On the Structure of Valiant's Complexity Classes

Peter Bürgisser

Institut für Mathematik, Universität Zürich, Winterthurerstr. 190,
CH-8057 Zürich, Switzerland. E-mail: buerg@amath.unizh.ch

Abstract. In [25, 27] Valiant developed an algebraic analogue of the theory of NP-completeness for computations with polynomials over a field. We further develop this theory in the spirit of structural complexity and obtain analogues of well-known results by Baker, Gill, and Solovay [1], Ladner [18], and Schöning [23, 24].
We show that if Valiant's hypothesis is true, then there is a p-definable family, which is neither p-computable nor VNP-complete. More generally, we define the posets of p-degrees and c-degrees of p-definable families and prove that any countable poset can embedded in either of them, provided Valiant's hypothesis is true. Moreover, we establish the existence of minimal pairs for VP in VNP.
Over finite fields, we give a *specific* example of a family of polynomials which is neither VNP-complete nor p-computable, provided the polynomial hierarchy does not collapse.
We define relativized complexity classes VP^h and VNP^h and construct complete families in these classes. Moreover, we prove that there is a p-family h satisfying $\mathrm{VP}^h = \mathrm{VNP}^h$.

1 Introduction

One of the most important developments in theoretical computer science is the concept of NP-completeness. Recently, initiated by a paper by Blum, Shub, and Smale [5] (BSS-model), there has been a growing interest in investigating such concepts over general algebraic structures, with the purpose of classifying the complexity of continous problems. But already ten years earlier, Valiant [25, 27] had developed a convincing analogue of the theory of NP-completeness in an entirely algebraic framework, in connection with his famous hardness result for the permanent [26]. In fact, the polynomial enumerators of many NP-complete graph problems turn out to be complete in Valiant's sense (cf. [7]). The major differences between the BSS-model and Valiant's model are the absence of uniformity conditions in the latter, and the fact that only straight-line computations are considered (no branching). Both structured models are adapted to the framework of polynomial computations, and we believe that they will be useful for classifing the intrinsic complexity of problems in computer algebra (compare Heintz and Morgenstern [15]).

Our goal is to further develop Valiant's approach along the lines of discrete structural complexity theory.

We show that if Valiant's hypothesis is true, then, over any field, there is a p-definable family which is neither p-computable nor VNP-complete. A similar result due to Ladner [18] in the classical P-NP-setting is well-known. Ladner's proof is a diagonalization argument based on an effective enumeration of all polynomial time Turing machines. However, over uncountable structures, this approach causes problems. Malajovich and Meer [20] were able to carry over Ladner's theorem to the setting of the BSS-model over the complex numbers by employing a transfer principle due to Blum et al. [4], which allows a reduction to the countable field of algebraic numbers. The corresponding question over the reals is still open, but it is known to be true in the nonuniform BSS-setting, cf. Ben-David et al. [2]. (For a detailed treatement of these questions in a general model-theoretic context see Chapuis and Koiran [10].)

In our proof of the analogue of Ladner's theorem, the nonuniformity of Valiant's model is essential, since that allows an enumeration of all polynomial straight-line programs over a possibly uncountable field "in blocks". In Sect. 3 we formalize this idea in a general abstract setting by studying certain compatible quasi-orders on the set $\Omega^{\mathbb{N}}$ of families in a quasi-ordered set $(\Omega, \leq)$, and by proving an analogue of Schöning's uniform diagonalization theorem [23]. Hereby, our notion of a *nice subset* of $\Omega^{\mathbb{N}}$ serves as a substitute for the notion of a recursively presentable set. Based on this theorem, we proceed in Sect. 4 by providing an elegant proof that any countable poset can be embedded in the poset of degrees corresponding to a compatible quasi-order. This is applied in Sect. 5 in Valiant's setting to an analogue of the polynomial Turing reduction (c-reduction), as well as to the p-projection. A similar result in the classical P-NP-setting for polynomial Turing or polynomial many-one degrees was stated by Ladner [18]; however, he presented a proof only in a special case. We further remark that the existence of minimal pairs for VP in VNP can be easily guaranteed by our approach. (See Landweber et al. [19] and Schöning [24] for corresponding results in the classical P-NP setting.)

A striking discovery is that we can describe *specific* families of polynomials which are neither VNP-complete nor p-computable. In fact, the family of cut enumerators over a finite field of characteristic p has this property, provided $\mathrm{Mod}_p\mathrm{NP}$ is not contained in P/poly. (The latter condition is satisfied if the polynomial hierarchy does not collapse at the second level.) In the classical, as well as in the BSS-setting, only artificial problems are known to have such properties. This is discussed in Section 6.

