VC-DIMENSIONS OF SHORT PRESBURGER FORMULAS

DANNY NGUYEN, IGOR PAK

Received June 5, 2018
Online First March 13, 2019

We study VC-dimensions of short formulas in Presburger Arithmetic, defined to have a bounded number of variables, quantifiers and atoms. We give both lower and upper bounds, which are tight up to a polynomial factor in the bit length of the formula.

1. Introduction

The notion of VC-dimension was introduced by Vapnik and Červonenkis in [15]. Although originally motivated by applications in probability and statistics, it was quickly adapted to computer science, learning theory, combinatorics, logic and other areas. We refer to [16] for the extensive review of the subject, and to [3] for an accessible introduction to combinatorial and logical aspects.

1.1. Definitions of VC-dimension and VC-density

Let $X$ be a set and $S \subseteq 2^X$ be a family of subsets of $X$. For a subset $A \subseteq X$, let $S \cap A := \{ S \cap A : S \in S \}$ be the family of subsets of $A$ cut out by $S$. We say that $A \subseteq X$ is shattered by $S$ if $S \cap A = 2^A$, i.e., for every subset $B \subseteq A$, there is $S \in S$ with $B = S \cap A$. The largest size $|A|$ among all subsets $A \subseteq X$ shattered by $S$ is called the VC-dimension of $S$, denoted by VC($S$). If no such largest size $|A|$ exists, we write VC($S$) = $\infty$.

Mathematics Subject Classification (2010): 03C45, 52C07
The shatter function \( \pi_S \) is defined as follows:
\[
\pi_S(n) = \max \{|S \cap A| : A \subseteq X, |A| = n\}.
\]
The VC-density of \( S \), denoted by \( \text{vc}(S) \) is defined as
\[
\inf \left\{ r \in \mathbb{R}^+ : \limsup_{n \to \infty} \frac{\pi_S(n)}{n^r} < \infty \right\}.
\]
The classical theorem of Sauer and Shelah [11,12] states that
\[
\text{vc}(S) \leq \text{VC}(S).
\]
In other words, \( \pi_S(n) = O(n^d) \) in case \( S \) has finite VC-dimension \( d \). In general, VC-density can be much smaller than VC-dimension, and also behaves a lot better under various operations on \( S \).

1.2. NIP theories and bounds on VC-dimension/density

It is of interest to distinguish the first-order theories in which VC-dimension and VC-density behave nicely. Let \( \mathcal{L} \) be a first-order language and \( M \) be an \( \mathcal{L} \)-structure. Consider a partitioned \( \mathcal{L} \)-formula \( F(x; y) \) whose free variables are separated into two groups \( x \in M^m \) (objects) and \( y \in M^n \) (parameters). For each parameter tuple \( y \in M^n \), let
\[
S_y = \{ x \in M^m : M \models F(x; y) \}.
\]
Associated to \( F \) is the family \( S_F = \{ S_y : y \in M^n \} \). We say that \( F \) is NIP, short for “\( F \) does not have the independence property”, if \( S_F \) has finite VC-dimension. The structure \( M \) is called NIP if every partitioned \( \mathcal{L} \)-formula \( F \) is NIP in \( M \).

One prominent example of an NIP structure is Presburger Arithmetic \( \text{PA} = (\mathbb{Z}, <, +) \), which is the first-order structure on \( \mathbb{Z} \) with only addition and inequalities. The main result of this paper are the lower and upper bounds on the VC-dimensions of PA-formulas. These are contrasted with the following notable bounds on the VC-density:

**Theorem 1.1** ([1]). Given a PA-formula \( F(x; y) \) with \( y \in \mathbb{Z}^n \), \( \text{vc}(S_F) \leq n \) holds.

In other words, VC-density in the setting of PA can be bounded solely by the dimension of the parameter variables \( y \). It cannot grow very large when we vary the number of object variables \( x \), quantified variables or the description of \( F \). This follows from a more general result in [1], which says
that every quasi-o-minimal structure satisfies a similar bound on the VC-density. We refer to [1] for the precise statement of this result and for the powerful techniques used to bound the VC-density.

Karpinski and Macintyre raised a natural question whether similar bounds would hold for the VC-dimension. In [5], they gave upper bounds for the VC-dimension in some o-minimal structures (PA is not one), which are polynomial in the parameter dimension $n$. Later, they extended their arguments in [6] to obtain upper bounds on the VC-density, this time linear in $n$. Also in [6], the authors claimed to have an effective bound on the VC-dimensions of PA-formulas. However, we cannot locate such an explicit bound in any papers. To our knowledge, no effective upper bounds on the VC-dimensions of general PA-formulas exist in the literature.

