Satisfiability of cross product terms is complete for real nondeterministic polytime Blum-Shub-Smale machines*

Christian Herrmann Johanna Sokoli Martin Ziegler
Dept. of Mathematics, TU Darmstadt, GERMANY

Nondeterministic polynomial-time Blum-Shub-Smale Machines over the reals give rise to a discrete complexity class between **NP** and **PSPACE**. Several problems, mostly from real algebraic geometry / polynomial systems, have been shown complete (under many-one reduction by polynomial-time Turing machines) for this class. We exhibit a new one based on questions about expressions built from cross products only.

1 Motivation

The Millennium Question "**P** vs. **NP**" asks whether polynomial-time algorithms that may guess, and then verify, bits can be turned into deterministic ones. It arose from the Cook–Levin–Theorem asserting Boolean Satisfiability to be complete for **NP**; which initiated the identification of more and more other natural problems also complete [GaJo79].

The Millennium Question is posed [Smal98] also for models able to guess objects more general than bits. More precisely a Blum-Shub-Smale (BSS) machine over a ring R may operate on elements from R within unit time. It induces the nondeterministic polynomial-time complexity class $\mathbf{NP}_R$; for which the following problem FEAS_R has been shown complete [BSS89, MAIN THEOREM]:

Given† *a system of multivariate polynomials over R,*
does it admit a joint root from R ?

See also [Cuck93, THEOREM 3.1] or [BCSS98, §5.4]. More precisely $\mathsf{FEAS}_R \subseteq R^*$ is $\mathbf{NP}_R$–complete with respect to many-one (aka Karp) reducibility by polynomial-time BSS-machines *with* the capability to peruse finitely many fixed constants from R. BSS Machines with*out* constants on the other hand give, restricted to *binary* inputs, rise to the discrete complexity class $\mathbf{BP}(\mathbf{NP}^0_R)$ [MeMi97, DEFINITION 3.2]; for which the following problem $\mathsf{FEAS}^0_R \subseteq \{0,1\}^*$ is complete under many-one reduction by polynomial-time Turing machines:

Given a system of multivariate polynomials with 0*s and* ±1*s as coefficients,*
does it admit a joint root from R ?

BSS machines over $\mathbb{R}$ coincide with the real-RAM model from Computational Geometry [BKOS97] and underlie algorithms in Semialgebraic Geometry [Gius91, Lece00, BüSc09]. They give rise to a particularly rich structural complexity theory resembling the classical Turing Machine-based one – but often (unavoidably) with surprisingly different proofs [Bürg00, BaMe13]. It is known that $\mathbf{NP} \subseteq \mathbf{BP}(\mathbf{NP}^0_{\mathbb{R}}) \subseteq$ **PSPACE** holds [Grig88, Cann88, HRS90, Rene92]. $\mathsf{FEAS}_{\mathbb{R}}$ and $\mathsf{FEAS}^0_{\mathbb{R}}$ are sometimes referred to as existential theory over the reals. However even in this highly important case $R = \mathbb{R}$, and in striking contrast to **NP**, relatively few other natural problems have yet been identified as complete:

*Supported in parts by the *Marie Curie International Research Staff Exchange Scheme Fellowship* 294962 within the 7th European Community Framework Programme

†e.g. as lists of monomials and their coefficients or as algebraic expressions

Submitted to:
MCU 2013

- Several questions about systems of polynomials [CuRo92, Koir99]
- Stretchability of pseudoline arrangements [Shor91]
- Realizability of oriented matroids [Rich99]
- Loading neural networks with real weights [Zhan92]
- Several geometric properties of graphs [Scha10]
- Satisfiability in Quantum Logic QSAT, starting from dimension 3 [HeZi11].

The present work extends this list: We study questions about expressions built using variables and the cross (aka vector) product "$\times$" only, and we establish some of them complete for $\mathbf{NP}_{\mathbb{R}}$ or $\mathbf{BP}(\mathbf{NP}^0_{\mathbb{R}})$. These problems are in a sense 'simplest' as they involve only one binary operation symbol (as opposed to $+,\cdot$ for $\mathsf{FEAS}^0_{\mathbb{R}}$ or $\vee,\neg$ for QSAT); in fact so simple that their (trans-**NP**) hardness may appear as surprising.

Remark 1. *Another decision problem related to $\mathsf{FEAS}_{\mathcal{R}}$ and $\mathsf{FEAS}^0_{\mathcal{R}}$ is the question of whether a given multivariate polynomial p is identically zero or not. In dense representation (list of monomials and coefficients) this can easily be solved (over rings $\mathcal{R}$ of characteristic 0) by checking whether all coefficients vanish or not. However when p is given as a expression, expanding that based on the distributive law may result in an exponential blow-up of description length. The following Polynomial Identity Testing problem is thus not known to be polytime decidable:*

> *Given a multivariate ring term $p(X_1,\ldots,X_n)$ with constants 0 and ± 1,*
> *does it admit an assignment $x_1,\ldots,x_n$ such that $p(x_1,\ldots,x_n)\neq 0$*

It can be solved, though, in randomized polytime with one-sided error (class $\mathbf{RP}\subseteq\mathbf{NP}$) based on the Schwartz-Zippel Lemma, cmp. [MR95, §1.5 and THM 7.2].

