



HAL
open science

How Far From a Worst Solution a Random Solution of a k CSP Instance Can Be?

Jean-François Culus, Sophie Toulouse

► **To cite this version:**

Jean-François Culus, Sophie Toulouse. How Far From a Worst Solution a Random Solution of a k CSP Instance Can Be?. International Workshop on Combinatorial Algorithms, Jul 2018, Singapore, Singapore. hal-02350145

HAL Id: hal-02350145

<https://hal.univ-antilles.fr/hal-02350145v1>

Submitted on 5 Nov 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

How Far From a Worst Solution a Random Solution of a k CSP Instance Can Be?

Jean-François Culus¹ and Sophie Toulouse² ✉

¹ CEREGMIA, Université des Antilles, France
jean-francois-culus@espe-martinique.fr

² LIPN (UMR CNRS 7030), Institut Galilée, Université Paris 13, France
sophie.toulouse@lipn.univ-paris13.fr

Abstract. Given an instance I of an optimization constraint satisfaction problem (CSP), finding solutions with value at least the expected value of a random solution is easy. We wonder how good such solutions can be. Namely, we initiate the study of ratio $\rho_E(I) = (\mathbb{E}_X[v(I, X)] - \text{wor}(I)) / (\text{opt}(I) - \text{wor}(I))$ where $\text{opt}(I)$, $\text{wor}(I)$ and $\mathbb{E}_X[v(I, X)]$ refer to respectively the optimal, the worst, and the average solution values on I . We here focus on the case when the variables have a domain of size $q \geq 2$ and the constraint arity is at most $k \geq 2$, where k, q are two constant integers. Connecting this ratio to the highest frequency in orthogonal arrays with specified parameters, we prove that it is $\Omega(1/n^{k/2})$ if $q = 2$, $\Omega(1/n^{k-1 - \lceil \log_{p^\kappa}(k-1) \rceil})$ where p^κ is the smallest prime power such that $p^\kappa \geq q$ otherwise, and $\Omega(1/q^k)$ in $(\max\{q, k\} + 1)$ -partite instances.

Keywords: Average differential ratio · Optimization constraint satisfaction problems · Orthogonal arrays

1 Introduction

Given an integer $q \geq 2$, an optimization *Constraint Satisfaction Problem* (CSP) over $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ considers a set $\{x_1, \dots, x_n\}$ of \mathbb{Z}_q -valued variables and a set $\{C_1, \dots, C_m\}$ of constraints, where a constraint consists of the application of a (non constant) predicate $P_i : \mathbb{Z}_q^{k_i} \rightarrow \{0, 1\}$ to a tuple $x_{J_i} = (x_{i_1}, \dots, x_{i_{k_i}})$ of variables. The goal is then to assign values to the variables so as to satisfy either as many, or as few constraints as possible. For instance, in the *Maximum Satisfiability Problem* (Max Sat), the goal is to satisfy as many disjunctive clauses as possible. In *Min Lin-q*, the goal is to satisfy as few equations of a system of linear equations modulo q as possible.

Most often, a positive weight w_i is associated with each constraint C_i . Given a positive integer N , we represent by $[N]$ the discrete interval $\{1, \dots, N\}$. The goal is then to optimize an objective function of the form

$$\sum_{i=1}^m w_i C_i = \sum_{i=1}^m w_i P_i(x_{J_i}) = \sum_{i=1}^m w_i P_i(x_{i_1}, \dots, x_{i_{k_i}})$$

over \mathbb{Z}_q^n where for all $i \in [m]$: $k_i \in [n]$, $P_i : \mathbb{Z}_q^{k_i} \rightarrow \{0, 1\}$, $J_i = (i_1, \dots, i_{k_i}) \subseteq [n]$ and $w_i > 0$. The special case when functions P_i all belong to a specific family \mathcal{F}

of functions is referred to as $\text{CSP}(\mathcal{F})$ in the literature. Given a predicate P , the restriction to constraints of the form $P(x_{J_i} + v_i)$ where v_i is a constant vector is referred to as CSP-P . For example, given a positive integer k , XOR^k is the k -ary boolean predicate that accepts entries (y_1, \dots, y_k) with $y_1 + \dots + y_k \equiv 1 \pmod 2$; then $\text{Lin-2} = \text{CSP-}\{\text{XOR}^k \mid k \in \mathbb{N}^*\} = \text{CSP}(\{\text{XOR}^k, 1 - \text{XOR}^k \mid k \in \mathbb{N}^*\})$.

We here consider the slight generalization where functions P_i may be real-valued. In the sequel, we denote by CSP-q the corresponding problem, and by $k \text{CSP-q}$ (*resp.*, EkCSP-q) the special case when every constraint depends on at most (*resp.*, exactly) k variables, where k is a universal constant integer. As $k \text{CSP-q}$ is **NP-hard** even in case when $q = k = 2$ [9], a major issue as regards optimization CSPs consists in charactering their approximation degree.

1.1 Around the Average Solution Value

Thereafter, given an instance I of CSP-q , we denote by $v(I, \cdot)$ its objective function, by $w(I) = \sum_{i=1}^m w_i$ the total weight on I , by $\text{opt}(I)$ and $\text{wor}(I)$ respectively the optimum and the worst solution values on I . It is convenient to think of the average solution value on I as the expected value $\mathbb{E}_X[v(I, X)]$ of a random solution where $X = (X_1, \dots, X_n)$ is a vector of pairwise independent random variables, each uniformly distributed over \mathbb{Z}_q . This value expresses as:

$$\mathbb{E}_X[v(I, X)] = \sum_{i=1}^m w_i \mathbb{E}_X[P_i(X_{J_i})] = \sum_{i=1}^m w_i r_{P_i}$$

where given $i \in [m]$, r_{P_i} refers to the average value of P_i over $\mathbb{Z}_q^{k_i}$. For example, on an instance I of Lin-2 , the average solution value equals $w(I)/2$.

