbf{x},\mathbf{y}$ variables, i.e. all together up to $1+2(n+s)$ different objects. Formula $\Gamma(n,s,k)$ will thus use

- atoms q_i^u with $u=1,\ldots,k$ and $i \in \{-(n+s),\ldots,-1,0,1,\ldots,(n+s)\}$

The intended meaning of these is:

- $q_0^u = 1$ iff $1 \in D_u$,
- $q_i^u = 1$ for $i=1,\ldots,n$ iff $x_i \in D^u$, and for $i=-1,\ldots,-n$ iff $x_i^0 \in D^u$,
- $q_{n+j}^u = 1$ for $j=1,\ldots,s$ iff $y_j \in D^u$, and
  $q_{-n+j}^u = 1$ for $j=-1,\ldots,-s$ iff $y_j^0 \in D^u$.

We shall call these variables $\mathbf{q}$-variables and their set $\mathbf{q}$.

There will be also $\mathbf{p}$-variables $p_{u,v}$, $u=1,\ldots,k$ and $v=1,\ldots,t$ (we shall specify t in a moment). The intended meaning is that an assignment $\mathbf{a}^u \in \{0,1\}^t$ for $\mathbf{p}_u = p_{u,1},\ldots,p_{u,t}$ uniquely determines complete information about how D_u was inferred from earlier clauses and if $D_u \in \mathrm{Def}_C^{n,s}$ it also contains information assuring that $\mathrm{Def}_C^{n,s}$ clauses have the right form. To simplify the notation we shall assume that $k \geq 3s$ and $s > n$ and that the clauses of $\mathrm{Def}_C^{n,s}$ are listed as first $3s$ clauses $D_1, \ldots, D_{3s}$, with $D_{3r-2}, D_{3r-1}, D_{3r}$ defining the instruction for y_r (if the instruction needs only one or two clauses the other are dummy, say $\{1\}$).

There are at most $2 + n + (r-1) + 2(r-1)^2 \leq O(k^2)$ instructions how to compute y_r and $\mathbf{a}^u$ has to specify this uniquely for $u = 1, \ldots, 3s$. For $u = 3s+1, \ldots, k$ we need $\mathbf{a}^u$ to specify by which rule and from which earlier clauses was D_u inferred: there are at most $2 + (u-1) + (2+n+s)(u-1)^2 \leq k^3$ possibilities. Thus if we pick $t := 3 \log k$, $\{0,1\}^t$ has enough room to encode by its elements all possible situations.

It will be convenient to describe the clauses forming $\Gamma(n, s, k)$ as sequents

$$\ell_1, \ldots, \ell_e \ \rightarrow \ \ell_{e+1}, \ldots, \ell_f$$

representing the clause

$$\ell_1^0, \ldots, \ell_e^0, \ell_{e+1}, \ldots, \ell_f \ .$$

For $\mathbf{a} \in \{0,1\}^t$ let $\mathbf{p}_u(\mathbf{a})$ be the set of literals

$$(p_{u,1})^{a_1}, \ldots, (p_{u,t})^{a_t} \ .$$

That is, $\mathbf{a}$ is the unique truth assignment satisfying the conjunction of literals in $\mathbf{p}_u(\mathbf{a})$.

The set $\Gamma(n, s, k)$ consists of the following clauses divided into five groups:

γ1. For $u \in \{3r-2, 3r-1, 3r\}$ for $r = 1, \ldots, s$, if $\mathbf{a} \in \{0,1\}^t$ does not specify a valid instruction for computing y_r then $\Gamma(n, s, k)$ contains clause

$$\mathbf{p}_u(\mathbf{a}) \rightarrow \ .$$

γ2. For $u \in \{3r-2, 3r-1, 3r\}$ for $r = 1, \ldots, s$, if $\mathbf{a} \in \{0,1\}^t$ does specify a valid instruction for computing y_r then we know about constant 1 and about every **x**- and **y**-variable whether or not it occurs in D_u and whether or not this occurrence is positive or negative. Hence we include in $\Gamma(n, s, k)$ for every **q**-variable q_i^u exactly one of the clauses

$$\mathbf{p}_u(\mathbf{a}) \rightarrow q_i^u \ \text{ or } \ \mathbf{p}_u(\mathbf{a}) \rightarrow \neg q_i^u$$

as specified by $\mathbf{a}$.