2 Cross Product and Induced Problems

The cross product in $\mathbb{R}^3$ is well-known due to its many applications in physics such as torque or electromagnetism. Mathematically it constitutes the mapping

$$\times : \mathbb{R}^3\times\mathbb{R}^3 \ni \big((v_0,v_1,v_2),(w_0,w_1,w_2)\big) \mapsto (v_1w_2-v_2w_1,\, v_2w_0-v_0w_2,\, v_0w_1-v_1w_0) \in \mathbb{R}^3 \quad . \qquad (1)$$

It is bilinear (thus justifying the name "product") but anti-commutative $\vec{v}\times\vec{w}=-\vec{v}\times\vec{w}$ and non-associative and fails the cancellation law. The following is easily verified:

Fact 2. *a) For any independent $\vec{v},\vec{w}$, the cross product $\vec{u}=\vec{v}\times\vec{w}$ is uniquely determined by the following: $\vec{u}\perp\vec{v}$, $\vec{u}\perp\vec{w}$ (where "$\perp$" denotes orthogonality), the triplet $\vec{v},\vec{w},\vec{u}$ is right-handed, and lengths satisfy $\|\vec{u}\|=\|\vec{v}\|\cdot\|\vec{w}\|\cos\angle(\vec{v},\vec{w})$. In particular, parallel $\vec{v},\vec{w}$ are mapped to $\vec{0}$.*

b) Cross products commute with simultaneous orientation preserving orthogonal transformations: For $O\in\mathbb{R}^{3\times 3}$ with $O\cdot O^\dagger=\mathrm{id}$ and $\det(O)=1$ it holds $(O\cdot\vec{v})\times(O\cdot\vec{w})=O\cdot(\vec{v}\times\vec{w})$, where $O^\dagger$ denotes the transposed matrix.

Definition 3. *Fix a field $\mathbb{F}\subseteq\mathbb{R}$.*

a) A term $t(V_1,\ldots,V_n)$ (over "$\times$", in variables $V_1,\ldots,V_n$) is either one of the variables or $(s\times t)$ for terms s,t (in variables $V_1,\ldots,V_n$).

b) For $\vec{v}_1,\ldots,\vec{v}_n\in\mathbb{F}^3$ the value $t(v_1,\ldots,v_n)$ is defined inductively via Eq. (1).

c) *A term with affine constants is a term $t(V_1,\ldots,V_n;W_1,\ldots,W_m)$ where variables $W_1,\ldots,W_m$ have been pre-assigned certain values $\vec{w}_1,\ldots,\vec{w}_m \in \mathbb{R}^3$.*

d) *Recall that $\mathbb{P}^2(\mathbb{F}) := \{\mathbb{F}\vec{v} : \vec{0} \neq \vec{v} \in \mathbb{F}^3\}$ denotes the real projective plane, where $\mathbb{F}\vec{v} = \{\lambda\vec{v} : \lambda \in \mathbb{F}\}$. For distinct $\mathbb{F}\vec{v},\mathbb{F}\vec{w} \in \mathbb{P}^2(\mathbb{F})$ (well-)define $(\mathbb{F}\vec{v}) \times (\mathbb{F}\vec{w}) := \mathbb{F}(\vec{v}\times\vec{w})$; $\mathbb{F}\vec{v}\times\mathbb{F}\vec{v}$ is undefined.*

e) *For a term $t(V_1,\ldots,V_n)$ and $\mathbb{F}\vec{v}_1,\ldots,\mathbb{F}\vec{v}_n \in \mathbb{P}^2(\mathbb{F})$, the value $t(\mathbb{F}\vec{v}_1,\ldots,\mathbb{F}\vec{v}_n)$ is defined inductively via d), provided all sub-terms are defined.*

f) *A term with projective constants is a term $t(V_1,\ldots,V_n;W_1,\ldots,W_m)$ where variables $W_1,\ldots,W_m$ have been pre-assigned certain values $\mathbb{R}\vec{w}_1,\ldots,\mathbb{R}\vec{w}_m \in \mathbb{P}^2(\mathbb{R})$.*

Note that every term admits an affine assignment making it evaluate to $\vec{0}$. Some terms in fact always evaluate to $\vec{0}$; equivalently: are projectively undefined everywhere.

Example 4. *Consider the term $t(V,W) := \Big(\big(V\times(V\times W)\big)\times V\Big)\times(V\times W)$. Observe that $\vec{v}$, $\vec{v}\times\vec{w}$, and $\vec{v}\times(\vec{v}\times\vec{w})$ together form an orthogonal system for any non-parallel $\vec{v},\vec{w}$. Moreover $\big(\vec{v}\times(\vec{v}\times\vec{w})\big)\times\vec{v}$ is parallel to $\vec{v}\times\vec{w}$. Therefore $t(\vec{v},\vec{w}) = \vec{0}$ holds for every choice of $\vec{v},\vec{w}\in\mathbb{R}^3$.*

We are interested in the computational complexity of the following discrete decision problems:

Definition 5. a) $\mathsf{XNONTRIV}^0_{\mathbb{F}^3} := \big\{\langle t(V_1,\ldots,V_n)\rangle \;\big|\; n\in\mathbb{N},\ \exists\vec{v}_1,\ldots,\vec{v}_n\in\mathbb{F}^3 : t(\vec{v}_1,\ldots,\vec{v}_n)\neq\vec{0}\big\}$.

b) $\mathsf{XNONTRIV}^0_{\mathbb{P}^2(\mathbb{F})} := \big\{\langle t(V_1,\ldots,V_n)\rangle \;\big|\; n\in\mathbb{N},\ \exists\mathbb{F}\vec{v}_1,\ldots,\mathbb{F}\vec{v}_n] \in\mathbb{P}^2(\mathbb{F}) : t(\mathbb{F}\vec{v}_1,\ldots,\mathbb{F}\vec{v}_n)$ *defined*$\big\}$.