Finally, in Sect. 7, we define relative versions VP^h and VNP^h of Valiant's complexity classes with respect to a p-family h. For these, we have obtained some results in the spirit of Baker et al. [1]. Over infinite fields, we can construct (artificial) VP^h-complete and VNP^h-complete families with respect to p-projection. Moreover, we can construct a p-family h satisfying $\mathrm{VP}^h = \mathrm{VNP}^h$. We do not know whether there exists a p-family h such that $\mathrm{VP}^h \neq \mathrm{VNP}^h$. Let us remark that Emerson [12] has transfered the results of Baker et al. [1] to the BSS-model.

Acknowledgement. Thanks go to Michael Clausen for encouraging me to investigate these questions.

2 Valiant's Model

We briefly recall the main features of Valiant's algebraic model. For detailed expositions see von zur Gathen [14] and [8, Chap. 21].

In this section $\Omega := k[X_1, X_2, \ldots]$ denotes the polynomial ring over a fixed field k in countably many variables X_i. A *p-family* over k is a sequence $f = (f_n) \in \Omega^{\mathbb{N}}$ of multivariate polynomials such that the number of variables as well as the degree of f_n are polynomially bounded (p-bounded) functions of n. An example of a p-family is the permanent family $\mathrm{PER} = (\mathrm{PER}_n)$, where PER_n is the permanent of an n by n matrix with distinct indeterminate entries.

Let $L(f_n)$ denote the total complexity of f_n, that is, the minimum number of arithmetic operations $+, -, *$ sufficient to compute f_n from the variables X_i and constants in k by a straight-line program. We call a p-family f *p-computable* iff $n \mapsto L(f_n)$ is p-bounded. The p-computable families constitute the complexity class VP. We remark that the restriction to p-bounded degrees is a severe one: although X^{2^n} can be computed with only n multiplications, the corresponding sequence is not considered to be p-computable, as the degrees grow exponentially.

A p-family $f = (f_n)$ is called *p-definable* iff there exists a p-computable family $g = (g_n)$ with $g_n \in k[X_1, \ldots, X_{u(n)}]$ such that for all n

$$f_n(X_1, \ldots, X_{v(n)}) = \sum_{e \in \{0,1\}^{u(n)-v(n)}} g_n(X_1, \ldots, X_{v(n)}, e_{v(n)+1}, \ldots, e_{u(n)}) \ . \quad (1)$$

The set of p-definable families form the complexity class VNP. The class VP is obviously contained in VNP, and *Valiant's hypothesis* claims that this inclusion is strict. We can consider this as an algebraic counterpart of the well-known hypothesis $\mathrm{P} \neq \mathrm{NP}$ due to Cook [11]. Let us mention the following recent result due to the author, which reveals a close connection between these two hypotheses. The crucial step in its proof is the elimination of constants in the field, which relies on a recent method developed by Koiran [17].

Theorem 2.1 ([6]). *If Valiant's hypothesis were false over the field k, then the nonuniform versions of the complexity classes* NC, P, NP, *and* PH *would be equal. In particular, the polynomial hierarchy would collapse to the second level. Hereby, we assume that k is finite or of characteristic zero; in the second case we assume a generalized Riemann hypothesis.*

We define now a quasi-order $\leq_p$ called *p-projection* on the set $\Omega^{\mathbb{N}}$ of families in Ω. Let us call a function $t\colon \mathbb{N} \to \mathbb{N}$ *p-bounded from above and below* iff there exists some $c > 0$ such that $n^{1/c} - c \leq t(n) \leq n^c + c$ for all n. A polynomial f_n is said to be a *projection* of a polynomial $g_m \in k[X_1, \ldots, X_u]$, for short $f_n \leq g_m$, iff

$$f_n(X_1, \ldots, X_{v(n)}) = g_m(a_1, \ldots, a_u)$$

for some $a_i \in k \cup \{X_1, \ldots, X_{v(n)}\}$. That is, f_n can be derived from g_m through substitution by indeterminates and constants. We call a p-family $f = (f_n)$ a

p-projection of $g = (g_m)$, in symbols $f \leq_p g$, iff there exists a function $t\colon \mathbb{N} \to \mathbb{N}$ which is p-bounded from above and below such that

$$\exists n_0\ \forall n \geq n_0 : f_n \leq g_{t(n)} \ . \tag{2}$$

(Our definition of $\leq_p$ differs slightly from the one given in [25] as we also require a lower bound on the growth of the functions t.) Finally, a p-family $g \in \mathrm{VNP}$ is called *VNP-complete* (with regard to p-projection) iff any $f \in \mathrm{VNP}$ is a p-projection of g.