Solutions with value at least $\mathbb{E}_X[v(I, X)]$ are computationally easy to find, *e.g.* using the conditional expectation technique [13]. Therefore, two questions can naturally be asked: is it possible to compute within polynomial time solutions that beat the average solution value, and what is the gain of the average solution value over the worst solution value?

The former question notably leads to the concept of approximation of the *advantage over a random assignment* [11], herein referred to as *gain approximation*. The advantage of a given solution x over a random assignment is the difference $v(I, x) - \mathbb{E}_X[v(I, X)]$ if one maximizes, $\mathbb{E}_X[v(I, X)] - v(I, x)$ if one minimizes. Given $\rho \in]0, 1]$, x approximates the optimum gain $|\text{opt}(I) - \mathbb{E}_X[v(I, X)]|$ over $\mathbb{E}_X[v(I, X)]$ within factor ρ *iff* x achieves a *gain ratio*

$$\rho_G(I, x) = \frac{v(I, x) - \mathbb{E}_X[v(I, X)]}{\text{opt}(I) - \mathbb{E}_X[v(I, X)]} \quad (1)$$

at least ρ . A given CSP Π is ρ -*gain approximable* (where ρ possibly depends on parameters of the considered instance I) if it is possible to compute within polynomial time on every instance I of Π a solution with gain ratio at least $\rho(I)$. The corresponding issue consists in determining “the best” ρ for which Π is ρ -gain approximable. Håstad and Venkatesh introduced in [11] this approximation measure motivated by the fact that for numerous predicates P , for all constant $\varepsilon > 0$, finding solutions with value at least $(r_P + \varepsilon)w(I)$ on almost satisfiable

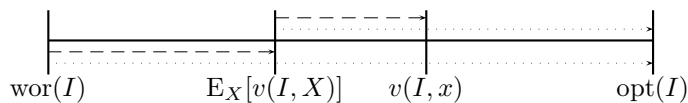


Fig. 1. Quantities involved in $\rho_G(I, x)$ and $\rho_E(I)$.

instances of **Max CSP-P** is **NP-hard**. For example, for all $k \geq 3$, XOR^k is such a predicate [10]. Thus for all $k \geq 3$, **kLin-2** is **NP-hard** to approximate to within any constant gain factor. It is, though, approximable within an expected gain factor of $\Omega(\sqrt{1/m})$ [11].

The latter question leads to the notion of *advantage of a random solution over the worst solution value*. Namely, we say that the average solution value on I is ρ -approximate if the ratio

$$\rho_E(I) = \frac{\mathbb{E}_X[v(I, X)] - \text{wor}(I)}{\text{opt}(I) - \text{wor}(I)} \quad (2)$$

of the gain of $\mathbb{E}_X[v(I, X)]$ over $\text{wor}(I)$ to the diameter of I is at least ρ . Given a CSP Π , we say that the average solution value is ρ -approximate for Π provided that $\rho_E(I) \geq \rho$ holds for all instances I of Π . The issue here consists in exhibiting “the tightest” possible lower bound ρ for ρ_E . For example, on an instance I of **E3 Lin-2**, as given any x , any equation is satisfied either by x or by its complement, we have $\text{opt}(I) + \text{wor}(I) = w(I) = 2 \times \mathbb{E}_X[v(I, X)]$ [7]. Equivalently, $\rho_E(I)$ is equal to $1/2$. By contrast, for **E2 Lin-2**, we show that $\rho_E(I) \in \Omega(1/n)$, while there are satisfiable instances I on which $\rho_E(I) \in \Theta(1/n)$.

Figure 1 pictures the quantities involved in ratios (1) and (2). The two questions are complementary, and the latter has potential to enlighten the former. For instance, we may think that the more $\mathbb{E}_X[v(I, X)]$ does a good job at getting away from $\text{wor}(I)$, the more it is computationally difficult to get away from it.

1.2 Outline

Our goal is to estimate $\rho_E(I)$ on instances I of **kCSP-q** given two integers $q \geq 2, k \geq 2$. To the best of our knowledge, such a study has not been carried out so far. We may nevertheless make mention of a result due to Feige et al., and that concerns the restriction to *submodular functions*. A function $P : \{0, 1\}^n \rightarrow \mathbb{R}$ is submodular *iff* it satisfies for all $y, z \in \{0, 1\}^n$ that

$$P(y) + P(z) \geq P(y_1 \vee z_1, \dots, y_n \vee z_n) + P(y_1 \wedge z_1, \dots, y_n \wedge z_n)$$

As shown in [8], given any maximizer x^* of such a function P , we have:

$$\mathbb{E}_X[P(X)] \geq P(x^*)/4 + P(\bar{x}_1^*, \dots, \bar{x}_n^*)/4 + P(0, \dots, 0)/4 + P(1, \dots, 1)/4 \quad (3)$$

Since a conical combination of submodular pseudo-boolean functions is submodular, it follows from (3) that, on an instance I of **Max CSP-2** in which functions

Table 1. Lower bounds for ρ_E on instances of k CSP- q given two integers $q \geq 2, k \geq 2$: p^κ refers to the smallest prime power greater than or equal to q .

q	k	restriction	ρ_E
≥ 2	≥ 2	$(k+1)$ -partite instances of k CSP- q	$1/q^k$
≥ 2	$< p^\kappa$	$(p^\kappa+1)$ -partite instances of k CSP- q	$\Omega(1/q^k)$
≥ 3	$= 3$	$(2^{\lceil \log_2 q \rceil} + 2)$ -partite instances of 3 CSP- q	$\Omega(1/q^3)$
$= 2$	≥ 2	k CSP-2	$\Omega(1/n^{\lfloor k/2 \rfloor})$
≥ 3	≥ 2	k CSP- q	$\Omega(1/n^{k-1-\lfloor \log_{p^\kappa}(k-1) \rfloor})$

P_i all are submodular, we have $E_X[v(I, X)] \geq \text{opt}(I)/4 + 3 \times \text{wor}(I)/4$ and thus, $\rho_E(I) \geq 1/4$.