c) $\mathsf{XUVEC}^0_{\mathbb{F}^3} := \big\{\langle t(V_1,\ldots,V_n)\rangle \;\big|\; n\in\mathbb{N},\ \exists\vec{v}_1,\ldots,\vec{v}_n\in\mathbb{F}^3 : t(\vec{v}_1,\ldots,\vec{v}_n) = \vec{e}_3 := (0,0,1)\big\}$.

d) $\mathsf{XNONEQUIV}^0_{\mathbb{P}^2(\mathbb{F})} := \big\{\langle s(V_1,\ldots,V_n), t(V_1,\ldots,V_n)\rangle \;\big|$
$n\in\mathbb{N},\ \exists\mathbb{F}\vec{v}_1,\ldots,\mathbb{F}\vec{v}_n\in\mathbb{P}^2(\mathbb{F}) : s(\mathbb{F}\vec{v}_1,\ldots,\mathbb{F}\vec{v}_n)\neq t(\mathbb{F}\vec{v}_1,\ldots,\mathbb{F}\vec{v}_n)$, *both sides defined*$\big\}$.

e) $\mathsf{XSAT}^0_{\mathbb{F}^3} := \big\{\langle t_1(V_1,\ldots,V_n)\rangle \;\big|\; n\in\mathbb{N},\ \exists\vec{v}_1,\ldots,\vec{v}_n\in\mathbb{F}^3 : t(\vec{v}_1,\ldots,\vec{v}_n) = \vec{v}_1\neq\vec{0}\big\}$.

f) $\mathsf{XSAT}^0_{\mathbb{P}^2(\mathbb{F})} := \big\{\langle t_1(V_1,\ldots,V_n)\rangle \;\big|\; n\in\mathbb{N},\ \exists\mathbb{F}\vec{v}_1,\ldots,\mathbb{F}\vec{v}_n\in\mathbb{P}^2(\mathbb{F}) : t(\mathbb{F}\vec{v}_1,\ldots,\mathbb{F}\vec{v}_n) = \mathbb{F}\vec{v}_1\big\}$.

Real *variants of problems a) to f) without superscript 0 are defined similarly for input terms* with *constants; e.g.* $\mathsf{XSAT}_{\mathbb{R}^3} := \big\{\langle t_1(V_1,\ldots,V_n;\vec{w}_1,\ldots,\vec{w}_k)\rangle \;\big|\; n,k\in\mathbb{N},\ \vec{w}_1,\ldots,\vec{w}_k\in\mathbb{R}^3$
$\exists\vec{v}_1,\ldots,\vec{v}_n\in\mathbb{R}^3 : t(\vec{v}_1,\ldots,\vec{v}_n;\vec{w}_1,\ldots,\vec{w}_k) = \vec{v}_1\neq\vec{0}\big\} \subseteq \mathbb{R}^*$.

Our main result is

Theorem 6. a) *Among the above discrete decision problems,* $\mathsf{XNONTRIV}^0_{\mathbb{R}^3}$, $\mathsf{XNONTRIV}^0_{\mathbb{P}^2(\mathbb{R})}$, $\mathsf{XUVEC}^0_{\mathbb{R}^3}$, *and* $\mathsf{XNONEQUIV}^0_{\mathbb{P}^2(\mathbb{R})}$ *are polytime equivalent to polynomial identity testing (and in particular belong to* **RP***).*

b) *For any fixed field $\mathbb{F}\subseteq\mathbb{R}$, the discrete decision problems* $\mathsf{XSAT}^0_{\mathbb{F}^3}$ *and* $\mathsf{XSAT}^0_{\mathbb{P}^2(\mathbb{F})}$ *are* $\mathbf{BP}(\mathbf{NP}^0_{\mathbb{F}})$*–complete.*

c) $\mathsf{XSAT}_{\mathbb{R}^3}$ *and* $\mathsf{XSAT}_{\mathbb{P}^2(\mathbb{R})}$ *are* $\mathbf{NP}_{\mathbb{R}}$*–complete.*

This establishes a normal form for cross product equations with a variable on the right-hand side — in spite of the lack of a cancellation law.

3 Proofs

$\mathsf{XNONTRIV}^0_{\mathbb{P}^2(\mathbb{F})}$ is equal to $\mathsf{XNONTRIV}^0_{\mathbb{F}^3}$ as a set; and it holds $\mathsf{XNONTRIV}^0_{\mathbb{P}^2(\mathbb{R})} = \mathsf{XUVEC}^0_{\mathbb{R}^3}$: Suppose $t(\vec{v}_1,\ldots,\vec{v}_n) =: \vec{w}\neq\vec{0}$. Since t is homogeneous in each coordinate, by suitably scaling some argument $\vec{v}_j$ we may w.l.o.g. suppose[‡] $|\vec{w}| = 1$. Now take an orientation preserving orthogonal transformation

[‡] This requires taking square roots

O with $O\cdot\vec{w}=\vec{e}_3$: 2b) yields $t(O\cdot\vec{v}_1,\ldots,O\cdot\vec{v}_n)=\vec{e}_3$. Concerning the reduction from $\mathsf{XNONEQUIV}^0_{\mathbb{P}^2(\mathbb{F})}$ to $\mathsf{XNONTRIV}^0_{\mathbb{F}}$ observe that, for $\vec{v}_1,\ldots,\vec{v}_n\in\mathbb{F}^3\setminus\{\vec{0}\}$, $\mathbb{F}s(\vec{v}_1,\ldots,\vec{v}_n)\neq\mathbb{F}t(\vec{v}_1,\ldots,\vec{v}_n)$ implies $s(\vec{v}_1,\ldots,\vec{v}_n)\times t(\vec{v}_1,\ldots,\vec{v}_n)\neq 0$ and vice versa. Conversely an instance to $\mathsf{XNONTRIV}^0_{\mathbb{F}}$ is either a variable (trivial case) or of the form $s\times t$; in which case nontriviality is equivalent to projective nonequivalence of s,t.