1.3. Main results

We consider PA-formulas with a fixed number of variables (both quantified and free). Clearly, this also restricts the number of quantifier alternations in $F$. The atoms in $F$ are linear inequalities in these variables with some integer constants and coefficients (in binary). Given such a formula $F$, denote by $\ell(F)$ the length of $F$, i.e., the total bit length of all symbols, operations, integer coefficients and constants in $F$.

We can further restrict the form of a PA-formula by requiring that it does not contain too many inequalities. For fixed $k$ and $t$, denote by Short-PA($k,t$) the family of PA-formulas with at most $k$ variables (both free and quantified) and $t$ inequalities. When $k$ and $t$ are clear, a formula $F \in$ Short-PA($k,t$) is simply called a short Presburger formula. In this case, $\ell(F)$ is essentially the total length of a bounded number of integer coefficients and constants. Our main result is a lower bound on the VC-dimensions of short Presburger formulas:

**Theorem 1.2.** For every $d$, there is a short Presburger formula $F(x; y) = \exists u \forall v \Psi(x, y, u, v)$ in the class Short-PA(10, 18) with

$$\ell(F) = O(d^2) \quad \text{and} \quad \text{VC}(F) \geq d.$$  

Here $x, y$ are singletons and $u \in \mathbb{Z}^6, v \in \mathbb{Z}^2$. The expression $\Psi$ is quantifier-free, and can be computed in probabilistic polynomial time in $d$.

So in contrast with VC-density, the VC-dimension of a PA-formula $F$ crucially depends on the actual length $\ell(F)$. For the formulas in the theorem, we have:

$$\text{VC}(F) = \Omega((\ell(F) \frac{1}{2}), \quad \text{and} \quad \text{vc}(F) \leq 1,$$
where the last inequality follows by Theorem 1.1. Note that if one is allowed
an unrestricted number of inequalities in $F$, a similar lower bound to Theo-
rem 1.2 can be easily established by an elementary combinatorial argument.
However, since the formula $F$ is short, we can only work with a few integer
coefficients and constants. t various decision problems with short Presburger
sentences are intractable.

The construction in Theorem 1.2 uses a number-theoretic technique that
employs continued fractions to encode a union of many arithmetic progres-
sions. This technique was explored earlier in [8] to show that various decision
problems with short Presburger sentences are intractable. In this construc-
tion we need to pick a prime roughly larger than $4^d$, which can be done in
probabilistic polynomial time in $d$. This can be modified to a deterministic
algorithm with run-time polynomial in $d$, at the cost of increasing $\ell(F)$:

**Theorem 1.3.** For every $d$, there is a short Presburger formula $F(x;y) =
\exists u \forall v \Psi(x,y,u,v)$ in the class Short-PA(10,18) with

$$\ell(F) = O(d^3) \quad \text{and} \quad \text{VC}(F) \geq d.$$  

Here $x,y$ are singletons and $u \in \mathbb{Z}^6$, $v \in \mathbb{Z}^2$. The expression $\Psi$
is quantifier-
free, and can be computed in deterministic polynomial time in $d$.

We conclude with the following polynomial upper bound for the VC-
dimensions of all (not necessarily short) Presburger formulas in a fixed num-
ber of variables:

**Theorem 1.4.** For a Presburger formula $F(x;y)$ with at most $k$
variables (both free and quantified), we have:

$$\text{VC}(F) = O(\ell(F)^c),$$

where $c$ and the $O(\cdot)$ constant depend only on $k$.

This upper bound implies that Theorem 1.2 is tight up to a polynomial
factor. The proof of Theorem 1.4 uses an algorithm from [7] for decomposing
a semilinear set, i.e., one defined by a PA-formula, into polynomially many
simpler pieces. Each such piece is a polyhedron intersecting a periodic set,
whose VC-dimension can be bounded by elementary arguments.

We note that the number of quantified variables is vital in Theorem 1.4.
In §3.3, we construct PA-formulas $F(x;y)$ with $x,y$ singletons and many
quantified variables, for which $\text{VC}(F)$ grows doubly exponentially compared
to $\ell(F)$.
2. Proofs

We start with Theorem 1.3, and then show how it can be modified to give Theorem 1.2.