In k CSP- q , thought, the functions that may occur in the constraints are not constrained otherwise than by their arity. In order to exhibit lower bounds for $\rho_E(I)$, we seek expressions of $E_X[v(I, X)]$ as a conical combination of the optimum solution value and as few other solution values as possible. We adopt kind of a neighbourhood approach: we associate with each solution x of I a multiset $S(I, x)$ of solutions with the same average solution value as the whole solution set, of relatively small size, and in which x occurs at least once. In the next section, we show how to derive such solution multisets from hypothetical orthogonal arrays (see Definition 2) with specified parameters that rely on characteristics of I (main theorem). In Section 3, we derive lower bounds for ρ_E either from orthogonal arrays of the literature, or by reduction from one alphabet size to a greater one. These bounds are summarized in Table 1. In the last section, we briefly discuss the obtained results and perspectives for further research.

2 Seeking Symmetries in the Solution Set

Let us start with a simple example. Given an integer $q \geq 2$, we denote by \mathcal{O}_q the set of functions $P : \mathbb{Z}_q^k \rightarrow \mathbb{R}$ with $k \in \mathbb{N}^*$ that satisfy:

$$\sum_{a=0}^{q-1} P(y_1 + a, \dots, y_k + a)/q = r_P, \quad y \in \mathbb{Z}_q^k \quad (4)$$

\mathcal{O}_q is a natural generalization to q -ary alphabets of such boolean functions P as XOR^3 that, when using a $\{-1, 1\}$ -encoding of truth values, are odd. For example, the predicate on \mathbb{Z}_q^3 that accepts solutions to equation $y_1 + y_2 - y_3 \equiv 0 \pmod q$ is a function of \mathcal{O}_q . By (4), given any instance I of CSP(\mathcal{O}_q), we have:

$$v(I, x)/q + \sum_{a=1}^{q-1} v(I, (x_1 + a, \dots, x_n + a))/q = E_X[v(I, X)], \quad x \in \mathbb{Z}_q^n \quad (5)$$

Taking (5) at a solution x with optimal value, one trivially gets that the average value is $1/q$ -approximate on I . Hence, for this CSP, one shall define $S(I, x)$ by $S(I, x) = \{x + (a, \dots, a) \mid a \in \mathbb{Z}_q\}$.

2.1 Partition-Based Solution Families

We base our solution families $S(I, x)$ on a specific partition $\mathcal{V} = \{V_1, \dots, V_\nu\}$ of $[n]$. These families then rely on an array M with ν columns and coefficients in

\mathbb{Z}_q . Given $x \in \mathbb{Z}_q^n$, each row $M_r = (M_r^1, \dots, M_r^\nu)$ of M gives rise in $S(I, x)$ to the vector obtained from x by translating for each $c \in [\nu]$ by M_r^c all its coordinates with index in V_c . Formally, let R refer to the number of rows in the array, and let $\pi_{\mathcal{V}} : \mathbb{Z}_q^\nu \rightarrow \mathbb{Z}_q^n$ be defined by:

$$\pi_{\mathcal{V}}(u)_{V_c} = (u_c, u_c, \dots, u_c), c \in [\nu], \quad u \in \mathbb{Z}_q^\nu \quad (6)$$

Then we define $S(I, \cdot)$ by:

$$S(I, x) = (x + \pi_{\mathcal{V}}(M_r) \mid r \in [R]), \quad x \in \mathbb{Z}_q^n \quad (7)$$

We more specifically seek pairs (\mathcal{V}, M) that satisfy the following condition:

$$\sum_{r=1}^R P_i(x_{J_i} + \pi_{\mathcal{V}}(M_r)_{J_i})/R = r_{P_i}, \quad i \in [m], \quad x \in \mathbb{Z}_q^n \quad (8)$$

For example, when I is an instance of $\text{CSP}(\mathcal{O}_q)$, one may consider the pair (\mathcal{V}, M) where $\mathcal{V} = \{\{[n]\}\}$ and $M = (0, 1, \dots, q-1)^T$. Requirement (8) ensures that the average solution value over $S(I, x)$ equals the average solution value on I . Since this holds for all $x \in \mathbb{Z}_q^n$, this in particular holds for a solution multiset $S(I, x^*)$ where x^* is optimal. If R^* refers to the number of times $(0, \dots, 0)$ occurs as a row in M , then R^* precisely is the number of times x^* occurs in $S(I, x^*)$. Then for such a solution multiset, we have:

$$\begin{aligned} E_X[v(I, X)] &= \sum_{r=1}^R v(I, x^* + \pi_{\mathcal{V}}(M_r))/R \\ &= R^* \times v(I, x^*)/R + \sum_{r \in [R]: M_r \neq (0, \dots, 0)} v(I, x^* + \pi_{\mathcal{V}}(M_r))/R \end{aligned}$$

Therefore, the average solution value on I is R^*/R -approximate.

Observe that we may assume that $(0, \dots, 0)$ is a vector of highest frequency in M , since the array obtained by shifting every row of M by $u \in \mathbb{Z}_q^\nu$ still satisfies (8).