We now reduce $\mathsf{XNONTRIV}^0_{\mathbb{R}^3}$ to polynomial identity testing, observing that $\vec{u}\times\vec{v}$ is a triple of bilinear polynomials in the 6 variables u_x,u_y,u_z,v_x,v_y,v_z with coefficients $0,\pm 1$. Thus, $t(\vec{v}_1,\ldots,\vec{v}_n)$ amounts to a triple of terms p_x,p_y,p_z in $3n$ variables with coefficients $0,\pm1$. Now by construction a real assignment $\vec{v}_1,\ldots,\vec{v}_n$ makes t evaluate to nonzero iff the three terms p_x,p_y,p_z do not simultaneously evaluate to zero. This yields the reduction $t\mapsto p_x^2+p_y^2+p_z^2$.

Concerning $\mathsf{XSAT}_{\mathbb{R}^3}$, a nondeterministic real BSS machine can, given a term $t(V_1,\ldots,V_n;\vec{w}_1,\ldots,\vec{w}_k)$ with constants $\vec{w}_j\in\mathbb{R}^3$, in time polynomial in the length of t guess an assignment $\vec{v}_1,\ldots,\vec{v}_n\in\mathbb{R}^3$ and apply Eq. (1) to evaluate t and verify the result to be nonzero. Similarly a nondeterministic BSS machine over $\mathbb{F}$ can, given a term $t(V_1,\ldots,V_n)$ without constants, in polytime guess and evaluate it on an assignment $\vec{v}_1,\ldots,\vec{v}_n\in\mathbb{F}^3$.

$\mathsf{XSAT}^0_{\mathbb{P}^2(\mathbb{R})}$ reduces to $\mathsf{XSAT}^0_{\mathbb{R}^3}$ in polytime as follows: For any $\vec{w}$ non-parallel to $\vec{t}$, $\vec{t}':=(\vec{t}\times\vec{w})\times\big((\vec{t}\times\vec{w})\times t\big)$ is a multiple of $\vec{t}$; see Fig. 1a). Note that scaling $\vec{w}$ affects $\vec{t}'$ quadratically. Similarly, $\big(\vec{w}\times(\vec{t}\times\vec{w})\big)\times\vec{t}$ is a multiple of $\vec{t}\times\vec{w}$; and replacing it in the first subterm defining $\vec{t}'$ (and renaming $\vec{t},\vec{t}'$ to $\vec{s},\vec{s}'$) shows that $\vec{s}':=\Big(\big(\vec{w}\times(\vec{s}\times\vec{w})\big)\times\vec{s}\Big)\times\big(\vec{s}\times(\vec{s}\times\vec{w})\big)$ is a multiple of $\vec{s}$; one scaling cubically with $\vec{w}$. So $\mathbb{R}$ being closed under cubic roots, $s(V_1,\ldots,V_n)=V_1$ is satisfiable over $\mathbb{P}^2(\mathbb{R})$ iff $s(V_1,\ldots,V_n)=\lambda^3V_1$ is satisfiable over $\mathbb{R}^3$ for some $\lambda\in\mathbb{R}$ iff $s'(V_1,\ldots,V_n,W)=V_1$ is satisfiable over $\mathbb{R}^3$, where $s':=\Big(\big(W\times(s\times W)\big)\times s\Big)\times\big(s\times(s\times W)\big)$. The reduction for the case *with* constants, that is from $\mathsf{XSAT}_{\mathbb{P}^2(\mathbb{R})}$ to $\mathsf{XSAT}_{\mathbb{R}^3}$, works similarly.

3.1 Hardness

It remains to reduce (in polynomial time)

i) $\mathsf{FEAS}_{\mathbb{R}}$ to $\mathsf{XSAT}_{\mathbb{P}^2(\mathbb{R})}$ and

ii) $\mathsf{FEAS}^0_{\mathbb{F}}$ to $\mathsf{XSAT}^0_{\mathbb{P}^2(\mathbb{F})}$ and

iii) polynomial identity testing to $\mathsf{XNONTRIV}^0_{\mathbb{P}^2(\mathbb{R})}$.

These can be regarded as quantitative refinements of [HaSv96]. We first recall some elementary, but useful facts about the cross product in the projective setting.

Fact 7. *Consider $U,V,W,T\in\mathbb{P}^2(\mathbb{F})$. By 'plane' we mean 2-dimensional linear subspace.*

1) $U=V\times W$ iff the plane orthogonal to U is spanned by V,W. In particular, $V\times W=W\times V$.

2) If $V\times W$ and $U\times T$ are defined then $(V\times W)\times(U\times T)$ is the intersection of the plane spanned by V,W with the plane spanned by U,T; undefined if this intersection is degenerate.