**Proof of Theorem 1.3.** Let \( A = \{1, 2, \ldots, d\} \) and \( S = 2^A \). Since \( S \) contains all of the subsets of \( A \), we have \( \text{VC}(S) = d \). We order the sets in \( S \) lexicographically. In other words, for \( S, S' \in S \), we have \( S < S' \) if \( \sum_{i \in S} 2^i < \sum_{i \in S'} 2^i \). Thus, the sets in \( S \) can be indexed as 
\[
S_0 < S_1 < \cdots < S_{2^d-1},
\]
where \( S_0 = \emptyset, S_1 = \{1\}, \ldots, S_{2^d-1} = A \). Next, define:

\[
T := \bigsqcup_{0 \leq j < 2^d} \{i + dj : i \in S_j\}.
\]

We show in Lemma 2.1 below that the set \( T \) is definable by a short PA formula \( G_T(t) \) with only 8 quantified variables and 18 inequalities. Using this, it is clear that the parametrized formula 
\[
F_T(x; y) := G_T(x + dy)
\]
describes the family \( S \) (with \( y \) as the parameter), and thus has VC-dimension \( d \). We remark that \( G_T \) has only 1 quantifier alternation (see below).

**Lemma 2.1.** The set \( T \) is definable by a short Presburger formula \( G_T(t) = \exists u \forall v \Psi(t, u, v) \) with \( u \in \mathbb{Z}^6, v \in \mathbb{Z}^2 \) and \( \Psi \) a Boolean combination of at most 18 inequalities in \( t, u, v \) with binary length \( \ell(\Psi) = O(d^3) \).

**Proof.** Our strategy is to represent the set \( T \) as a union of arithmetic progressions (APs). In [8], given \( d \) progressions \( \text{AP}_i = \{a_i, a_i + c_i, \ldots, a_i + b_i c_i\} \), we gave a method to define \( \text{AP}_1 \cup \cdots \cup \text{AP}_d \) by a short Presburger formula of length polynomial in \( \sum \log(a_i b_i c_i) \). For each \( 1 \leq i \leq d \), let \( J_i = \{j : 0 \leq j < 2^d, i \in S_j\} \). From (2.1), we have:

\[
T = \bigsqcup_{i=1}^d \{i + dJ_i\}.
\]

From the lexicographic ordering of the sets \( S_j \), we can easily describe each set \( J_i \) as:

\[
J_i = \{m + 2^{i-1} + 2^j n : 0 \leq m < 2^{i-1}, 0 \leq n < 2^{d-i}\}.
\]

So each set \( J_i \) is not simply an AP, but the Minkowski sum of two APs. However, we can easily modify each \( J_i \) into an AP by defining:

\[
J'_i = \{2^d(m + 2^{i-1}) + 2^j n : 0 \leq m < 2^{i-1}, 0 \leq n < 2^{d-i}\}.
\]
It is clear that \( J'_i \) is an AP that starts at \( 2^{d+i-1} \) and ends at \( 2^{d+i} - 2^i \) with step size \( 2^i \). Let \( \text{AP}_i := i + dJ'_i \) and

\[
(2.5) \quad T' = \bigcup_{i=1}^{d} \text{AP}_i.
\]

This is a union of \( d \) arithmetic progressions. Using the construction from [8], we can define \( T' \) by a short Presburger formula:

\[
t' \in T' \iff \exists w \forall v \Phi(t', w, v),
\]

where \( t' \in \mathbb{Z}, \ w, v \in \mathbb{Z}^2 \) and \( \Phi \) is a Boolean combination of at most 10 inequalities. This construction works by finding a single continued fraction \( \alpha = [a_0; b_0, a_1, b_1, \ldots, a_{2d-1}] \) whose successive convergents encode the first and last points of our \( \text{AP}_1, \ldots, \text{AP}_d \). We refer to Section 4 in [8] for the details. For each \( i \), the smallest and largest terms in \( \text{AP}_i \) are respectively \( \beta_i = i + d2^{d+i-1} \) and \( \gamma_i = i + d(2^{d+i} - 2^i) \), which have binary lengths \( O(d) \). Each term \( a_k \) and \( b_k \) in the continued fraction \( \alpha \) is at most the product of these \( \beta_i \) and \( \gamma_i \). Since \( \prod_{i=1}^{d} \beta_i \gamma_i \) has binary length \( O(d^2) \), and so does each term \( a_k \) and \( b_k \). Therefore, the final continued fraction \( \alpha \) is a rational number \( p/q \) with binary length \( O(d^3) \). This implies that \( \ell(\Phi) = O(d^3) \) as well.