γ3. For $u = 3s+1, \ldots, k$, if $\mathbf{a} \in \{0,1\}^t$ does not specify a valid inference for D_u, $\Gamma(n, s, k)$ contains clause

$$\mathbf{p}_u(\mathbf{a}) \rightarrow \ .$$

γ4. For $u = 3s+1, \ldots, k$, if $\mathbf{a} \in \{0,1\}^t$ does specify a valid inference for D_u, three cases can happen:

(a) D_u was inferred from D_v, D_w resolving literal ℓ, where $\ell \in D_v$ and $\ell^0 \in D_w$, and ℓ an **x**- or an **y**-literal.

Let $i \in \{(-(n+s), \dots, -1, 1, \dots, (n+s)\}$ correspond to ℓ and $-i$ to ℓ^0. Then $\Gamma(n,s,k)$ contains clauses:

$$\mathbf{p}_u(\mathbf{a}) \to q_i^v \qquad \mathbf{p}_u(\mathbf{a}) \to q_{-i}^w \qquad \mathbf{p}_u(\mathbf{a}) \to \neg q_i^u \qquad \mathbf{p}_u(\mathbf{a}) \to \neg q_{-i}^u$$

(these clauses enforce that ℓ and ℓ^0 appear in D_u, D_v, D_w as prescribed by the resolution rule),

and for $j \neq i, -i$, $j \in \{(-(n+s), \dots, -1, 1, \dots, (n+s)\}$ $\Gamma(n,s,k)$ contains further clauses

$$\mathbf{p}_u(\mathbf{a}), q_j^v \to q_j^u \qquad \mathbf{p}_u(\mathbf{a}), q_j^w \to q_j^u \qquad \mathbf{p}_u(\mathbf{a}), q_j^u \to q_j^v, q_j^w$$

(these clauses enforce that other literals are passed from D_v, D_w to D_u and that no other are).

(b) D_u was inferred by weakening from D_v, $v < u$. Then $\Gamma(n,s,k)$ contains all clauses

$$\mathbf{p}_u(\mathbf{a}), q_i^v \to q_i^u \ .$$

(c) D_u was inferred as a 1-axiom. Then $\Gamma(n,s,k)$ contains clause:

$$\mathbf{p}_u(\mathbf{a}) \to q_0^u \ .$$

γ5. Finally we add to $\Gamma(n,s,k)$ clauses

$$\to \neg q_i^k$$

for all i, enforcing that $D_k = \emptyset$.

Let us summarize.

Lemma 1.1 *For all $n \geq 0$, $s > n$, $k \geq 3s$ the set $\Gamma(n,s,k)$ contains $O(k^5)$ clauses of width at most $3 + 3\log k$ and it is not satisfiable.*

2 Reductions

Reflection principles for a proof system Q imply, over an arbitrary fixed base proof system satisfying a few technical properties, all Q-provable formulas and only with a polynomial slow-down over Q. This means that if φ has a Q-proof of size m then φ can be derived in the base system from a substitution instance of a reflection principle for Q by a proof of size at most $m^{O(1)}$. The reader can find all details in [8, Sec.9.3] but these details are not needed for the arguments below (although they may help in understanding what is going on).

The set $\Gamma(n,s,k)$ expresses conditions an R^w-refutation of some set $\mathrm{Def}_C^{n,s}$ would have to satisfy and hence it is the formulas $\neg \bigwedge \Gamma(n,s,k)$ which correspond to reflection principles for ER. An ER-refutation of a set Δ of clauses amounts to proving the formula $\neg \bigwedge \Delta$. Thus we want derivations (in some base system, here it will be R^w) of $\neg \bigwedge \Delta$ from an instance of $\neg \bigwedge \Gamma(n, s, k)$. In the framework of refutation systems this means that we look for derivations from Δ of all clauses of a substitution instance of $\Gamma(n, s, k)$. In fact, it will be enough to consider $\Gamma(0, s, k)$.

A map σ assigning to variables from a set Y constants $0, 1$ or disjunctions of literals corresponding to a set of variables X will be called *a clause substitution* and the maximal size of a disjunction σ assigns is *the width* of σ.