3) $V\times(W\times V)$ is the orthogonal projection of W into the plane orthogonal to V; undefined iff $W=V$, i.e. in case the projection is degenerate.

The following considerations are heavily inspired by the works of John von Neumann but for the sake of self-containment here boiled down explicitly.

Lemma 8. *Fix a subfield $\mathbb{F}$ of $\mathbb{R}$. Let $\vec{v}_1, \vec{v}_2, \vec{v}_3$ denote an orthogonal basis of $\mathbb{F}^3$. Then $V_j := \mathbb{F}\vec{v}_j$ satisfies $V_1 \times V_2 = V_3$, $V_2 \times V_3 = V_1$, and $V_3 \times V_1 = V_2$. Moreover abbreviating $V_{12} := \mathbb{F}(\vec{v}_1 - \vec{v}_2)$ and $V_{23} := \mathbb{F}(\vec{v}_2 - \vec{v}_3)$ and $V_{13} := \mathbb{F}(\vec{v}_1 - \vec{v}_3)$, we have for $r,s \in \mathbb{F}$:*

a) $\mathbb{F}(\vec{v}_1 - rs\vec{v}_2) \;=\; V_3 \times \big[\mathbb{F}(\vec{v}_3 - r\vec{v}_2) \times \mathbb{F}(\vec{v}_1 - s\vec{v}_3)\big]$

b) $\mathbb{F}(\vec{v}_1 - s\vec{v}_3) \;=\; V_2 \times \big[V_{23} \times \mathbb{F}(\vec{v}_1 - s\vec{v}_2)\big]$

c) $\mathbb{F}(\vec{v}_3 - r\vec{v}_2) \;=\; V_1 \times \big[V_{13} \times \mathbb{F}(\vec{v}_1 - r\vec{v}_2)\big]$

d) $\mathbb{F}\big(\vec{v}_1 - (r-s)\vec{v}_2\big) \;=\; V_3 \times \Big[\big([V_{23} \times \mathbb{F}(\vec{v}_1 - r\vec{v}_2)] \times [V_2 \times \mathbb{F}(\vec{v}_1 - s\vec{v}_3)]\big) \times V_3\Big]$

e) $V_{13} \;=\; V_2 \times (V_{12} \times V_{23})$.

f) For $W \in \mathbb{P}^2(\mathbb{F})$, the expression $\iota(W) := (W \times V_3) \times \Big(\big((W \times V_3) \times V_3\big) \times V_2\Big)$ is defined precisely when $W = \mathbb{F}(\vec{v}_1 - r\vec{v}_2 + s\vec{v}_3)$ for some $s \in \mathbb{F}$ and a unique $r \in \mathbb{F}$; and in this case $\iota(W) = \mathbb{F}(\vec{v}_1 - r\vec{v}_2)$. Moreover, if $W = \mathbb{F}(\vec{v}_1 - r\vec{v}_2)$ then $\iota(W) = W$.

Note that the V_j here do not denote variables but elements of $\mathbb{P}^2(\mathbb{F})$. Concerning the proof of Lemma Lemma 8, e.g. for a) observe that $\vec{v}_1 - rs\vec{v}_2 = \vec{v}_1 - s\vec{v}_3 - s(\vec{v}_3 - r\vec{v}_2)$ is orthogonal to V_3 and contained in the plane spanned by $\vec{v}_3 - r\vec{v}_2$. In d) one applies 3) of Fact 7 with subterm W evaluating to $\mathbb{F}(\vec{v}_1 - (r - s)\vec{v}_2 - s\vec{v}_3)$ in view of 2). For f) observe that, if W lies in the V_2–V_3–plane, its projection $(W \times V_3) \times V_3$ according to 3) coincides with V_2 (corresponding to slope $r = \pm\infty$) and renders the entire term undefined; whereas for W not in the V_2–V_3–plane, $\big((W \times V_3) \times V_3\big) \times V_2$ coincides with V_3.

Let us abbreviate $\bar{V} := (V_1, V_2, V_3, V_{12}, V_{23})$ derived from an orthogonal basis $\vec{v}_1, \vec{v}_2, \vec{v}_3$ as above. In terms of von Staudt's encoding of elements $r \in \mathbb{F}$ as projective points $\Theta_{\bar{V}}(r) := \mathbb{F}(\vec{v}_1 - r\vec{v}_2) \perp \mathbb{F}\vec{v}_3$, Lemma 8a+d) demonstrate how to express the ring operations using only the crossproduct; note that $r + s = r - (0 - s)$ where $0 \in \mathbb{F}$ is encoded as V_1. Lemma 8a) involves two other encodings such as $\mathbb{F}(\vec{v}_1 - s\vec{v}_3)$, but Lemma 8b+c) exhibit how to express these using the cross product and $\Theta_{\bar{V}}$ only as well as V_{23} and V_{13}. V_{13} can even be disposed off by means of Lemma 8e). Plugging b)+c)+e) into a) and d), we conclude that there exist cross product terms $\ominus(R,S;\bar{V})$ and $\otimes(R,S;\bar{V})$ in variables R, S with constants $\bar{V} = \big(V_1 = \Theta_{\bar{V}}(0), V_2, V_3, V_{12} = \Theta_{\bar{V}}(1), V_{23}\big)$ as above such that for every $r,s \in \mathbb{F}$ it holds $\Theta_{\bar{V}}(rs) = \otimes\big(\Theta_{\bar{V}}(r), \Theta_{\bar{V}}(s); \bar{V}\big)$ and $\Theta_{\bar{V}}(r - s) = \ominus\big(\Theta_{\bar{V}}(r), \Theta_{\bar{V}}(s); \bar{V}\big)$