To get a formula for \( T \), note that from (2.2), (2.3), (2.4) and (2.5), we have:

\[
t \in T \iff \exists t', i, r, s: \ t' \in T', \ 1 \le i \le d, \ 0 \le s < 2^d, \ t' = i + d(2^d r + s), \ t = i + d(r + s).^1
\]

Here \( r \) and \( s \), respectively stand for \( m + 2^{i-1} \) and \( 2^i n \) in (2.3). Using \( \exists w \forall v \Phi(t', w, v) \) to express \( t' \in T' \), we get a formula \( G_T(t) \) defining \( T \) with 8 quantified variables \( t', i, r, s \in \mathbb{Z}, \ w, v \in \mathbb{Z}^2 \) and 18 inequalities. Note that \( t', i, r, s \) and \( w \) are existential variables, so \( G_T \) has the form \( \exists u \forall v \Psi(t, u, v) \) with \( u \in \mathbb{Z}^6, v \in \mathbb{Z}^2 \) and \( \Psi \) quantifier-free.

**Proof of Theorem 1.2.** Note that the above construction of \( F_T \) and \( G_T \) is deterministic with run-time polynomial in \( d \). In Theorem 1.2, only the existence of a short PA formula with high VC-dimension is needed. For this, our lower bound can be improved to \( \text{VC}(F) \ge c \sqrt{\ell(F)} \), for some \( c > 0 \), as follows. Recall that \( \beta_i = i + d2^{d+i-1} \) and \( \gamma_i = i + d(2^{d+i} - 2^i) \) are the smallest and largest terms of each \( \text{AP}_i \) in (2.5). Pick the smallest prime \( p \) larger than \( \max(\gamma_1, \ldots, \gamma_d) \approx d4^d \). This prime \( p \) can substitute for the large number \( M \)

---

^1 Each equality is a pair of inequalities.
in Section 4.1 of [8], which was (deterministically) chosen as $1 + \prod_{i=1}^{d} \beta_i \cdot \gamma_i$, so that it is larger and coprime to all $\beta_i$ and $\gamma_i$. The rest of the construction follows verbatim. Note that $\log p = O(d)$ by Chebyshev’s theorem. So the final continued fraction $\alpha = [a_0; b_0, a_1, b_1, \ldots, a_{2d-1}]$ has length $O(d^2)$, because now each term $a_k, b_k$ has length at most $\log p$. This completes the proof.

**Proof of Theorem 1.4.** Let $F(x; y)$ be any PA formula with free variables $x \in \mathbb{Z}^m$, $y \in \mathbb{Z}^n$ and $n'$ other quantified variables, where $m, n, n'$ are fixed. In [7] (Theorem 5.2), we gave the following polynomial decomposition on the semilinear set defined by $F$:

$$(2.6) \quad \Sigma_F := \{(x, y) \in \mathbb{Z}^{m+n} : F(x; y) = \text{true}\} = \bigsqcup_{j=1}^{r} R_j \cap T_j.$$ 

Here each $R_j$ is a polyhedron in $\mathbb{R}^{m+n}$, and each $T_j \subseteq \mathbb{Z}^{m+n}$ is a periodic set, i.e., a union of several cosets of some lattice $T_j \subseteq \mathbb{Z}^{m+n}$. In other words, the set defined by $F$ is a union of $r$ pieces, each of which is a polyhedron intersecting a periodic set. Our decomposition is algorithmic, in the sense that the pieces $R_j$ and lattices $T_j$ can be found in time $O(\ell(F)^c)$, with $c$ and $O(\cdot)$ depending only on $m, n, n'$. The algorithm describes each piece $R_j$ by a system of inequalities and each lattice $T_j$ by a basis. Denote by $\ell(R_j)$ and $\ell(T_j)$ the total binary lengths of these systems and basis vectors, respectively. These also satisfy:

$$(2.7) \quad \sum_{j=1}^{r} \ell(R_j) + \ell(T_j) = O(\ell(F)^c).$$

Each $R_j$ can be written as the intersection $H_{j1} \cap \cdots \cap H_{jf_j}$, where each $H_{jk}$ is a half-space in $\mathbb{R}^{m+n}$, and $f_j$ is the number of facets of $R_j$. Note that $f_j \leq \ell(R_j) = O(\ell(F)^c)$. We rewrite (2.6) as:

$$(2.8) \quad \Sigma_F = \bigsqcup_{j=1}^{r} H_{j1} \cap \cdots \cap H_{jf_j} \cap T_j.$$ 

Therefore, the set $\Sigma_F$ is a Boolean combination of $f_1 + \cdots + f_r$ half-spaces and $r$ periodic sets. In total, there are

$$(2.9) \quad f_1 + \cdots + f_r + r = O(\ell(F)^c)$$

of those basic sets.