2.2 Solution Families Derived from Orthogonal Arrays

Given $i \in [m]$, we denote by $(c_{i,1}, \dots, c_{i,k_i})$ the sequence of indices in $[\nu]$ such that $(i_1, \dots, i_{k_i}) \in V_{c_{i,1}} \times \dots \times V_{c_{i,k_i}}$. Then given any $x \in \mathbb{Z}_q^n$, over $S(I, x)$, P_i is evaluated at entries

$$x_{J_i} + \pi_{\mathcal{V}}(M_r)_{J_i} = (x_{i_1} + M_r^{c_{i,1}}, \dots, x_{i_{k_i}} + M_r^{c_{i,k_i}}), \quad r \in [R]$$

(\mathcal{V}, M) therefore in particular satisfies (8) at (i, x) provided that these entries coincide the same number of times with each $u \in \mathbb{Z}_q^{k_i}$. Equivalently, (8) is satisfied at (i, x) provided that each $u \in \mathbb{Z}_q^{k_i}$ occurs R/q^{k_i} times in vector multiset

$$((M_r^{c_{i,1}}, \dots, M_r^{c_{i,k_i}}) \mid r \in [R]) \quad (9)$$

On the one hand, this may not occur unless indices $c_{i,1}, \dots, c_{i,k_i}$ are pairwise distinct. On the other hand, assuming that these indices indeed are pairwise distinct, $\{c_{i,1}, \dots, c_{i,k_i}\}$ can be any at most k -cardinality subset of $[\nu]$. These observations suggest to consider a pair (\mathcal{V}, M) where \mathcal{V} is a *strong coloring* of the *primary hypergraph* of I , and M is *orthogonal of strength k* :

Table 2. An $OA(27, 5, 3, 2)$ on \mathbb{Z}_3 (we picture the transpose).

M^1	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	
M^2	0	0	0	1	1	1	2	2	2	0	0	0	1	1	1	2	2	2	0	0	0	1	1	1	2	2	2
M^3	0	0	2	0	1	1	1	2	2	1	1	2	0	0	2	0	1	2	0	1	2	1	2	2	0	0	1
M^4	0	0	2	1	0	1	2	1	2	1	2	1	2	2	0	0	0	1	1	2	0	1	0	2	1	2	0
M^5	0	0	2	1	1	2	2	0	1	2	0	1	0	2	1	2	1	0	1	1	2	0	2	0	2	1	0

Definition 1. The primary hypergraph of a CSP instance I is the hypergraph G_I where: for each $j \in [n]$, there is a vertex j in G_I ; for each $i \in [m]$, there is a hyperedge $e_i = (i_1, \dots, i_{k_i})$ in G_I . A strong coloring of G_I is a partition $\{U_1, \dots, U_\nu\}$ of $[n]$ such that for all $c \in [\nu]$ and all $i \in [m]$, $|U_c \cap \{i_1, \dots, i_{k_i}\}| \leq 1$. I is said ν -partite whenever such a partition exists.

Definition 2. Let $q \geq 2, t \geq 1, \nu \geq t$ and R be four integers, and Σ be a set of q symbols. Then an $R \times \nu$ array M with entries in Σ is an Orthogonal Array of strength t , $OA(R, \nu, q, t)$ in short, if given any sequence $J = (c_1, \dots, c_t)$ of t column indices, each $v \in \Sigma^t$ occurs the same number of times as a row in subarray $M^J = (M^{c_1}, \dots, M^{c_t})$. (See Table 2 for an illustration.)

Since $k_i \leq k, i \in [m]$, such a pair (\mathcal{V}, M) indeed satisfies for all $i \in [m]$ that the vectors of (9) coincide R/q^{k_i} times with each $u \in \mathbb{Z}_q^{k_i}$ and thus, (8).

It is possible to reduce the number of columns and possibly the strength of the array if functions P_i all satisfy, for some integer $t > 0$, that their average value when fixing any t of their variables is equal to their average value. Namely, given two integers $q \geq 2, t \geq 1$, we define \mathcal{I}_q^t as the set of functions $P : \mathbb{Z}^k \rightarrow \mathbb{R}$ with $k \in \mathbb{N}^*$ that satisfy:

$$\sum_{y \in \mathbb{Z}_q^k: y_J = v} P(y)/q^{k-t} = r_P, \quad J \subseteq [k], |J| = t, v \in \mathbb{Z}_q^t \quad (10)$$

Such functions notably arise in the establishment of inapproximability bounds for k CSP-q. Notably, for all $k \geq 3$, if the accepting entries of a k -ary predicate $P \in \mathcal{I}_q^2$ form a subgroup of \mathbb{Z}_q^k , then Max CSP-P is **NP-hard** to approximate within any constant factor greater than r_P [4]. For example, the predicate that accepts solutions to equation $y_1 + y_2 - y_3 \equiv 0 \pmod q$ over \mathbb{Z}_q^3 is such a predicate.

Thus assume that $P_i \in \mathcal{I}_q^t, i \in [m]$ holds for some $t > 0$. It is then possible to fix up to t coordinates of $\pi_{\mathcal{V}}(M_r)_{J_i}$, and still obtain when averaging $P_i(x_{J_i} + \pi_{\mathcal{V}}(M_r)_{J_i})$ over $r \in [R]$ the average value of P_i . Hence, rather than a strong coloring $\{U_1, \dots, U_\nu\}$ of G_I , we consider partition $\mathcal{V} = \{U_1, \dots, U_{\nu-t}, V_0\}$ where $V_0 = U_{\nu-t+1} \cup \dots \cup U_\nu$ of $[n]$. M consequently has $\nu-t+1$ columns. Given $i \in [m]$, we denote by K_i the set $\{c_{i,1}, \dots, c_{i,k_i}\} \cap \{1, \dots, \nu-t\}$ of column indices, by s_i its cardinality. For the sake of clarity, we assume *w.l.o.g.* that $K_i = \{c_{i,1}, \dots, c_{i,s_i}\}$. Over $S(I, x)$, P_i is evaluated at entries

$$(x_{i_1} + M_r^{c_{i,1}}, \dots, x_{i_{s_i}} + M_r^{c_{i,s_i}}, x_{i_{s_i+1}} + M_r^{\nu-t+1}, \dots, x_{i_{k_i}} + M_r^{\nu-t+1}), r \in [R]$$

where $k_i - s_i \leq t$ and $s_i \leq \min\{\nu-t, k_i\} \leq \min\{\nu-t, k\}$. We deduce that setting *e.g.* $M = N \times \{0\}$ where N is an orthogonal array of strength $\min\{\nu-t, k\}$ on $\nu-t$ columns, one obtains a pair (\mathcal{V}, M) that satisfies (8).