In [25] Valiant obtained the remarkable result that the permanent family (if $\mathrm{char} k \neq 2$) and the family of Hamilton cycle polynomials are VNP-complete. It turns out that the "polynomial enumerators" of several NP-complete graph problems like Clique, H-factors, Hamilton cycles in planar graphs etc. are VNP-complete as well (cf. [7]).

3 An Abstract Diagonalization Theorem

Let a quasi-ordered set $(\Omega, \leq)$ be fixed. Elements of the set $\Omega^{\mathbb{N}}$ of sequences in Ω will be called *families* in the sequel. We may formally define a quasi-order $\leq_p$ (the abstract p-projection) on the set $\Omega^{\mathbb{N}}$ of families as in (2). Two families f and g are said to be *p-equivalent* iff $f \leq_p g$ and $g \leq_p f$. We call the equivalence classes *p-degrees* and denote by $\mathcal{D}_p$ the poset of all p-degrees with the partial order induced by $\leq_p$. $f <_p g$ shall mean that $f \leq_p g$ but not $g \leq_p f$. The *join* $f \cup g$ of two families $f, g \in \Omega^{\mathbb{N}}$ is defined as

$$f \cup g := (f_0, g_0, f_1, g_1, f_2, g_2, \ldots) \ .$$

It is easy to see that the join of two p-degrees is well-defined and that it is the smallest upper bound of these p-degrees in $\mathcal{D}_p$. The poset $\mathcal{D}_p$ of p-degrees is thus a join-semilattice.

Definition 3.1. We call a subset of $\Omega^{\mathbb{N}}$ *nice* iff it can be written as a countable union of cartesian products $\prod_{n \in \mathbb{N}} F_n$, where $F_n \subseteq \Omega$.

It is clear that countable unions and finite intersections of nice subsets of $\Omega^{\mathbb{N}}$ are again nice. However, one can show that the nice subsets are not closed under the formation of complements and countable intersections. Every nice set is measurable with respect to the product of σ-algebras $\otimes_n 2^{\Omega}$, but one can show that the converse is not true.

We call two families (f_n) and (g_n) *equal almost everywhere* iff $f_n = g_n$ for all but finitely many n. This is clearly an equivalence relation which is well defined on p-degrees. A subset $\mathcal{C} \subseteq \Omega^{\mathbb{N}}$ is called *closed under finite variation* iff $f \in \mathcal{C}$ implies $g \in \mathcal{C}$, provided f and g are equal almost everywhere.

The following theorem is inspired by Schöning's "uniform diagonalization theorem" [23] and can be proved similarly. We note that the nice sets serve as a substitute for the recursively presentable sets appearing there.

Theorem 3.2. *Let $\mathcal{F}, \mathcal{G}$ be nice subsets of $\Omega^{\mathbb{N}}$ which are closed under finite variation. Moreover, let $f, g \in \Omega^{\mathbb{N}}$ such that $f \notin \mathcal{F}$ and $g \notin \mathcal{G}$. Then there exists $h \in \Omega^{\mathbb{N}}$ satisfying $h \leq_p f \cup g$ and $h \notin \mathcal{F} \cup \mathcal{G}$.*

4 An Abstract Embedding Theorem

Again let a quasi-ordered set $(\Omega, \leq)$ be fixed and denote by $\leq_p$ the corresponding abstract p-projection. We extend our discussion to any quasi-order on $\Omega^{\mathbb{N}}$ which satisfies certain some compatibility conditions.

Definition 4.1. A quasi-order $\leq_c$ of $\Omega^{\mathbb{N}}$ is called *compatible*, iff the following conditions are satisfied:

(a) $\forall f, g : f \leq_p g \Rightarrow f \leq_c g$.
(b) $\forall f, g, h : f \leq_c h, g \leq_c h \Rightarrow f \cup g \leq_c h$.
(c) The sets $\{h \mid h \leq_c g\}$ and $\{h \mid f \leq_c h\}$ are nice for all $f, g \in \Omega^{\mathbb{N}}$.

It turns out that the quasi-order $\leq_p$ is compatible.

In the sequel, let a compatible quasi-order $\leq_c$ on $\Omega^{\mathbb{N}}$ be fixed. We call two families f and g *c-equivalent* iff $f \leq_c g$ and $g \leq_c f$. The corresponding equivalence classes are a union of certain p-degrees and called *c-degrees*. We denote by $\mathcal{D}_c$ the poset of all c-degrees with the partial order induced by $\leq_c$. $f <_c g$ means that $f \leq_c g$, but f and g are not c-equivalent. We say that $f <_p g$ *strongly* iff $f \leq_p g$ and $f <_c g$.