Let Γ, Δ be two sets of clauses in disjoint sets of variables Y and X, respectively (to avoid any confusion when dealing with substitutions). We say that a clause substitution σ is a *clause reduction* of Δ to Γ iff σ substitutes for Y-variables clauses of X-literals such that for each clause $D \in \Gamma$ one of the following cases occurs:

(a) $\sigma(D)$ is a 1-axiom,

(b) $\sigma(D)$ has the form:
$$\Pi, \bigvee E \to \bigvee F, \Sigma \tag{1}$$
where $E \subseteq F$ are sets of literals.

(c) $\sigma(D)$ contains as a subset a clause from Δ,

Note that in cases (a) and (b) $\sigma(D)$ is logically valid, and if $\sigma(D)$ is written in the sequent form then being a 1-axiom may also mean that $\neg 1$ is in its antecedent.

For the construction in the proof of the next theorem it will be handy to use the following notation. For z a variable and $\mathbf{a}, \mathbf{b} \in \{0, 1\}^t$ put
$$sel(z, \mathbf{a}, \mathbf{b})$$
to be the t-tuple from $\{0, 1, z, \neg z\}^t$ whose i-th coordinate is
$$sel(z, a_i, b_i) := (a_i \wedge z) \vee (b_i \wedge \neg z) \vee (a_i \wedge b_i)\ .$$
That is, $sel(z, a_i, b_i)$ is a constant or a literal defined by the following cases:
$$sel(z, a_i, b_i) := \begin{cases} 0 & \text{if } a_i = b_i = 0 \\ 1 & \text{if } a_i = b_i = 1 \\ z & \text{if } a_i = 1 \wedge b_i = 0 \\ \neg z & \text{if } a_i = 0 \wedge b_i = 1. \end{cases}$$

Theorem 2.1 *Assume Δ is a set of clauses of width $\leq w$ in n variables that has an ER-refutation π with $k(\pi)$ clauses.*

Then for some $k = O(nk((\pi))$ and $s \leq k/3$ there is a clause reduction σ of Δ to $\Gamma(0, s, k)$ and σ has the width at most $\max(w, 3)$.

Proof :

Assume $\mathbf{x}$ are the n variables of Δ. Introducing up to $O(nk(\pi))$ new extensions variables we may assume the width of π is at most $\max(w, 3)$. Let $\mathbf{y}$ be

s extensions atoms used in π. We may further rearrange the resulting proof so that the clauses defining the $\mathbf{y}$ variables are precisely the first $3s$ clauses and are followed by all $|\Delta|$ clauses from Δ. Let $k = O(nk(\pi))$ be the number of steps in the resulting ER-refutation and call these steps D_u.

Take the set $\Gamma(0, s, k)$. Our aim is to define a clause substitution σ such that every clause of $\sigma(\Gamma(0, s, k))$ is logically true or can be derived by a weakening from a clause of Δ. In fact, all clauses D of $\Gamma(0, s, k)$ will yield logically valid $\sigma(D)$ falling under items (a) and (b) of the definition of clauses reductions except possibly when D is from group $\gamma 4(c)$: if $\sigma(D)$ will not be a 1-axiom then it will follow by a weakening from a clauses of Δ.

Define the substitution σ for the $\mathbf{p}$- and $\mathbf{q}$-variables of $\Gamma(0, s, k)$ as follows:

1. For all $\mathbf{q}$-variables q_i^u with $i \neq 0$ substitute 0 or 1, depending on whether the $\mathbf{y}$-literal corresponding to i occurs in D_u.

2. For all variables q_0^u substitute $\bigvee E_u$, where E_u is the set of $\mathbf{x}$-literals occurring in D_u together with 1, if $1 \in D_u$. (Note that $|E_u| \leq w$.)

3. For $\mathbf{p}$-variables $\mathbf{p}_u$ with $u = 3r-2, 3r-1, 3r$ and $r \leq s$ define σ as follows:

   (a) If D_u is one of the three clauses corresponding to an instruction of the form $y_r := x_j$, put
   $$\sigma(\mathbf{p}_u) \ := \ sel(x_j, \mathbf{a}, \mathbf{b})$$
   where $\mathbf{a}$ and $\mathbf{b} \in \{0,1\}^t$ define the instructions $y_r := 1$ and $y_r := 0$, respectively.

   (b) Otherwise substitute for $\mathbf{p}_u$ the string $\mathbf{a}^u \in \{0,1\}^t$ defining the particular instruction of $\mathrm{Def}_C^{n,s}$ in π.