For a set $\Gamma \subseteq \mathbb{R}^{m+n}$ and $y \in \mathbb{Z}^n$, denote by $\Gamma_y$ the subset $\{x \in \mathbb{Z}^m : (x, y) \in \Gamma\}$ and by $S_\Gamma$ the family $\{\Gamma_y : y \in \mathbb{Z}^n\}$. For a half-space $H \subset \mathbb{R}^{m+n}$, it is easy
to see that \( VC(S_H) = 1 \). For each periodic set \( T_j \) with period lattice \( T_j \), the family \( S_{T_j} \) has cardinality at most \( \det(T_j \cap \mathbb{Z}^n) \leq 2^{O(\ell(T_j))} \). Thus, we have

\[
VC(S_{T_j}) \leq \log |S_{T_j}| = O(\ell(T_j)).
\]

Let \( \Gamma_1, \ldots, \Gamma_t \subseteq \mathbb{Z}^{m+n} \) be any \( t \) sets with \( VC(S_{\Gamma_i}) = d_i \). By an application of the Sauer-Shelah lemma ([11,12]), if \( \Sigma \) is any Boolean combination of \( \Gamma_1, \ldots, \Gamma_t \), then we can bound \( VC(S_{\Sigma}) \) as:

\[
VC(S_{\Sigma}) = O((d_1 + \cdots + d_t) \log(d_1 + \cdots + d_t)).
\]

Applying this to (2.8), we get \( VC(S_{\Sigma_F}) = O(\ell \log \ell) \), where

\[
\ell = \sum_{j=1}^r \left( VC(S_{T_j}) + \sum_{j' = 1}^{f_j} VC(S_{H_{j,j'}}) \right) \leq \sum_{j=1}^r VC(S_{T_j}) + f_j.
\]

By (2.7), (2.9) and (2.10), we have \( \ell = O(\ell(F)^c) \). We conclude that \( VC(F) = O(\ell(F)^{2c}) \).

\[\square\]

3. Final remarks and open problems

3.1.

The proof of Theorem 1.2 is almost completely efficient except for finding a small prime \( p \) larger than a given integer \( N \). This problem is considered to be computationally very difficult in the deterministic case, and only exponential algorithms are known (see [9,14]).

3.2.

Our constructed short formula \( F \) is of the form \( \exists \forall \). It is interesting to see if similar polynomial lower bounds are obtainable with existential short formulas. For such a formula \( F(x;y) = \exists z \Phi(x,y,z) \), the quantifier-free expression \( \Phi(x,y,z) \) captures the set of integer points \( \Gamma \) lying in a union of some polyhedra \( P_i \)'s. Note that the total number of polyhedra and their facets should be bounded, since we are working with short formulas. Therefore, \( F \) simply capture the pairs \((x,y)\) in the projection of \( \Gamma \) along the \( z \) direction. Denote this set by \( \text{proj}(\Gamma) \). The work of Barvinok and Woods [2] shows that \( \text{proj}(\Gamma) \) has a short generating function, and can even be counted efficiently in polynomial time. In our construction, the set that yields high VC-dimension is a union arithmetic progressions, which cannot be counted efficiently unless \( P = \text{NP} \) (see [13]). This difference indicates that \( \text{proj}(\Gamma) \) has a much simpler combinatorial structure, and may not attain a high VC-dimension.
3.3.

One can ask about the VC-dimension of a general PA-formula with no restriction on the number of variables, quantifier alternations or atoms. Fischer and Rabin famously showed in [4] that PA has decision complexity at least doubly exponential in the general setting. For every $\ell > 0$, they constructed a formula $\text{Prod}_\ell(a, b, c)$ of length $O(\ell)$ so that for every triple 

$$0 \leq a, b, c < 2^{2^{2\ell}},$$

we have $\text{Prod}_\ell(a, b, c) = \text{true}$ if and only if $ab = c$. Using this “partial multiplication” relation, one can easily construct a formula $F_\ell(x; y)$ of length $O(\ell)$ and VC-dimension at least $2^{2^\ell}$. This can be done by constructing a set similar to $T$ in (2.1) with $d$ replaced by $2^{2^\ell}$ using $\text{Prod}_\ell$. We leave the details to the reader.