Let $(X, \subseteq)$ be a poset. A map $\varphi\colon X \to \Omega^{\mathbb{N}}$ is called an *embedding* of X in $\Omega^{\mathbb{N}}$ (with respect to $\leq_c$) if $x \subseteq y$ implies $\varphi(x) \leq_c \varphi(y)$ and vice versa. We call φ a *strong embedding* iff we have for all $x, y \in X$

$$x \subseteq y \Rightarrow \varphi(x) \leq_p \varphi(y) \text{ and } \varphi(x) \leq_c \varphi(y) \Rightarrow x \subseteq y \ .$$

The following theorem implies immediately that any countable poset can be embedded in both of the posets $\mathcal{D}_p$ and $\mathcal{D}_c$, provided $\mathcal{D}_c$ does not consist of a single point only.

Theorem 4.2. *For any countable poset $(X, \subseteq)$ and elements $f, g \in \Omega^{\mathbb{N}}$ with $f <_c g$ there is an embedding $X \to \{h \mid f <_c h <_c g\}$. If additionally $f \leq_p g$, then there is a strong embedding $X \to \{h \mid f <_p h <_p g\}$.*

It easy to see that any countable poset $(X, \subseteq)$ can be embedded in a countable lattice. For the proof of the above theorem, we may therefore assume that $(X, \subseteq)$ is a lattice.

Lemma 4.3. *Let $(X, \subseteq)$ be a countable lattice. Then there exists an enumeration $x_0, x_1, x_2, \ldots$ of X such each $X_n := \{x_0, \ldots, x_n\}$ is closed under taking meets: that is, $x \cap y \in X_n$ for all $x, y \in X_n$.*

For proving Thm. 4.2 we assume the situation of this lemma and show the following claim by induction on n. There is a map $\varphi_n\colon X_n \to \Omega^{\mathbb{N}}$ satisfying

$$f <_p \cap_{x\in X_n} \varphi_n(x) \text{ strongly } , \ \cup_{x\in X_n} \varphi_n(x) <_p g \text{ strongly } ,$$

and for all $x, y, y_1, \ldots, y_s \in X_n$ we have

$$x \subseteq y \Rightarrow \varphi_n(x) \leq_p \varphi_n(y), \ \varphi_n(x) \leq_c \varphi_n(y_1) \cup \ldots \cup \varphi_n(y_s) \Rightarrow x \subseteq y_1 \cup \ldots \cup y_s \ .$$

This is done by invoking Thm. 3.2 several times. Due to lack of space, we can not provide more details. To give the reader an idea of how Thm. 3.2 can be applied, we just note that the induction start $n = 0$ is obtained by applying this theorem to the nice sets $\mathcal{F} := \{h \mid g \leq_c h \cup f\}$ and $\mathcal{G} := \{h \mid h \leq_c f\}$. Note that $f \notin \mathcal{F}$ and $g \notin \mathcal{G}$ by our assumption $f <_c g$.

5 Structure of Valiant's Complexity Classes

In this section, we apply our previous results to the setting of Valiant. Let $\Omega := k[X_1, X_2, \ldots]$ denote the polynomial ring over a fixed field k in countably many variables X_i and consider the projection $\leq$, which is a quasi-order on Ω. (Recall that $f \leq g$ iff f can be obtained from g by a substitution of its variables by variables or constants in k.) The corresponding quasi-order $\leq_p$ on $\Omega^{\mathbb{N}}$ is the usual p-projection.

To avoid confusions, we remark that in the future symbols like $f, g, h, \ldots$ will be used to denote either polynomials or sequences of polynomials; it will always be clear from the context what is meant.

We are going to introduce the concept of oracle computations. Let a polynomial $g \in k[X_1, \ldots, X_a]$ be given. We will consider straight-line programs which, beside the usual arithmetic operations, have the ability to evaluate the "oracle polynomial" g at previously computed values at unit cost. This can easily be formalized by considering straight-line programs Γ of type $\{+, -, *, o\}$, where the symbol o stands for the oracle operation of arity a.

Definition 5.1. The *oracle complexity* $L^g(f_1, \ldots, f_s)$ of a set of polynomials $f_1, \ldots, f_s \in \Omega$ with respect to the oracle polynomial g is the minimum number of arithmetic operations $+, -, *$ and evaluations of g (at previously computed values) that are sufficient to compute f from the indeterminates X_i and constants in k.

We introduce next the notion of c-reduction, which can be seen as an analogue of the polynomial Turing reduction for Valiant's setting. (c is an acronym for $c$omputation.) One might also interpret the p-projection as an analogue of the polynomial many-one reduction, however, the p-projection is much finer.