4. For $\mathbf{p}_u$ variables with $u = 3s+1, \ldots, 3s+|\Delta|$ substitute $\mathbf{a} \in \{0,1\}^t$ defining the clause D_u as being a 1-axiom.

5. For $u = 3s + |\Delta| + 1, \ldots, k$ consider several cases what to substitute for $\mathbf{p}_u$:

   (a) D_u was inferred as a 1-axiom: substitute for $\mathbf{p}_u$ as in item 4.

   (b) D_u was derived in π by weakening from D_v: substitute for $\mathbf{p}_u$ the $\mathbf{a}$ specifying this information.

   (c) D_u was derived by resolution from D_e, D_f resolving variable y_i: substitute for $\mathbf{p}_u$ the $\mathbf{a}$ specifying this information.

   (d) As in (c) but the resolved variable was x_i. Assume $x_i \in D_e$ and $\neg x_i \in D_f$. Substitute for $\mathbf{p}_u$ the expression
   $$sel(x_i, \mathbf{a}, \mathbf{b})$$
   where $\mathbf{a}, \mathbf{b} \in \{0,1\}^t$ specify that D_u was derived by the weakening from D_f or D_e, respectively.

We need to verify that for every clause $D \in \Gamma(0,s,k)$, $\sigma(D)$ falls under one of the three cases (a), (b) or (c) in the definition of reductions by clause-substitutions above. We shall treat the five groups $\gamma 1$ - $\gamma 5$ of clauses forming $\Gamma(0,s,k)$ separately.

If $D = \mathbf{p}_u(\mathbf{a}) \rightarrow$ belongs to groups $\gamma 1$ or $\gamma 3$, $\sigma(\mathbf{p}_u(\mathbf{a}))$ contains a false literal and so $\sigma(D)$ is a 1-axiom.

If D is from group $\gamma 2$, then $\sigma(D)$ is clearly a 1-axiom by the definition of $\sigma(q_i^u)$ for all instructions for y_r falling under 3(b) above, i.e. except when it has the form $y_r := x_j$. In the latter case the instruction is represented by clauses

$$\{y_r, \neg x_j\}\ ,\quad \{\neg y_r, x_j\}\ ,\quad \{1\}$$

and D is one of them. The definition of σ in 3(a) above using selection term on x_j yields $\sigma(D)$ which either contains 0 in the antecedent (and hence $\sigma(D)$ is a 1-axiom) or one of the literals x_j, x_j^0 occurs in both antecedent and succedent of $\sigma(D)$ and hence it falls under the case (b) of the definition of reductions.

If D is from group $\gamma 4$(a) then by item 5(c) of the definition of σ, $\sigma(D)$ becomes a 1-axiom. If D is from group $\gamma 4$(b) then $\sigma(D)$ falls under the case (b) of the definition of reductions: in particular, for $i = 0$, $\sigma(q_i^v)$ is contained in $\sigma(q_i^u)$ (the E and F in that definition). If D is from group $\gamma 4$(c) of $\Gamma(0,s,k)$ then $\sigma(D)$ is either a 1-axiom as $\sigma(q_0^u)$ contains constant 1 if D_u was a 1-axiom, or it falls under the case (c) of the definition of reductions as $\sigma(q_0^u)$ is $D_u \in \Delta$ (item 4 of the definition of σ).

Finally, D from group $\gamma 5$ of $\Gamma(0,s,k)$ is trivially turned by σ to a 1-axiom.

q.e.d.

We may interpret Theorem 2.1 as a proof-theoretic reduction: each clause of $\sigma(\Gamma(0,s,k))$ can be derived from Δ very easily in any proof system P simulating efficiently the weakening rule and deriving quickly all 1-axioms and all formulas as in (1) and hence the task to refute Δ is in P reduced to the task to refute $\Gamma(0,s,k)$. One can easily list various suitable weak P (e.g. tree-like $R^*(\log)$ or talk about R^w-derivations of F, Π from all Σ, ℓ, $\ell \in E$, in (1)) but it seems redundant to do so.