Now any polynomial $p \in \mathbb{F}[X_1, \ldots, X_n]$ is composed, using the two ring operations, from variables and coefficients from $\mathbb{F}$. More precisely, according to Lemma 8, the above encoding extends to a mapping $\Theta_{\bar{V}}$ assigning, to any ring term $p(X_1, \ldots, X_n)$ with constants $c \in \mathbb{F}$, some cross product term t_p in variables $X_1, \ldots, X_n$ with constants $\Theta_{\bar{V}}(c) \in \mathbb{P}^2(\mathbb{F})$ and constants $V_1, V_2, V_3, V_{12}, V_{23} \in \mathbb{P}^2(\mathbb{F})$; moreover $\Theta_{\bar{V}}$ 'commutes' with the map $p \mapsto t_p$ in the sense that

$$t_p\big(\Theta_{\bar{V}}(x_1), \ldots, \Theta_{\bar{V}}(x_n)\big) \;=\; \Theta_{\bar{V}}\big(p(x_1, \ldots, x_n)\big) \quad . \tag{2}$$

Since t_p is defined by structural induction over p using the constant-size terms from Lemma 8, it can be evaluated by a BSS machine in time polynomial in the description length of the ring term p.

Moreover by Lemma 8f) precisely the $\iota_{\bar{V}}(W)$ are images under $\Theta_{\bar{V}}$. Thus, every satisfying assignment to the cross product equation

$$t'_p \;:=\; \Big(t_p\big(\iota(X_1), \ldots, \iota(X_n)\big) \;=\; V_1\Big) \tag{3}$$

comes from a root $(r_1, \ldots, r_n)$ of p; namely the unique r_j such that $X_j = \mathbb{F}(\vec{v}_1 + r_j\vec{v}_2 + s_j\vec{v}_3)$. Conversely, given a root $(r_1, \ldots, r_n)$ of p, $X_j := \Theta_{\bar{V}}(r_j)$ yields a a satisfying assignment for the equation $t'_p = V_1$.

Similarly, (the partial map given by) $t'_p \times V_1$ is nontrivial iff p is not identically zero. We have thus proved Claim i).

In order to establish also the remaining Claims ii) and iii) we turn every d-variate ring term p with coefficients $0, \pm 1$ into an 'equivalent' cross product term t''_p with*out* constants and in particular avoiding explicit reference to the fixed $V_1, V_2, V_3, V_{12}, V_{23}$ from Lemma 8 based on the following

Observation 9. *Fix a subfield* $\mathbb{F}$ *of* $\mathbb{R}$. *To* $A, B, C \in \mathbb{P}^2(\mathbb{F})$ *consider*

$$V_{12} := B \quad V_2 := (A \times B) \times A \quad V_{23} := C \times A \quad V_1 := V_2 \times V_{23} \quad V_3 := \big(V_{23} \times (B \times V_2)\big) \times B \qquad (4)$$

a) These may be undefined in cases such as $A = B$ *(whence* $V_2 = \perp$*) or when* $A, C, A \times B$ *are collinear (thus* $V_{23} = V_2$ *and* $V_1 = \perp$*) or when* A, B, C *are collinear (where* $V_{23} = A \times B$ *and* $V_3 = \perp$*) or when* $A \perp B$ *(where* $B = V_2$ *and* $V_3 = \perp$*).*

b) On the other hand for example $A := \mathbb{F}\vec{v}_1$, $B := \mathbb{F}(\vec{v}_2 - \vec{v}_1)$ *and* $C := \mathbb{F}(\vec{v}_2 + \vec{v}_3)$*, defined in terms of an orthogonal basis, recover* $V_1, V_2, V_3, V_{12}, V_{23}$ *from Lemma 8.*

c) Conversely when all quantities in Eq. (4) are defined, then $V_1 = A$ *and there exists a right-handed orthogonal basis* $\vec{v}_1, \vec{v}_2, \vec{v}_3$ *of* $\mathbb{F}^3$ *such that* $V_j = \mathbb{F}\vec{v}_j$ *and* $V_{12} = \mathbb{F}(\vec{v}_1 - \vec{v}_2)$ *and* $V_{23} = \mathbb{F}(\vec{v}_2 - \vec{v}_3)$*.*

We may thus replace the tuple of projective constants $\bar{V}$ in the above reduction $p \mapsto t_p$ mapping a ring term $p(X_1, \dots, X_n)$ to a cross product term $t_p(X_1, \dots, X_n; \bar{V})$ with the subterms $V_1(A,B,C), \dots, V_{23}(A,B,C)$ (considering A, B, C as variables) according to Observation 9 to obtain a constant free cross product term $t''_p(X_1, \dots, X_n; A, B, C)$ such that the map $p \mapsto t''_p$ commutes with $\Theta_{\bar{V}}$ for any projective assignment on which t''_p is defined and $\bar{V}(A,B,C)$ given by the values of the subterms V_i, V_{ij}.