Definition 5.2. Let $f = (f_n)$, $g = (g_n) \in \Omega^{\mathbb{N}}$. We call f a *c-reduction* (or polynomial oracle reduction) of g, shortly $f \leq_c g$, iff there is a p-bounded function $t\colon \mathbb{N} \to \mathbb{N}$ such that $n \mapsto L^{g_{t(n)}}(f_n)$ is p-bounded.

It easy to check that $\leq_c$ is a quasi-order of $\Omega^{\mathbb{N}}$. Note that for a p-family f we have $f \leq_c 0$ iff $f \in \mathrm{VP}$. The nonuniformity in the definition of the c-reduction allows to conclude that $\leq_c$ is compatible (compare Def. 4.1(c)).

Lemma 5.3. *The c-reduction $\leq_c$ is a compatible quasi-order on $\Omega^{\mathbb{N}}$.*

This implies for instance that VP and VNP are nice subsets of $\Omega^{\mathbb{N}}$. Let us call a p-degree or a c-degree *p-definable* iff it contains a p-definable family. Note that a p-definable p-degree consists of p-definable families only, whereas a p-definable c-degree might also contain families which are not in VNP. This is because $f \leq_c g$ and $g \in \mathrm{VNP}$ might not imply that $f \in \mathrm{VNP}$. We denote by $\mathcal{PD}_p$ the set of p-degrees of p-definable families and by $\mathcal{PD}_c$ the set of c-degrees of p-definable families.

The main result of this section is analogous to that of Ladner's work [18]. It follows easily from Thm. 4.2.

Theorem 5.4. *Any countable poset can be embedded in either of the posets $\mathcal{PD}_p$ or $\mathcal{PD}_c$, provided Valiant's hypothesis is true.*

Corollary 5.5. *If Valiant's hypothesis is true, then there is a p-definable family which is neither p-computable nor* VNP*-complete with respect to c-reduction.*

6 A Specific Family neither Complete nor p-Computable

We begin by recalling some facts from discrete complexity theory. For a prime number p the class $\mathrm{Mod}_p\mathrm{NP}$ is defined as the set of languages $\{x \in \{0,1\}^* \mid \varphi(x) \equiv 1 \bmod p\}$, where $\varphi\colon \{0,1\}^* \to \mathbb{N}$ is a function in #P (cf. Cai and Hemachandra [9]). This generalizes the class parity polynomial time $\oplus P$, which was introduced by Papadimitriou and Zachos [22]. We remark that if $\varphi\colon \{0,1\}^* \to \mathbb{N}$ is #P-complete with respect to parsimonious reductions, then the corresponding language $\{x \mid \varphi(x) \equiv 1 \bmod p\}$ is $\mathrm{Mod}_p\mathrm{NP}$-complete (with respect to polynomial many-one reductions).

From a well known randomized reduction due to Valiant and Vazirani [28] one can deduce the following inclusion of nonuniform complexity classes

$$\mathrm{NP/poly} \subseteq \mathrm{Mod}_p\mathrm{NP/poly} \ . \tag{3}$$

(For details see [6]; the notation $\mathcal{C}$/poly stands for the nonuniform version of the complexity class $\mathcal{C}$, cf. Karp and Lipton [16].)

Let $K_n = (\underline{n}, E_n)$ denote the complete graph on the set of nodes $\underline{n} := \{1, 2, \ldots, n\}$ and let $w\colon E_n \to \mathbb{N}$ be a weight function. A *cut* of K_n is a partition $S := \{A, B\}$ of $\underline{n}$ into two nonempty subsets. An edge is said to be separated by S if it connects a node of A with a node of B. The weight $w(S)$ of S is defined as the sum of the weights of all edges separated by S.

The counting problem #Cut is the following: given K_n, a weight function $w\colon E_n \to \{0, 1, \ldots, n^3\}$, and a natural number $s < D_n := n^3\binom{n}{2}$, what is the

number of cuts of K_n of weight s? (The required upper bound n^3 on the weights is just a useful technical assumption.) The related decision problem $\mathrm{Mod}_p\,\textsc{Cut}$ just asks for the residue class modulo a prime p of the number of cuts of weight s. This problem is clearly in $\mathrm{Mod}_p\mathrm{NP}$.

It is well known that the computation of a cut of maximal weight of a given graph is NP-hard. By a straightforward modification of the proof of this fact given in Papadimitriou [21, p. 191], one can strengthen this as follows.