Alternatively, we may interpret the theorem as a reduction between relativized total NP search problems (see e.g. [1] for definitions). That is, given an ER-refutation π of Δ in n variables $\mathbf{x}$ with $k(\pi)$ steps, we have $\Gamma(0,s,k)$ for specific s,k bounded by $O(nk(\pi))$ such that it holds:

- *For any assignment α to variables $\mathbf{x}$ of Δ (α is the oracle), if we know a clause of $\Gamma(0,s,k)$ false under the assignment $\alpha \circ \sigma$ to its variables, we also know a clause of Δ false under α: $\alpha \circ \sigma(D)$ can only fail if it falls under item 2 of the definition of reductions and hence it contains a clause of Δ false under α.*

Note that, for a fixed π and $\Gamma(0,s,k)$ with parameters determined by it, computing σ requires at most w calls to α. Hence if w is a constant or at least bounded by $\log(n|\Delta|)$ the reduction is polynomial time in the sense of [1].

It is well-known (see e.g. [8, 6]) that propositional translations of a second order $\forall\Sigma_1^b(\alpha)$-formula (expressing the totality of a relativized NP search problem) that is provable in bounded arithmetic theory V_1^1 of Buss [3] have polynomial size Extended Frege proofs, i.e. in the refutation set-up the corresponding sets of clauses have polynomial size ER-refutations. This is [8, Thm.9.1.5], building on earlier results of Cook [4] and Buss [3].

Theorem 2.1 thus yields the following statement (the definability of the reduction in V_1^0 follows from its explicit nature).

Corollary 2.2 *Assume that a relativized NP search problem is provably total in bounded arithmetic theory V_1^1.*

Then the problem polynomially reduces $\Gamma(0, s, k)$ and the reduction is definable in V_1^0.

3 Total NP search problems $i\Gamma$

Following Papadimitriou [12] we shall consider total (non-relativized) NP search problems given as follows. Let $D(\mathbf{v}^1, \ldots, \mathbf{v}^t)$ be a circuit with tm inputs divided into t blocks of size m. Such D defines a t-ary relation on $\{0,1\}^m$; as a structure it may be exponentially large relative to the size of D. The general form of search tasks we shall consider is: Given pair $(1^{(m)}, D)$, find a subset $W \subseteq \{0,1\}^m$ of some specific polynomial size $m^{O(1)}$ such that the induced substructure contains a specific configuration known to exists by a general combinatorial or geometric statement. [10] gives several examples but perhaps the most interesting is when $t = 2$ and we think of D as defining an undirected graph without loops and W either contains a list of $m/2$ vertices from $\{0,1\}^m$ inducing a homogeneous subgraphs or one or two vertices certifying that D has a loop or is non-symmetric. Ramsey's theorem $2^m \to (m/2)_2^2$ guarantees the existence of such a W.

We shall use the idea of implicit proofs from [9], proofs of exponential size described bit-by-bit by a circuit and accompanied by a certificate that the circuit indeed defines a proof. In particular, a refutation of a formula ϕ in *implicit ER* proof system, denoted iER, is a pair (ρ, D) such that:

- $D(u, v)$ is a circuit with two inputs strings $u, v \in \{0,1\}^m$ defining a $2^m \times 2^m$ 0-1 array which we interpret as describing an ER-refutation of ϕ in the same sense as truth assignments to **p**- and **q**-variable of $\Gamma(0, s, k)$ talk about a potential ER-refutation,

- ρ is an ER-proof of the propositional formula formalizing the statement:

  – *D defines a valid ER-refutation of ϕ.*

The reader is invited to consult [9] for details of the definition.

The way how we shall use iER was first employed (and justified) in [10, Thm.5.4]. The idea is simple: we may allow D above to describe not only refutations of polynomial size formulas (as it was defined in [9]) but of exponential size formulas given themselves by small circuits.

In particular, if $(\exists y, |y| \leq |x|^c)\varphi(x,y)$ is a Σ^b_1-formula with $\varphi \in \Sigma^b_0$, then the sentence $(\forall x, |x| = n)(\exists y, |y| \leq |x|^c)\varphi(x,y)$ is true iff the set

$$\neg\varphi(x,w)\ ,\ \text{all } w \text{ such that } \ |w| \leq n^c \tag{2}$$

is not satisfiable by any $x \in \{0,1\}^n$, and hence it is refutable (in ER, in particular). The set (2) has exponential size but it can be easily generated by a size $n^{O(c)}$ circuit from w's. We use these ideas as follows.