Thereafter, given an instance I of CSP- q , we denote by ν_I the *strong chromatic number* of G_I (that is, ν_I is the smallest integer such that I is ν_I -partite), and by t_I the greatest integer such that $P_i \in \mathcal{I}_q^{t_I}, i \in [m]$ (thus t_I possibly is 0). In all, the preceding discussion establishes the following connection between the average solution value of CSP instances and orthogonal arrays:

Theorem 1. *Given any three integers $q \geq 2, t \geq 1, \nu \geq t$, we define $\rho(\nu, q, t)$ as the greatest $\rho \in [0, 1]$ for which an $OA(R, \nu, q, t)$ with highest frequency ρ exists. (For example, the $OA(27, 5, 3, 2)$ of Table 2 does achieve $\rho(5, 3, 2) = 2/27$.)*

Then for all integers $k \geq 2, q \geq 2$, the average solution value on an instance I of k CSP- q is $\rho(\nu_I - t_I, q, \min\{k, \nu_I - t_I\})$ -approximate.

3 Approximation Quality of the Average Solution Value

3.1 From an Alphabet Size to a Greater One

We derive lower bounds for ρ_E from orthogonal arrays with a relatively small number of rows of the literature. Such arrays often require q to be a prime power. However, we can derive lower bounds for ρ_E in case when q is not a prime power from lower bounds for ρ_E in case when q is a prime power:

Theorem 2. *Let $q \geq 3, k \geq 2$ be two integers. Then for all primes p , the average solution value on an instance I of k CSP- q is $\rho(\nu_I, p^{\lceil \log_p q \rceil}, k)$ -approximate.*

Proof. Let $\kappa = \lceil \log_p q \rceil, d = p^\kappa$, and let $\pi = (\pi_1, \dots, \pi_n)$ be a vector of surjective maps from \mathbb{Z}_d to \mathbb{Z}_q . We interpret I as the instance $f_\pi(I)$ of CSP- d where:

1. for each $j \in [n]$, there is in $f_\pi(I)$ a variable z_j with domain \mathbb{Z}_d ;
2. for each $i \in [m]$, there is in $f_\pi(I)$ a constraint $P_i(\pi_{i_1}(z_{i_1}), \dots, \pi_{i_{k_i}}(z_{i_{k_i}}))$, with the same associated weight w_i as C_i in I .

So as to retrieve solutions of I from solutions of $f_\pi(I)$, we define $g_\pi(I, \cdot)$ by $g_\pi(I, z) = (\pi_1(z_1), \dots, \pi_n(z_n)), z \in \mathbb{Z}_d^n$. By construction, $g_\pi(I, \cdot)$ is surjective, and satisfies for all $z \in \mathbb{Z}_d^n$ that $v(I, g_\pi(I, z)) = v(f_\pi(I), z)$. The extremal solution values on I and $f_\pi(I)$ therefore satisfy:

$$\text{opt}(f_\pi(I)) = \text{opt}(I), \text{wor}(f_\pi(I)) = \text{wor}(I) \tag{11}$$

By contrast, $E_Z[v(f_\pi(I), Z)]$ may differ from $E_X[v(I, X)]$, due to the fact that two distinct vectors $x, x' \in \mathbb{Z}_q^n$ may be the image by $g_\pi(I, \cdot)$ of a distinct number of vectors of \mathbb{Z}_d^n . Hence, rather than a single vector π , we consider a vector $\Pi = (\Pi_1, \dots, \Pi_n)$ of random maps that are independently and uniformly distributed over the set \mathcal{M} of surjective maps from \mathbb{Z}_d to \mathbb{Z}_q .

Let $j \in [n], a \in \mathbb{Z}_d, b \in \mathbb{Z}_q, b' \in \mathbb{Z}_q \setminus \{b\}$. Consider then function σ on \mathcal{M} that maps any $\pi \in \mathcal{M}$ to the map $\sigma(\pi) : \mathbb{Z}_d \rightarrow \mathbb{Z}_q$ defined by $\sigma(\pi)(c) = b'$ if $\pi(c) = b$, b if $\pi(c) = b'$ and $\pi(c)$ otherwise. σ clearly is a bijection on \mathcal{M} . Hence, we have:

$$|\{\pi \in \mathcal{M} \mid \pi(a) = b\}| = |\{\pi \in \mathcal{M} \mid \sigma(\pi)(a) = b'\}| = |\{\pi \in \mathcal{M} \mid \pi(a) = b'\}|$$

Since $\sum_{b=0}^{q-1} \mathbb{P}_{\Pi_j}[II_j(a) = b] = 1$ holds for all $j \in [n]$ and all $a \in \mathbb{Z}_d$, we first deduce that probabilities $\mathbb{P}_{\Pi_j}[II_j(a) = b]$ all are equal to $1/q$. We then deduce that probabilities $\mathbb{P}_{\Pi}[g_{\Pi}(I, z) = x]$, $z \in \mathbb{Z}_d^n$, $x \in \mathbb{Z}_q^n$ all are equal to $\prod_{j=1}^n \mathbb{P}_{\Pi_j}[II_j(z_j) = x_j] = 1/q^n$. Accordingly, given any $z \in \mathbb{Z}_d^n$, we have:

$$\mathbb{E}_{\Pi}[v(I, g_{\Pi}(I, z))] = \sum_{x \in \mathbb{Z}_q^n} v(I, x) \times \mathbb{P}_{\Pi}[g_{\Pi}(I, z) = x] = \mathbb{E}_X[v(I, X)]$$

