An Approach to the Set Partition Problem

Alexandr V. Seliverstov

Abstract. The article focuses on methods to confirm the smoothness of some cubic hypersurfaces that are closely related to the set partition problem.

Let us recall the set partition problem [1]. Given a multiset of positive integers $\{\alpha_0, \ldots, \alpha_n\}$. Can it be partitioned into two subsets with equal sums of elements? Points with coordinates ± 1 are called $(-1,1)$-points. The problem is to recognize whether a $(-1,1)$-point belongs to the hyperplane given by the linear equation $\alpha_0 + \alpha_1 x_1 + \cdots + \alpha_n x_n = 0$. It is hard to find a $(-1,1)$-point belonging to the hyperplane in high dimensions [2]. On the other hand, one can find $(-1,1)$-points belonging to the hyperplane given by a linear function with integer coefficients near zero, using dynamic programming [1].

Let us consider an affine hypersurface $\mathcal{F}$ that is the vanishing locus of a square-free polynomial f. A straight line passing through the selected point $U \in \mathcal{F}$ is the set of points with coordinates $((x_1 - u_1)t + u_1, \ldots, (x_n - u_n)t + u_n)$, where $(u_1, \ldots, u_n)$ are coordinates at U, and t is a parameter. Let us denote by $r(t)$ a univariate polynomial that is the restriction of the polynomial f to the line, and by $B[f,U]$ the discriminant of $r(t)/t$. Since $r(0) = 0$, $r(t)/t$ is a polynomial of degree at most $d-1$, where $d = \deg f$. If $\deg r(t) < d-1$, then we use the formula for degree $d-1$ by means of substitution the zero as the leading coefficient. If the point U is smooth, then $B[f,U](x_1, \ldots, x_n)$ defines a cone.

Let us denote by $\mathbb{K}$ a finite extension of the field of rational numbers $\mathbb{Q}$. Any smooth cubic curve is not unirational. In accordance with [3], for each cubic surface as well as high dimensional hypersurface $\mathcal{X}$ defined over $\mathbb{K}$, if $\mathcal{X}$ is irreducible, $\mathcal{X}$ is not a cone, and $\mathcal{X}$ contains a $\mathbb{K}$-point, then $\mathcal{X}$ is unirational over $\mathbb{K}$. That is, we have not only a lot of $\mathbb{K}$-points but also a rational map from the set of $\mathbb{Q}$-points of the affine space to the set of $\mathbb{K}$-points of $\mathcal{X}$. The explicit parameterizations of the Clebsch diagonal surface as well as the Fermat cubic surface are exemplified in [4]. Both surfaces are rational over $\mathbb{Q}$.

Let us denote $f = \alpha_0 + \alpha_1 x_1^3 + \cdots + \alpha_n x_n^3$ and $h = \alpha_0 + \alpha_1 x_1 + \cdots + \alpha_n x_n$, where all coefficients $\alpha_0, \ldots, \alpha_n$ are nonzero. $\mathcal{F}$ denotes the affine cubic hypersurface given by the equation $f = 0$ as well as $\mathcal{H}$ denotes the hyperplane given by $h = 0$. The following theorem improves the result from [5] in case of cubic hypersurfaces.

Theorem 1. *Given a multiset of positive integers $\{\alpha_0, \ldots, \alpha_n\}$. There exists a one-to-one correspondence between singular points of the hyperplane section $\mathcal{F} \cap \mathcal{H}$ and $(-1, 1)$-points belonging to the hyperplane $\mathcal{H}$.*

Proof. If both polynomials f and h vanish simultaneously at a $(-1, 1)$-point, then the hyperplane $\mathcal{H}$ is tangent to the hypersurface $\mathcal{F}$ at this point. Thus, the hyperplane section is singular. Contrariwise, at a singular point of the section, the hyperplane $\mathcal{H}$ coincides with the tangent hyperplane to the hypersurface $\mathcal{F}$. Since all the coefficients α_k are nonzero, both gradients ∇f and ∇h can be collinear only at the points whose coordinates satisfy the system of the equations $x_k^2 = x_j^2$ for all indices k and j. All the points are $(-1, 1)$-points. □

The polynomial $B[f, U]$ is equal to the discriminant of a univariate polynomial $at^2 + bt + c$. That is, $B[f, U] = b^2 - 4ac$, where the coefficients are sums of univariate polynomials $a = a_1(x_1) + \cdots + a_n(x_n)$, $b = b_1(x_1) + \cdots + b_n(x_n)$, and $c = c_0 + c_1x_1 + \cdots + c_nx_n$. Each monomial from $B[f, U](x_1, \ldots, x_n)$ is dependent on at most two variables.