Proposition 6.1. *#Cut is #P-complete with respect to parsimonious reductions. Thus* $\mathrm{Mod}_p\,\textsc{Cut}$ *is* $\mathrm{Mod}_p\mathrm{NP}$*-complete.*

The following p-family is related with the #Cut-problem. For $1 \le i < j \le n$ let X_{ij} be distinct indeterminates and set $X_{ji} := X_{ij}$. Let $q \in \mathbb{N}$, $q \ge 2$. The *cut enumerator* Cut_n^q is defined as

$$\mathrm{Cut}_n^q := \sum_S \prod_{i \in A, j \in B} X_{ij}^{q-1} \quad ,$$

where the sum is over all cuts $S = \{A, B\}$ of K_n. It is easy to see that $\mathrm{Cut}^q := (\mathrm{Cut}_n^q)$ is a p-definable family (over any field).

The connection to the counting problem #Cut is as follows. We may describe a weight function $w\colon E_n \to \{0, 1, \ldots, n^3\}$ of the complete graph K_n by the symmetric matrix $x \in \mathbb{N}^{n \times n}$ defined by $x_{ij} := 2^{nw(\{i,j\})}$. If $c(s)$ denotes the number of cuts in K_n of weight s, then we have

$$\mathrm{Cut}_n^q(x) = \sum_{\text{cut } S} 2^{(q-1)nw(S)} = \sum_{s < D_n} c(s) 2^{(q-1)ns} \quad .$$

As always $0 \le c(s) < 2^n \le 2^{(q-1)n}$, we can read off all the numbers $c(s)$ from the $2^{(q-1)n}$-ary expansion of $\mathrm{Cut}_n^q(x)$. Moreover, x can be computed from w in polynomial time by a Turing machine. This reasoning, together with Prop. 6.1, shows that the computation of $\mathrm{Cut}_n^q(x)$ for symmetric matrices $x \in \mathbb{N}^{n \times n}$ is #P-hard.

Over finite fields $\mathbb{F}_q$ the situation is different. Let $p := \mathrm{char}\,\mathbb{F}_q$.

Lemma 6.2. *To a symmetric matrix $x \in \mathbb{F}_q^{n \times n}$ we assign the graph $G(x)$ on the set of nodes $\underline{n}$ by requiring that $\{i, j\}$ is an edge iff $x_{ij} = 0$. Then we have*

$$\mathrm{Cut}_n^q(x) = 2^{N(x)-1} - 1 \bmod p \quad ,$$

where $N(x)$ is the number of connected components of $G(x)$. In particular, the value $\mathrm{Cut}_n^q(x)$ can be computed from a symmetric $x \in \mathbb{F}_q^{n \times n}$ in polynomial time by a Turing machine.

Proof. For any nonzero $\lambda \in \mathbb{F}_q$ we have $\lambda^{q-1} = 1$ by Fermat's theorem. Let $x \in \mathbb{F}_q^{n \times n}$ be symmetric. A partition $\{A, B\}$ of $\underline{n}$ contributes to $\mathrm{Cut}_n^q(x)$ either zero or one. The contribution is one iff $X_{ij} \neq 0$ for all $i \in A$, $j \in B$, that is, none of the nodes of A is connected with any node in B in the graph $G(x)$. This in turn means that A and B are both a union of certain connected components of the graph $G(x)$. The number of such partitions clearly equals $2^{N(x)} - 1$, where $N(x)$ is the number of connected components of $G(x)$. This proves the lemma. □

The main result of this section states that Cut^q is an explicit example of a p-family over the finite field $\mathbb{F}_q$, which is neither p-computable nor complete in VNP.

Theorem 6.3. *The family of cut enumerators* Cut^q *over a finite field* $\mathbb{F}_q$ *of characteristic* p *is neither* p*-computable nor* VNP*-complete with respect to* c*-reduction, provided* $\mathrm{Mod}_p\mathrm{NP} \not\subseteq \mathrm{P/poly}$.

We remark that the inclusion $\mathrm{Mod}_p\mathrm{NP} \subseteq \mathrm{P/poly}$ implied $\mathrm{NP/poly} \subseteq P/\mathrm{poly}$ by (3) and therefore, by a well-known result by Karp and Lipton [16], the collapse of the polynomial hierarchy at the second level.