Regarding upper bound, Oppen showed in [10] that any PA-formula $F$ of length $\ell$ is equivalent to a quantifier-free formula $G$ of length $2^{2^{2\ell}}$ for some universal constant $c > 0$. This implies that $\text{VC}(G)$, and thus $\text{VC}(F)$, is at most triply exponential in $\ell(F)$. We conjecture that a doubly exponential upper bound on $\text{VC}(F)$ holds in the general setting. It is unlikely that such an upper bound could be established by straightforward quantifier elimination, which generally results in triply exponential blow up (see [17, Thm 3.1]).

Acknowledgements. We are grateful to Matthias Aschenbrenner and Artém Chernikov for many interesting conversations and helpful remarks. This paper was finished while both authors were visitors at MSRI; we are thankful for the hospitality, great work environment and its busy schedule. The second author was partially supported by the NSF.

References

[1] M. Aschenbrenner, A. Dolich, D. Haskell, D. Macpherson and S. Starchenko: Vapnik-Chervonenkis density in some theories without the independence property, I, Trans. AMS 368 (2016), 5889–5949.
[2] A. Barvinok and K. Woods: Short rational generating functions for lattice point problems, Jour. AMS 16 (2003), 957–979.
[3] A. Chernikov: Models theory and combinatorics, course notes, UCLA; available electronically at https://tinyurl.com/y8ob6uyv.
[4] M. J. Fischer and M. O. Rabin: Super-Exponential Complexity of Presburger Arithmetic, in: Proc. SIAM-AMS Symposium in Applied Mathematics, AMS, Providence, RI, 1974, 27–41.
[5] M. Karpinski and A. Macintyre: Polynomial bounds for VC dimension of sigmoidal and general Pfaffian neural networks, *J. Comput. System Sci.* 54 (1997), 169–176.

[6] M. Karpinski and A. Macintyre: Approximating volumes and integrals in o-minimal and p-minimal theories, in: *Connections between model theory and algebraic and analytic geometry*, Seconda Univ. Napoli, Caserta, 2000, 149–177.

[7] D. Nguyen and I. Pak: Enumeration of integer points in projections of unbounded polyhedra, *SIAM J. Discrete Math.* 32 (2018), 986–1002.

[8] D. Nguyen and I. Pak: Short Presburger Arithmetic is hard, in: *Proc. 58th FOCS*, IEEE, Los Alamitos, CA, 2017, 37–48.

[9] J. C. Lagarias and A. M. Odlyzko: Computing $\pi(x)$: an analytic method, *J. Algorithms* 8 (1987), 173–191.

[10] D. C. Oppen: A $2^{2^{2^n}}$ upper bound on the complexity of Presburger arithmetic, *J. Comput. System Sci.* 16 (1978), 323–332.

[11] N. Sauer: On the density of families of sets, *J. Combin. Theory, Ser. A* 13 (1972), 145–147.

[12] S. Shelah: A combinatorial problem; stability and order for models and theories in infinitary languages, *Pacific J. Math.* 41 (1972), 247–261.

[13] L. J. Stockmeyer and A. R. Meyer: Word problems requiring exponential time: preliminary report, in: *Proc. Fifth STOC*, ACM, New York, 1973, 1–9.

[14] T. Tao, E. Croot and H. Helfgott: Deterministic methods to find primes, *Math. Comp.* 81 (2012), 1233–1246.

[15] V. N. Vapnik and A. Ja. Červonenkis: The uniform convergence of frequencies of the appearance of events to their probabilite, *Theor. Probability Appl.* 16 (1971), 264–280.

[16] V. N. Vapnik: *Statistical learning theory*, John Wiley, New York, 1998.

[17] V. D. Weispfenning: Complexity and uniformity of elimination in Presburger arithmetic, in: *Proc. 1997 ISSAC*, ACM, New York, 1997, 48–53.

Danny Nguyen

*Department of Mathematics*

*University of Michigan*

*Ann Arbor, MI 48109*

*ndanny@umich.edu*

Igor Pak

*Department of Mathematics*

*UCLA, Los Angeles, CA 90095*

*pak@math.ucla.edu*