Let us consider the factor ring $\mathbb{K}[x_1, \ldots, x_n]/\langle x_1^2 - 1, \ldots, x_n^2 - 1\rangle$. It is referred to as the set of multilinear polynomials. In this way, we have a surjective map φ from the set of all polynomials onto the set of multilinear polynomials.

Let us denote by $M[f, U](x_1, \ldots, x_{n-1})$ a multilinear polynomial that is an image of the restriction to the hyperplane $\mathcal{H}$ of the multilinear polynomial $\varphi(B[f, U])$. The restriction to the hyperplane $\mathcal{H}$ means that we substitute $x_n = -(\alpha_0 + \alpha_1x_1 + \cdots + \alpha_{n-1}x_{n-1})/\alpha_n$. Let us denote by $\mathcal{L}$ a linear space spanned by all multilinear polynomials $M[f, U](x_1, \ldots, x_{n-1})$, where $U \in \mathcal{F} \cap \mathcal{H}$.

A polynomial vanishes at a $(-1, 1)$-point if and only if its multilinear image vanishes at this point. Thus, if the hyperplane $\mathcal{H}$ contains a $(-1, 1)$-point, then all multilinear polynomials from $\mathcal{L}$ vanish at the point. Contrariwise, if a nonzero constant belongs to the linear space $\mathcal{L}$, then $\mathcal{H}$ does not contain any $(-1, 1)$-point. In the case, $\mathcal{F} \cap \mathcal{H}$ is smooth.

In case $n = 2$, let us consider values $\alpha_0 = 1$, $\alpha_1 = 3$, and $\alpha_2 = 2$. The intersection $\mathcal{F} \cap \mathcal{H}$ consist of two points $U(-1, 1)$ and $V(\frac{1}{5}, -\frac{4}{5})$. The multilinear polynomial $\varphi(B[f, U]) = -72x_2x_1 - 48x_2 - 144x_1 - 168$. The substitution $x_2 = -\frac{3x_1+1}{2}$ yields a univariate polynomial $108x_1^2 - 36x_1 - 144$. Its multilinear image $M[f, U] = -36x_1 - 36$. At the second point V the multilinear polynomial

$$M[f, V] = \frac{26172}{3125}x_1 + \frac{428292}{15625}.$$

Two polynomials $M[f, U]$ and $M[f, V]$ together span the whole linear space of univariate linear polynomials. The same holds for almost all values α_1 and α_2 because $\dim \mathcal{L}$ is a lower semi-continuous function.

Contrariwise, if $n = 2$ and $\alpha_0 = \alpha_1 = \alpha_2 = 1$, then $\dim \mathcal{L} = 1$. The intersection $\mathcal{F} \cap \mathcal{H}$ consist of two points $U(0, -1)$ and $V(-1, 0)$. The third point does not belong to the affine plane. So, $B[f, U] = -12x_1x_2 - 24x_2 - 12x_1 - 24$; the multilinear polynomial $M[f, U] = 24x_1 + 12$. On the other hand, at the point V the polynomial $B[f, V] = -12x_1x_2 - 12x_2 - 24x_1 - 24$; the multilinear polynomial $M[f, V]$ vanishes identically. Thus, the linear space $\mathcal{L}$ is a proper subspace in the two-dimensional space of univariate linear polynomials.

If $n = 4$ and $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = \alpha_4$, then $\dim \mathcal{L} = 1$. The space $\mathcal{L}$ is spanned by one polynomial $2(x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + x_3) + 3$. In the case, the intersection $\mathcal{F} \cap \mathcal{H}$ coincides with the Clebsch diagonal surface.

On the other hand, if $n = 4$, $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 1$, and a large integer $\alpha_4 \gg 1$, then $\dim \mathcal{L} \geq 5$. At the limit $\alpha_n \to \infty$ the intersection $\mathcal{F} \cap \mathcal{H}$ converges to the Fermat surface inside the coordinate hyperplane $x_4 = 0$. The corresponding linear space contains five linearly independent polynomials. Thus, the same holds true for all sufficiently large integers α_4.