Now let $\iota(X)$ denote the constant free term from Lemma 8g) in variables X, A, B, C (with subterms V_i as above). Then, from each satisfying assignment to $t'''_p := t''_p\big(\iota(X_1), \dots, \iota(X_n); A, B, C\big) = A$ one obtains as previously again a root $(r_1, \dots, r_n)$ of p: Observation 9c) justifies reusing the reasoning given in the case with constants. Conversely, given a root $(r_1, \dots, r_n)$ of p, evaluate A, B, C according to Observation 9b) and $X_j := \Theta_{\bar{V}}(r_j)$ to obtain a satisfying assignment for the equation $t'''_p = A$. Since the translation $p \mapsto t''_p$ can be carried out by structural induction in time polynomial in the description length of p, this establishes Claim ii). To deal with iii), consider $t'''_p \times A$. □

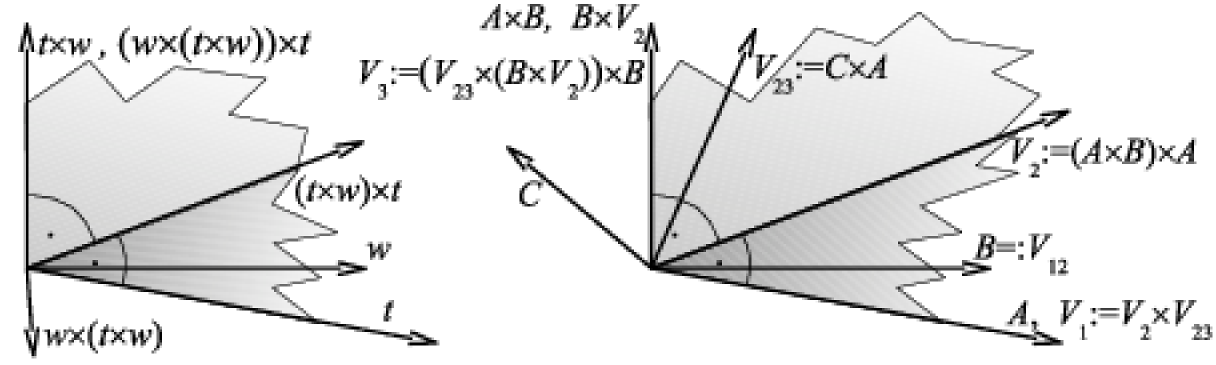

Figure 1: Illustrating the geometry of the terms considered a) in the reduction from $\mathsf{XSAT}^0_{\mathbb{P}^2(\mathbb{R})}$ to $\mathsf{XSAT}^0_{\mathbb{R}^3}$ and b) in Observation 9c.

Proof of Observation 9c). By construction, affine lines A and $A \times B$ and V_2 are pairwise orthogonal; see Fig. 1b). Moreover $A \neq B$ because $A \times B$ a subterm of V_2 is defined by hypothesis. Since both V_2 and

$V_{23} = C \times A$ are orthogonal to A, their projective cross product V_1 must coincide with A whenever defined and in particular $V_2 \neq V_{23}$; moreover V_2 and V_{23} and $A \times B$ lie in a common plane. $B \times V_2$ as subterm of V_3 being defined requires $V_2 \neq B$; yet these two and $A = V_1$ are orthogonal to $A \times B$ and thus lie in a common plane. In particular $B \times V_2 = A \times B$. Finally, V_{23} and $B \times V_2 = A \times B$ both being orthogonal to A, their defined cross product as subterm of V_3 requires $V_{23} \neq B \times V_2$ and $V_3 = B \times V_2 = A \times B$. To summarize: V_1, V_2, V_3 are pairwise orthogonal; and V_1, V_{12}, V_2 are pairwise distinct yet all orthogonal to V_3; similarly V_2, V_{23}, V_3 are pairwise distinct yet all orthogonal to V_1. Now choose $0 \neq \vec{v}_1 \in V_1$ arbitrary and $\vec{v}_2 \in V_2$ such that $V_{12} = \mathbb{F}(\vec{v}_1 - \vec{v}_2)$; finally choose $\vec{v}_3 \in V_3$ such that $V_{23} = \mathbb{F}(\vec{v}_2 - \vec{v}_3)$. If these pairwise orthogonal vectors $\vec{v}_1, \vec{v}_2, \vec{v}_3$ happen to form a left-handed system, simply flip all their signs. □

4 Conclusion

We have identified a new problem complete (i.e. universal) for nondeterministic polynomial-time BSS machines, namely from exterior algebra: the satisfiability of a single equation built only by iterating cross products. This enriches algebraic complexity theory and emphasizes the importance of the Turing (!) complexity class $\mathbf{BP}(\mathbf{NP}^0_{\mathbb{R}})$.

Moreover our proof yields a cross product equation $t'''_{X^2=2}(Y,A,B,C) = A$ solvable over $\mathbb{P}^2(\mathbb{R})$ but not over $\mathbb{P}^2(\mathbb{Q})$, the rational projective plane. In fact the decidability of $\mathsf{XSAT}^0_{\mathbb{P}^2(\mathbb{Q})}$ is equivalent to a long-standing open question [Poon09].

We wonder about the computational complexity of equations over the 7-dimensional cross product.

References

[BaMe13] M. Baartse, K. Meer: "The PCP Theorem for **NP** over the reals", pp.104–115 in *Proc. 30th Symp. on Theoret. Aspects of Computer Science* (STACS'13), Dagstuhl LIPIcs vol.**20**. doi:10.4230/LIPIcs.STACS.2013.104
Full version to appear in *Contemporary Mathematics*, American Mathematical Society.

[BCSS98] L. Blum, F. Cucker, M. Shub, S. Smale: "*Complexity and Real Computation*", Springer (1998).