The $i\Gamma(m)$ **NP search problem**, the instance of $i\Gamma$ for parameter m, is defined as follows:

1. The input is pair $(1^{(m)}, D)$ with $D(x,y)$ a size m^2 circuit with $2\cdot m$ inputs.
2. Interpret D as defining an evaluation of the $\mathbf{p}$ and $\mathbf{q}$-variables of $\Gamma(0,s,k)$ where $k = 2^m$ and $s = k^{1/2}$.

   [There are $2s+1$ variables q^u_i and $3\log k = 3m$ variables in $\mathbf{p}_u$, all $u \leq k = 2^m$, so D has enough input bits to define a $0-1$ array of bits evaluating all the variables.]
3. Output: find a clause of $\Gamma(0,s,k)$ false under the evaluation.

   [There are $O(k^5) = O(2^{5m})$ of possible outcomes so the output is $\leq 5m$ bits.]

The parameters are fixed at $|D| = m^2$ and $s = 2^{m/2}$ in order to reduce the number of parameters in the problem. Modifying m linearly allows to accommodate arbitrary polynomial relations among k, s and $\log k, |D|$.

We state and prove the next theorem using the ideas and referring to facts about the concepts described above; all details for these facts can be found in [9, 10] at the specifically cited places.

Theorem 3.1 *Assume an NP search problem is provably total in theory V^1_2. Then the problem can be polynomially reduced to $i\Gamma$. The reduction is definable in S^1_2.*

Moreover, $i\Gamma$ is itself provably total in V^1_2.

Proof :
Let $(\exists y, |y| \leq |x|^c)\varphi(x,y)$ be a Σ^b_1-formula with $\varphi \in \Sigma^b_0$ such that V^1_2 proves

$$\forall x(\exists y, |y| \leq |x|^c)\varphi(x,y)\ .$$

In particular, $|y| \leq |x|^c \wedge \varphi(x,y)$ defines a total NP search problem.

By the construction underlying [9, Thm.2.1], as shown in the proof of [10, Thm.5.4], there exists an iER refutation (ρ, B) of formulas from (2) above expressed as a set of $2^{O(n^c)}$ clauses of width $\leq w = n^{O(c)}$ such that:

- $B(i,j)$ is a size $n^{O(c)}$ circuit with $2 \cdot n^{O(c)}$ inputs describing an ER-refutation π of (2),

- circuit B is definable in S^1_2 from $1^{(n)}$ and S^1_2 proves that B defines an ER-refutation of the set (2) (ρ plays a role in this).

Use π for the definition of a clause-substitution σ as in the proof of Theorem 2.1 but whenever we need a bit of π we compute it by circuit B. The substitution has width $\leq w = n^{O(c)}$ and so the reduction so obtained is a polynomial reduction of the search problem $(\exists y, |y| \leq |x|^c)\varphi(x,y)$ for x of length $|x| = n$.

The second statement follows as V^1_2 proves the soundness iEF (= iER) proofs, cf. [9, Thm.2.1].

q.e.d.

One can generalize this construction to stronger theories as follows. In [9] we used the characterization from [7] of bounded first-order consequences of V^1_2 as those of formal system $S^1_2 + 1\text{-Exp}$: $\delta(x)$ is provable in this system iff S^1_2 proves

$$t(x) \leq |y| \rightarrow \delta(x)$$

for some term $t(x)$. The intuition is that while ER corresponds to S^1_2, iER corresponds to adding 1-Exp and that corresponds to extending first-order S^1_2 to second-order V^1_2. The construction in [9, 10] works also for $S^1_2 + 2\text{-Exp}$ (and third-order extension of S^1_2) and i(iER), and higher iterates, as pointed out in [9, Sec.4]. In general, if a theory T corresponds to a proof system P then iP corresponds to T + 1-Exp and one may try to define NP search problems analogous to $i\Gamma$ where B is assumed to describe a P-refutation. It is a challenge to describe this construction in a direct, combinatorially transparent, way.

4 Concluding remarks

One can restrict circuits C that can be used in $\mathrm{Def}^{n,s}_C$ to a class of circuits and it is clear from the construction that taking for these classes NC^1, AC^0 or $AC^0(2)$ yield statements analogous to Theorem 2.1 for Frege system and constant depth Frege system in the DeMorgan language, and constant depth Frege systems in DeMorgan language augmented by the parity connective, respectively. Similarly, Corollary 2.2 and Theorem 3.1 can be analogously derived for theories corresponding to those proof systems, cf. [8, 5].