The examples have been computed by means of the service MathPartner [6].

Let us define

$$\lambda(n) = \frac{n(n+1)}{2} + 1$$

that is the upper bound on $\dim \mathcal{L}$. In case $\alpha_0 = \alpha_1$, the section $\mathcal{F} \cap \mathcal{H}$ contains the point $(-1, 0, \dots, 0)$. Thus, for all $n \geq 4$, if $\mathcal{F} \cap \mathcal{H}$ is not a cone, then there exists a rational parametrization $\eta : \mathbb{Q}^{n-2} \dashrightarrow \mathcal{F} \cap \mathcal{H}$ defined over $\mathbb{Q}$, cf. [3]. Let the point $(-1, 0, \dots, 0)$ be the image of the locus of indeterminacy; η can be found in probabilistic polynomial time.

If the section $\mathcal{F} \cap \mathcal{H}$ contains a point over the field $\mathbb{K}$, then there exists a rational parametrization $\eta : \mathbb{K}^{n-2} \dashrightarrow \mathcal{F} \cap \mathcal{H}$ defined over $\mathbb{K}$. Let the initial $\mathbb{K}$-point be the image of the locus of indeterminacy.

Theorem 2. *Given a multiset of positive integers $\alpha_0, \dots, \alpha_n$, where $n \geq 4$ and $\mathcal{F} \cap \mathcal{H}$ is not a cone, and a real $\varepsilon > 0$. Let us consider the multilinear polynomials $M[f, \eta(P^{(k)})]$ for random points $P^{(k)}$, where the index k runs the segment $1 \leq k \leq \lambda(n)$, and all coordinates of the points $P^{(k)}$ are independent and uniformly distributed on the set of integers from one to $\lceil 2^{poly(n)}/\varepsilon \rceil$. The probability of spanning the whole linear space $\mathcal{L}$ is at least $1 - \varepsilon$.*

Proof. It is based on the Schwartz–Zippel lemma [7]. □

Thus, in case $n \geq 4$ and $\mathcal{F} \cap \mathcal{H}$ is not a cone, a basis of the linear space $\mathcal{L}$ can be computed in probabilistic polynomial time. In this way, the algorithm tries to find a rational parametrization $\eta : \mathbb{K}^{n-2} \dashrightarrow \mathcal{F} \cap \mathcal{H}$; if it failed because $\mathcal{F} \cap \mathcal{H}$ is a cone, then there exists a singular point. To prove the instance of the set partition problem has no solution, it is sufficient to check whether a nonzero constant belongs to the linear space $\mathcal{L}$. Of course, the condition is not necessary. On the other hand, if the linear space $\mathcal{L}$ contains a linear polynomial, one can reduce the dimension of the initial task.

References

[1] A. Schrijver, *Theory of linear and integer programming.* John Wiley and Sons, 1986.

[2] S. Margulies, S. Onn, and D.V. Pasechnik, On the complexity of Hilbert refutations for partition. *J. Symbolic Comput.* 66, 70–83 (2015). DOI:10.1016/j.jsc.2013.06.005

[3] J. Kollár, Unirationality of cubic hypersurfaces. *J. Inst. Math. Jussieu* 1:3, 467–476 (2002). DOI:10.1017/S1474748002000117

[4] I. Polo-Blanco, J. Top, A remark on parameterizing nonsingular cubic surfaces. *Computer Aided Geometric Design* 26, 842–849 (2009). DOI:10.1016/j.cagd.2009.06.001

[5] I.V. Latkin, A.V. Seliverstov, Computational complexity of fragments of the theory of complex numbers (in Russian). *Bull. Univ. Karaganda. Ser. Math.* 1, 47–55 (2015).

[6] G.I. Malaschonok, New generation of symbolic computation systems (in Russian). *Tambov University Reports. Series: Natural and Technical Sciences* 21:6, 2026–2041 (2016). DOI:10.20310/1810-0198-2016-21-6-2026-2041

[7] J.T. Schwartz, Fast probabilistic algorithms for verification of polynomial identities. *J. ACM* 27:4, 701–717 (1980). DOI:10.1145/322217.322225

Alexandr V. Seliverstov
Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute), Moscow, Russia
e-mail: `slvstv@iitp.ru`