[BKOS97] M. de Berg, M. van Kreveld, M. Overmars, O. Schwarzkopf: "*Computational Geometry, Algorithms and Applications*", Springer (1997).

[BSS89] L. Blum, M. Shub, S. Smale: "On a Theory of Computation and Complexity over the Real Numbers: **NP**–completeness, Recursive Functions, and Universal Machines", pp.1–46 in *Bulletin of the American Mathematical Society* (AMS Bulletin) vol.**21** (1989). doi:10.1090/S0273-0979-1989-15750-9

[Bürg00] P. Bürgisser: "*Completeness and Reduction in Algebraic Complexity Theory*", Springer (2000)

[BüSc09] P. Bürgisser, P. Scheiblechner: "On the Complexity of Counting Components of Algebraic Varieties", pp.1114–1136 in *Journal of Symbolic Computation* vol.**44:9** (2009). doi:10.1016/j.jsc.2008.02.009

[Cann88] J. Canny: "Some Algebraic and Geometric Computations in **PSPACE**", pp.460–467 in *Proc. 20th annual ACM Symposium on Theory of Computing* (SToC 1988). doi:10.1145/62212.62257

[Cuck93] F. Cucker: "On the Complexity of Quantifier Elimination: the Structural Approach", pp.400–408 in *The Computer Journal* vol.**36:5** (1993). doi:10.1093/comjnl/36.5.400

[CuRo92] F. Cucker, F. Rosselló: "On the Complexity of Some Problems for the Blum, Shub & Smale model", pp.117–129 in *Proc. LATIN'92*, Springer LNCS vol.**583**. doi:10.1007/BFb0023823

[GaJo79] M.R. GAREY, D.S. JOHNSON: "*Computers and Intractability: A Guide to the Theory of* **NP***–completeness*", Freeman (1979).

[Gius91] M. GIUSTI, J. HEINTZ: "Algorithmes – disons rapides – pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles", pp.169–193 in *Effective Methods in Algebraic Geometry (Proceedings of MEGA'90)*, T. Mora and C. Traverso editors, Birkhäuser (1991).

[Grig88] D.Y. GRIGORIEV: "Complexity of Deciding Tarski Algebra", pp.65–108 in *Journal of Symbolic Computation* vol.**5** (1988). doi:10.1016/S0747-7171(88)80006-3

[HaSv96] H. HAVLICEK, K. SVOZIL: "Density Conditions for Quantum Propositions", pp.5337–5341 in *Journal of Mathematical Physics* vol.**37** (1996). doi:10.1063/1.531738

[HeZi11] C. HERRMANN, M. ZIEGLER: "Computational Complexity of Quantum Satisfiability", pp.175–184 in *Proc. 26th Annual IEEE Symposium on Logic in Computer Science* (2011). doi:10.1109/LICS.2011.8

[HRS90] J. HEINTZ, M.-F. ROY, P. SOLERNÓ: "Sur la complexité du principe de Tarski–Seidenberg", pp.101–126 in *Bull. Soc. Math. France* vol.**118** (1990).

[Koir99] P. KOIRAN: "The Real Dimension Problem is $\mathbf{NP}_{\mathbb{R}}$–complete", pp.227–238 in *J. Complexity* vol.**15:2** (1999). doi:10.1006/jcom.1999.0502

[Lece00] G. LECERF: "Computing an Equidimensional Decomposition of an Algebraic Variety by means of Geometric Resolutions", pp.209–216 in *Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation* (ISSAC), ACM. doi:10.1145/345542.345633

[MeMi97] K. MEER, C. MICHAUX: "A Survey on Real Structural Complexity Theory", pp.113–148 in *Bulletin of the Belgian Mathematical Society* vol.**4** (1997).

[MR95] R. MOTVANI, P. RAGHAVAN: "*Randomized Algorithms*", Cambridge University Press (1995).

[Poon09] B. POONEN: "Characterizing Integers among Rational Numbers with a Universal-Existential Formula", in *American Journal of Mathematics* vol.**131:3** (2009).

[Rene92] J. RENEGAR: "On the Computational Complexity and Geometry of the First-order Theory of the Reals", pp.255–352 in *Journal of Symbolic Computation* vol.**13:3** (1992). doi:10.1016/S0747-7171(10)80003-3 doi:10.1016/S0747-7171(10)80004-5 doi:10.1016/S0747-7171(10)80005-7

[Rich99] J. RICHTER-GEBERT: "The Universality Theorems for Oriented Matroids and Polytopes", pp.269–292 in *Contemporary Mathematics* vol.**223** (1999). doi:10.1090/conm/223/03144

[Scha10] M. SCHAEFER: "Complexity of Some Geometric and Topological Problems", pp.334–344 in *Proc. 17th Int. Symp. on Graph Drawing*, Springer LNCS vol.**5849** (2010). doi:10.1007/978-3-642-11805-0_32

[Shor91] P. SHOR: "Stretchability of Pseudolines is **NP**–hard", pp.531–554 in *Applied Geometry and Discrete Mathematics — The Victor Klee Festschrift* (P. Gritzmann and B. Sturmfels Edts), DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol.**4** (1991). doi:10.1007/BF03025291

[Smal98] S. SMALE: "Mathematical Problems for the Next Century", pp.7–15 in *Math. Intelligencer* vol.**20:2** (1998).

[Zhan92] X.-D. ZHANG: "Complexity of Neural Network Learning in the Real Number Model", pp.146–149 in *Proc. Workshop on Physics and Computation* (1992). doi:10.1109/PHYCMP.1992.615511