Proof. (of Thm. 6.3) Let L be a language in $\mathrm{Mod}_p\mathrm{NP}$, say $L = \{x \in \{0,1\}^* \mid \varphi(x) \equiv 1 \bmod p\}$, where $\varphi\colon \{0,1\}^* \to \mathbb{N}$ is in the class #P. In [6] it is shown that there exists a p-definable family (f_n) over $\mathbb{F}_p$ such that $f_n \in \mathbb{F}_p[X_1, \ldots, X_n]$ and

$$\forall n\ \forall x \in \{0,1\}^n : f_n(x) = \varphi(x) \bmod p \ .$$

Assume now that Cut^q is VNP-complete with respect to c-reduction. Then we have $(f_n) \leq_c \mathrm{Cut}^q$, hence there is a p-bounded function $t\colon \mathbb{N} \to \mathbb{N}$ such that $L^{\mathrm{Cut}^q_{t(n)}}(f_n)$ is p-bounded. Lemma 6.2 tells us that $\mathrm{Cut}^q_{t(n)}$ can be evaluated in polynomial time on an input over $\mathbb{F}_q$. Hence we may design for each n a boolean circuit C_n of p-bounded size which computes $f_n(x)$ from $x \in \mathbb{F}_q^n$. This implies that the language L is contained in P/poly. We therefore arrive at the conclusion $\mathrm{Mod}_p\mathrm{NP} \subseteq \mathrm{P/poly}$.

Let $K_n = \mathbb{F}_q(\xi_n)$ be a field extension of $\mathbb{F}_q$ of degree $(q-1)D_n$. To an instance $w\colon E_n \to \{0, 1, \ldots, n^3\}$ of #CUT we assign the symmetric matrix $x \in K_n^{n \times n}$ defined by $x_{ij} := \xi_n^{w(\{i,j\})}$. Then we have

$$\mathrm{Cut}_n^q(x) = \sum_{\mathrm{cut}\ S} \xi_n^{(q-1)w(S)} = \sum_{s < D_n} (c(s) \bmod p)\, \xi_n^{(q-1)s} \quad ,$$

where $c(s)$ is the number of cuts in K_n of weight s. Note that the coefficients $c(s) \bmod p$ are uniquely determined by $\mathrm{Cut}_n^q(x)$.

Assume now that Cut^q is in $\mathrm{VP}_{\mathbb{F}_q}$. Hence for each n there is a straight-line program Γ_n of p-bounded size in n, which computes $\mathrm{Cut}_n^q(X)$ from constants in $\mathbb{F}_q$ and the indeterminates X_{ij} in the polynomial ring $\mathbb{F}_q[X_{ij} \mid 1 \leq i, j \leq n]$. By the universal property of the polynomial ring, Γ_n will compute $\mathrm{Cut}_n^q(x)$ in K_n from the same constants and $x \in K_n^{n \times n}$. We may simulate this computation by a boolean circuit of p-bounded size, since the arithmetic operations in K_n can be simulated by p-bounded circuits (note that D_n is p-bounded). In this way we could solve the Mod_p CUT problem in nonuniform polynomial time. As Mod_p CUT is $\mathrm{Mod}_p\mathrm{NP}$-complete by Prop. 6.1, this would imply that $\mathrm{Mod}_p\mathrm{NP} \subseteq \mathrm{P/poly}$. □

Remark 6.4. It would be interesting to find out whether Cut^2 is VNP-complete with respect to c-reduction (or even p-projection) over fields k of characteristic zero.

7 Relativized Complexity Classes

Our investigations here are inspired by the well-known results of Baker, Gill, and Solovay [1] on relativations of the classical P-NP question. Due to lack of space our exposition is very brief. Relative versions of the complexity classes VP and VNP can be defined as follows.

Definition 7.1. Let h be a p-family. VP^h consists of all p-families f such that $f \leq_c h$. VNP^h is the set of all p-families $f = (f_n)$ which can be obtained from some $g = (g_n) \in \mathrm{VP}^h$ in the sense of (1).

Note that VP^h and VNP^h specialize to VP and VNP if h is p-computable.

We are able to construct complete families for the complexity classes VP^h and VNP^h. The idea is to use a generalization of the concept of generic computations (cf. [8, Chap. 9]). In order to avoid an exponential growth of degrees, we combine this with an auxiliary result on the computation of homogeneous components, which works by evaluation and interpolation, and requires that k contains sufficiently many points. This way, we can prove the following.

Theorem 7.2. *For any p-family h over an infinite field k there exist VP^h-complete and VNP^h-complete families with respect to p-projection.*

In particular, this gives a new proof for the existence of VNP-complete families, which does not depend on Valiant's intricate reduction for the permanent.

By combining this theorem with some diagonalization argument, we are able to show the following.

Theorem 7.3. *There exists a p-family h such that $\mathrm{VP}^h = \mathrm{VNP}^h$ over infinite fields.*

Up to now we have not succeeded in establishing a p-family h such that $\mathrm{VP}^h \neq \mathrm{VNP}^h$. A promising approach for this is as follows (compare Bennett and Gill [3]). For each n choose independently $h_n \in k[X_1, \ldots, X_n]$ of degree most n *at random* according to some probability distribution. Since the classes VP^h and VNP^h are invariant under finite variation of h, the event $\mathcal{E} = \{h \mid \mathrm{VP}^h \neq \mathrm{VNP}^h\}$ is a so-called tail event. Kolmogorov's zero-one law (cf. Feller [13, Chap. 4]) implies therefore that $\mathrm{Prob}(\mathcal{E}) \in \{0, 1\}$. We conjecture that this probability is one if the h_n are chosen with independent $0, 1$-coefficients.