We eventually deduce that the expected average solution value on $f_{\Pi}(I)$ satisfies:

$$\mathbb{E}_{\Pi}[\mathbb{E}_Z[v(f_{\Pi}(I), Z)]] = \mathbb{E}_Z[\mathbb{E}_{\Pi}[v(I, g_{\Pi}(I, Z))]] = \mathbb{E}_X[v(I, X)] \quad (12)$$

By (12), there exists $\pi_* \in \mathcal{M}^n$ such that $\mathbb{E}_Z[v(f_{\pi_*}(I), Z)] \leq \mathbb{E}_X[v(I, X)]$ while by (11), for such a vector π_* , we have $\rho_E(I) \geq \rho_E(f_{\pi_*}(I))$. Since the supports of the constraints are unchanged by $f_{\pi}, \pi \in \mathcal{M}^n$, the result follows from Theorem 1. \square

3.2 Deriving Bounds from Orthogonal Arrays of the Literature

Let $q \geq 2, t \geq 1, \nu \geq t$ be three integers. The smallest positive integer R such that an $OA(R, \nu, q, t)$ exists is referred to as $F(\nu, q, t)$ in the literature. The highest frequency of a word in an array that achieves $F(\nu, q, t)$ naturally is at least $1/F(\nu, q, t)$. Also observe that $F(\nu, q, k) \leq F(\nu', q, k)$ naturally holds for all integers $\nu' > \nu$. Hence, according to Theorems 1 and 2, given any instance I of k CSP- q , we may exhibit lower bounds for $\rho_E(I)$ using inequalities:

$$\rho_E(I) \geq 1/F(\nu', q, \min\{\nu_I - t_I, k\}), \quad \nu' \in \mathbb{N}, \nu' \geq \nu_I - t_I \quad (13)$$

$$\rho_E(I) \geq 1/F(\nu', p^{\lceil \log_p q \rceil}, k), \quad \nu', p \in \mathbb{N}, \nu' \geq \nu_I, p \text{ prime} \quad (14)$$

First, we consider the case of instances with a bounded strong chromatic number. Given three integers $q \geq 2, k \geq 1, \nu \geq k$, there exists an $OA(q^k, \nu, q, k)$ provided that one of the following cases occurs (see *e.g.* [12]):

1. $\nu \in \{k, k+1\}$;
2. q is a prime power, $q > k$ and $\nu \in \{k+2, \dots, q+1\}$;
3. $k=3$, q is a power of 2, $q > 3$ and $\nu = q+2$.

1. is trivial, considering $M \simeq \mathbb{Z}_q^k$ if $\nu = k$, $M \simeq \{y \in \mathbb{Z}_q^{k+1} \mid y_1 + \dots + y_{k+1} \equiv 0 \pmod{q}\}$ otherwise. 2. and 3. are due to Bush. We deduce from (13) and (14) the following lower bounds for ρ_E in $O(\max\{q, k\})$ -partite instances of k CSP- q :

Corollary 1. *Let $q \geq 2, k \geq 2, \nu \geq k$ be three integers with $\nu \in O(\max\{q, k\})$ and I be a ν -partite instance of k CSP- q . We denote by p^{κ} the smallest prime power greater than or equal to q . Then on I , $\rho_E(I)$ is bounded below by:*

1. $1/q^{\nu-t_I} > 1/q^k$ if $\nu < k + t_I$;
2. $1/q^k$ if $\nu \leq k + t_I + 1$;
3. $1/q^k$ if q is a prime power, $q > k$ and $\nu \leq q + t_I + 1$;
4. $1/p^{\kappa k} \geq 1/(2(q-1))^k$ if q is not a prime power, $p^{\kappa} > k$ and $\nu \leq p^{\kappa} + 1$;

5. $1/q^3$ if $k = 3$, q is a power of 2, $q > 3$ and $\nu \leq q + t_I + 2$;
6. $1/2^{3\lceil \log_2 q \rceil} \geq 1/(2(q-1))^3$ if $k = 3$, q is not a power of 2 and $\nu \leq 2^{\lceil \log_2 q \rceil} + 2$.

For example, on a k -partite instance I of $\text{Lin}-\mathbf{q}$ in which equations all are of the form $(x_{i_1} + \dots + x_{i_k} \equiv \alpha_{i,0} \pmod{q})$, we have $\rho_E(I) \geq 1/q$.

For greater integers ν , we refer to families of orthogonal arrays that originate from infinite families of linear codes. Over the boolean alphabet, we consider dual codes of BCH codes. Namely, binary BCH codes allow for all integers $\kappa \geq 3, k \geq 1$ such that $2^\kappa - 1 \geq 2k + 1$ to construct an $OA(R, 2^\kappa - 1, 2, 2k)$ with $R \leq 2^{\kappa k}$ (see e.g. [12, 15]). For such pairs (κ, k) , we consequently have $F(2^\kappa - 1, 2, 2k) \leq 2^{\kappa k}$. Besides, as reported in [12], $F(2^\kappa, 2, 2k + 1) = 2 \times F(2^\kappa - 1, 2, 2k)$. Then, for such pairs (κ, k) , it also holds that $F(2^\kappa, 2, 2k + 1) \leq 2^{1+\kappa k}$. Accordingly:

Corollary 2. *Let $k \geq 2$ be an integer. Then on all instances I of \mathbf{kCSP} with $\nu_I - t_I \geq k + 2$, $\rho_E(I)$ is bounded below by:*

1. $1/2^{\lceil \log_2(\nu_I - t_I + 1) \rceil \lfloor k/2 \rfloor} \geq 1/2^{\lfloor k/2 \rfloor} \times 1/(\nu_I - t_I)^{\lfloor k/2 \rfloor}$ if k is even;
2. $1/2^{1 + \lceil \log_2(\nu_I - t_I) \rceil \lfloor k/2 \rfloor} \geq 1/2^{1 + \lfloor k/2 \rfloor} \times 1/(\nu_I - t_I - 1)^{\lfloor k/2 \rfloor}$ if k is odd.