For a given $s \geq 1$ and $k \geq 3s$ we can define the following random process yielding a set of clauses ($\mathbf{r}$ are the random bits used):

(i) Pick s instructions for computing variables $\mathbf{y}$ defining a circuit $C_{\mathbf{r}}$ without variables: the instruction for y_i is picked uniformly at random from all legal instructions for y_i,

(ii) substitute in $\Gamma(0,s,k)$ for all variables $\mathbf{p}_u$ and q^u_i with $u \leq 3s$ the bits defining clauses of $\mathrm{Def}^{0,s}_C$ corresponding to $C_{\mathbf{r}}$ chosen in step (i).

Let us denote the random set of clauses so constructed by $\Gamma(0,s,k)(C_{\mathbf{r}})$; it is always unsatisfiable. The following seem to be interesting open problems:

Q1 Is it true that with a high probability over $\mathbf{r}$ the set $\Gamma(0, s, k)(C_{\mathbf{r}})$ requires long refutations in any proof system not simulating ER?

Q2 Is it true that $\Gamma(0, s, k)$ can be reduced by a clause-substitution to a problem $\Gamma(0, s', k')(C)$ for some k' polynomially bounded in k and some *specific* size s' circuit C?

If the first question had an affirmative answer the sets $\Gamma(0, s, k)(C_{\mathbf{r}})$ would provide an easy to compute source of hard formulas that are always unsatisfiable (other proposed constructions yield sets unsatisfiable with a high probability but not always).

Acknowledgements:

The constructions described in this paper were developed as a part of an investigation into model-theoretic constructions described in [11]. It was after discussions with S. Buss in July 2015 about his current work [2] with A. Beckmann that I realized that the constructions could be of an independent interest. I also thank S. Buss for comments on the draft of this paper and to N. Thapen for discussions about the topic.

References

[1] P. Beame, S. A. Cook, J. Edmonds, R. Impagliazzo and T. Pitassi, The Relative Complexity of NP Search Problems, J. Computer Systems Sciences **57**, (1998), pp.3-19.

[2] A. Beckmann and S. R. Buss, The NP Search Problems of Frege and Extended Frege Proofs, preprint, (2016).

[3] S. R. Buss, *Bounded Arithmetic*. Naples, Bibliopolis, (1986).

[4] S. A. Cook, Feasibly constructive proofs and the propositional calculus, in: *Proc. 7^{th} Annual ACM Symp. on Theory of Computing*, (1975), pp. 83-97. ACM Press.

[5] S. A. Cook and P. Nguyen, *Logical foundations of proof complexity*, (ASL Perspectives in Logic Series, Cambridge University Press, (2014).

[6] L. Kolodziejczyk, P. Nguyen and N. Thapen, The provably total NP search problems of weak second order bounded arithmetic, *Annals of Pure and Applied Logic*, **162:6**, (2011), pp.419-446.

[7] J. Krajíček, Exponentiation and second-order bounded arithmetic, *Annals of Pure and Applied Logic*, **48(3)**, (1990), pp.261-276.

[8] J. Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press, (1995).

[9] J. Krajíček, Implicit proofs, *J. of Symbolic Logic*, **69(2)**, (2004), pp.387-397.

[10] J. Krajíček, Structured pigeonhole principle, search problems and hard tautologies, *J. of Symbolic Logic*, **70(2)**, (2005), pp.619-630.

[11] J. Krajíček, *Forcing with random variables and proof complexity*, London Mathematical Society Lecture Note Series, No.382, Cambridge University Press, (2011).

[12] C. H. Papadimitriou, On the complexity of the parity argument and other inefficient proofs of existence, *J.Computer and Systems Science*, **48(3)**, (1994), pp.498-532.

[13] G. S. Tseitin, On the complexity of derivations in propositional calculus, in: *Studies in mathematics and mathematical logic*, Part II (A. 0. Slisenko, editor), (1968), pp.115-125.

Mailing address:
Department of Algebra
Faculty of Mathematics and Physics
Charles University
Sokolovská 83, Prague 8, CZ - 186 75
The Czech Republic
krajicek@karlin.mff.cuni.cz