References

1. T. Baker, J. Gill, and R. Solovay. Relativizations of the $P =? NP$ question. *SIAM J. Comp.*, 4:431–442, 1975.
2. S. Ben-David, K. Meer, and C. Michaux. A note on non-complete problems in $\mathrm{NP}_{\mathbb{R}}$. Preprint, 1996.
3. C.H. Bennett and J. Gill. Relative to a random oracle A, $\mathrm{P}^A \neq \mathrm{NP}^A \neq \mathrm{co-NP}^A$ with probability 1. *SIAM J. Comp.*, 10:96–113, 1981.

4. L. Blum, F. Cucker, M. Shub, and S. Smale. Algebraic Settings for the Problem "$P \neq NP$?". In *The mathematics of numerical analysis*, number 32 in Lectures in Applied Mathematics, pages 125–144. Amer. Math. Soc., 1996.
5. L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers. *Bull. Amer. Math. Soc.*, 21:1–46, 1989.
6. P. Bürgisser. Cook's versus Valiant's hypothesis. Preprint, University of Zurich, 1997.
7. P. Bürgisser. Some complete families of polynomials. Manuscript, 1997.
8. P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic Complexity Theory*. Number 315 in Grundlehren der mathematischen Wissenschaften. Springer Verlag, 1996.
9. J. Cai and L.A. Hemachandra. On the power of parity polynomial time. In *Proc. STACS'89*, number 349 in LNCS, pages 229–239. Springer Verlag, 1989.
10. O. Chapuis and P. Koiran. Saturation and Stability in the Theory of Computation over the Reals. Preprint, 1997.
11. S.A. Cook. The complexity of theorem proving procedures. In *Proc. 3rd ACM STOC*, pages 151–158, 1971.
12. T. Emerson. Relativizations of the P=?NP question over the reals (and other ordered rings). *Theoret. Comp. Sci.*, 133:15–22, 1994.
13. W. Feller. *An introduction to probability theory and its applications*, volume 2. John Wiley & Sons, 1971.
14. J. von zur Gathen. Feasible arithmetic computations: Valiant's hypothesis. *J. Symb. Comp.*, 4:137–172, 1987.
15. J. Heintz and J. Morgenstern. On the intrinsic complexity of elimination theory. *Journal of Complexity*, 9:471–498, 1993.
16. R.M. Karp and R.J. Lipton. Turing machines that take advice. In *Logic and Algorithmic: An international Symposium held in honor of Ernst Specker*, pages 255–273. Monogr. No. 30 de l'Enseign. Math., 1982.
17. P. Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. *J. Compl.*, 12:273–286, 1996.
18. R.E. Ladner. On the structure of polynomial time reducibility. *J. ACM*, 22:155–171, 1975.
19. Landweber, Lipton, and Robertson. On the structure of sets in NP and other complexity classes. *Theoret. Comp. Sci.*, 15:181–200, 1981.
20. G. Malajovich and K. Meer. On the structure of $\mathrm{NP}_{\mathbb{C}}$. *SIAM J. Comp.* to appear.
21. C.H. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.
22. C.H. Papadimitriou and S. Zachos. Two remarks on the power of counting. In *Proc. 6th GI conference in Theoretical Computer Science*, number 145 in LNCS, pages 269–276. Springer Verlag, 1983.
23. U. Schöning. A uniform approach to obtain diagonal sets in complexity classes. *Theoret. Comp. Sci.*, 18:95–103, 1982.
24. U. Schöning. Minimal pairs for P. *Theoret. Comp. Sci.*, 31:41–48, 1984.
25. L.G. Valiant. Completeness classes in algebra. In *Proc. 11th ACM STOC*, pages 249–261, 1979.
26. L.G. Valiant. The complexity of computing the permanent. *Theoret. Comp. Sci.*, 8:189–201, 1979.
27. L.G. Valiant. Reducibility by algebraic projections. In *Logic and Algorithmic: an International Symposium held in honor of Ernst Specker*, volume 30, pages 365–380. Monographies de l'Enseignement Mathématique, 1982.
28. L.G. Valiant and V.V. Vazirani. NP is as easy as detecting unique solutions. *Theoret. Comp. Sci.*, 47:85–93, 1986.