For $\text{E2 Lin}-2$, which is a special case of $2\text{CSP}(\mathcal{I}_2^1)$, we thus obtain for ρ_E a lower bound of $1/2^{\lceil \log_2 \nu_I \rceil}$. We provide evidence that this bound is tight: given $n \in \mathbb{N}^*$, let I_n refer to the instance where G_{I_n} is the complete graph K_{2n} and equations all are of the form $(x_j + x_h \equiv 0 \pmod{2})$. These instances are trivially satisfiable by the vectors of allzeros and of allones. For all $n \in \mathbb{N}^*$, we have:

$$\rho_E(I_n) = \left(\binom{2n}{2} / 2 - 2 \binom{n}{2} \right) / \left(\binom{2n}{2} - 2 \binom{n}{2} \right) = 1/(2n) = 1/\nu_{I_n}$$

For greater prime powers q , trace-codes of Reed-Solomon codes give rise for all integers s, k, λ such that $q^s \geq k > q^\lambda \geq 1$ to $q^{1+s(k-1-\lambda)} \times q^s$ orthogonal arrays of strength k on \mathbb{Z}_q [3]. Accordingly:

Corollary 3. *Let $q \geq 3, k \geq 2$ be two integers. We denote by p^κ the smallest prime power such that $p^\kappa \geq q$, by λ the greatest integer such that $k > p^{\kappa\lambda}$. If q is a prime power, then for all instances I of $\mathbf{kCSP}-\mathbf{q}$ with $\nu_I - t_I \geq k$, we have:*

$$\rho_E(I) \geq 1/q^{1 + \lceil \log_q(\nu_I - t_I) \rceil (k-1-\lambda)} \geq 1/q^{k-\lambda} \times 1/(\nu_I - t_I - 1)^{k-1-\lambda}$$

Otherwise, for all instances I of $\mathbf{kCSP}-\mathbf{q}$ with $\nu_I \geq k$, we have:

$$\rho_E(I) \geq 1/p^{\kappa(1 + \lceil \log_{p^\kappa} \nu_I \rceil (k-1-\lambda))} \geq 1/(2(q-1))^{k-\lambda} \times 1/(\nu_I - 1)^{k-1-\lambda}$$

4 Concluding Remarks

In order to evaluate the quality of the average solution value, one shall compare the lower bounds we obtain for ρ_E to both gain and *differential* approximability bounds of the literature. The *differential approximation measure* (see [6] for an introduction) evaluates the performance of a given solution x by the ratio

$$\rho_D(I, x) = \frac{v(I, x) - \text{wor}(I)}{\text{opt}(I) - \text{wor}(I)} \quad (15)$$

Thus $\rho_E(I)$ precisely is the *average differential ratio* on I . ρ -differential approximable problems are defined just as the same as for the gain approximation measure. Notice that by definition of $\rho_G(I, x)$, $\rho_E(I)$ and $\rho_D(I, x)$, we have:

$$\rho_D(I, x) = \rho_E(I) + (1 - \rho_E(I)) \times \rho_G(I, x) \quad (16)$$

Hence, if a given CSP Π is ρ -gain approximable, and the average solution value is δ -approximate for Π , then Π is $[\rho + \delta(1 - \rho)]$ -differential approximable.

We summarize in Table 3 the bounds we are aware of. In this table, we take into account the fact that gain approximability lower bounds that hold for $\text{Lin}-2$ somehow extend to $k\text{CSP}-q$ for all integers $q \geq 2, k \geq 3$:

Proposition 1. *For all integers $q \geq 2, k \geq 2$, if $(k \lceil \log_2 q \rceil)\text{Lin}-2$ is approximable within gain factor ρ , then $k\text{CSP}-q$ is approximable within differential factor ρ and, provided that q is a power of 2, within gain factor ρ .*

Proof (sketch). Let I be an instance of $k\text{CSP}-q$. First map I to an instance J of $(\kappa k)\text{CSP}-2$ where $\kappa = \lceil \log_2 q \rceil$ using a binary encoding of the variables. Then map J to an instance H of $(\kappa k)\text{Lin}-2$ using the discrete Fourier transform. When $q = 2^\kappa$, the average solution values on I and J (and thus, on H) are identical. \square

For such symptomatic CSPs as the restriction of $\text{CSP}(\mathcal{I}_q^{k-1})$ to k -partite instances for all $k \geq 3$, and $\text{CSP}(\mathcal{O}_q)$, $E_X[v(I, X)]$ trivially brings the same differential approximation guarantee of $1/q$, which essentially is optimal, as in the standard approximation framework. By contrast, for $2\text{CSP}-2$, $E_X[v(I, X)]$ is of rather low quality, considering that $\Omega(1/n)$ is a tight lower bound for $\rho_E(I)$, while $2\text{CSP}-2$ is approximable within gain and differential factor respectively $\Omega(1/\ln n)$ and $\Omega(1)$. For greater integers k , in dense instances of $k\text{CSP}-2$, the factor of $\Omega(1/n^{\lceil k/2 \rceil})$ $E_X[v(I, X)]$ gains over $\text{wor}(I)$ is significantly greater than the best gain approximation guarantee of $\Omega(1/m)$ known so far, and comparable to the best expected gain factor of $\Omega(1/\sqrt{m})$ known so far.

Starting with a $R \times \nu$ -array M on \mathbb{Z}_q , we can define a probability distribution on \mathbb{Z}_q^ν by associating with each vector $u \in \mathbb{Z}_q^\nu$ its frequency in M . Then, M is orthogonal of strength t iff this distribution is *balanced t -wise independent*. This classical notion is strongly involved in the exhibition of approximation resistant predicates (e.g. see [2, 4]). A function $P : \mathbb{Z}_q^\nu \rightarrow \mathbb{R}$ with minimal value P_* similarly belongs to \mathcal{I}_q^t iff $1/q^\nu \times (P - P_*) / (r_P - P_*)$ defines a balanced t -wise independent distribution on \mathbb{Z}_q^ν . The analysis we proposed therefore reinforces the connection between balanced t -wise independence and approximability of $k\text{CSP}-q$ by allowing the establishment of positive results. Observe that the arrays we used contain no duplicated rows. Therefore, lower bounds for $\rho(\nu, q, k)$ (and thus, for ρ_E) could be improved by exhibiting orthogonal arrays (or balanced k -wise independent measures) that maximize their highest frequency. Table 4 provides a few illustrations of this fact.

The average differential ratio has potential to provide new insights into CSPs. First, the method we used to obtain lower bounds for ρ_E not only shows that $E_X[v(I, X)]$ achieves some differential ratio ρ , but also indicates that ρ -differential approximate solutions are spread all over the solution set. It thus

Table 3. Differential (ρ_D) and gain (ρ_G) approximability bounds for k CSP- q that are achievable by either deterministic (det.) or randomized (exp.) algorithms, and their comparison to ρ_E : p^κ refers to the smallest prime power $\geq q$; inapproximability bounds are given for all constant $\varepsilon > 0$, and assume $\mathbf{P} \neq \mathbf{NP}$.

Approximability bounds in k -partite instances of Ek CSP- q

k	q	t_I	ρ_G det.	ρ_D det.	ρ_E
$= 2$	$= 2$	$= 1$	0.561 [1]	0.78 [1]	$= 1/2$
≥ 3	≥ 2	$= k - 1$	$\neg \varepsilon$ [4]	$\neg 1/q + \varepsilon$ [4]	$\geq 1/q$
≥ 3	$\geq 2, \leq k$	$= 2$	$\neg \varepsilon$ [4]	$\neg O(k/q^{k-1}) + \varepsilon$ [4]	$\geq 1/q^{k-2}$
≥ 3	$\geq k$	$= 2$	$\neg \varepsilon$ [4]	$\neg O(k/q^{k-2}) + \varepsilon$ [4]	$\geq 1/q^{k-2}$

Gain approximability bounds for Ek CSP- q

k	q	t_I	ρ_G det.	ρ_G exp.	ρ_E
$= 2$	$= 2$	≥ 0	$\Omega(1/\ln n)$ [16]		$\Omega(1/\nu_I)$
$= 3$	$= 2$	$= 2$	$\Omega(1/m)$ [11]	$\Omega(\sqrt{\ln n/n})$ [14]	$= 1/2$
≥ 4	$= 2$	≥ 0	$\Omega(1/m)$ [11]	$\Omega(1/\sqrt{m})$ [11]	$\Omega(1/\nu_I^{\lfloor k/2 \rfloor})$
≥ 2	$= 2^\kappa, \geq 4$	≥ 0	$\Omega(1/m)$	$\Omega(1/\sqrt{m})$	$\Omega(1/\nu_I^{k-1-\lfloor \log_2 \kappa (k-1) \rfloor})$

Other differential approximability bounds for k CSP- q

k, q	ρ_D det.	ρ_D exp.	ρ_E
$k = 2$ or $(k, q) = (3, 2)$	$\Omega(1)$ [17, 5]		$\Omega(1/\nu_I)$
$k \geq 3$ and $q \geq 3$	$\Omega(1/m)$	$\Omega(1/\sqrt{m})$	$\Omega(1/\nu_I^{k-1-\lfloor \log_p \kappa (k-1) \rfloor})$

provides additional information on the repartition of solution values. Although we took into account parameters ν_I and t_I so as to refine our analysis, apart from the arity of their constraints, we did not restrict the instances we considered. Hence, a next step should be the identification of hypergraphs and function properties that allow to build partition-based solution families of low cardinality that satisfy (8). More generally, it would be worthwhile to characterize functions families \mathcal{F} (as the set of submodular functions [8]) such that $\text{Max CSP}(\mathcal{F})$ or $\text{Min CSP}(\mathcal{F})$ admits a constant lower bound for ρ_E . Finally, the properties of ρ_E viewed as a complexity measure, including its connections to other measures, should be investigated. Notably, the authors of [7] could derive from the hardness result of [10] for E3 Lin-2 a constant inapproximability bound of 0 for the diameter of instances of 3 Sat , precisely because for E3 Lin-2 , $\rho_E \in O(1)$.

References

1. Alon, N., Naor, A.: Approximating the Cut-norm via Grothendieck’s Inequality. *SIAM J. Comput.* **35**(4), 787–803 (2006). <https://doi.org/10.1137/S0097539704441629>
2. Austrin, P., Hästad, J.: Randomly Supported Independence and Resistance. *SIAM J. Comput.* **40**(1), 1–27 (2011). <https://doi.org/10.1137/100783534>
3. Bierbrauer, J.: Construction of orthogonal arrays. *J. of Statistical Planning and Inference* **56**(1), 39–47 (1996). [https://doi.org/10.1016/S0378-3758\(96\)00007-9](https://doi.org/10.1016/S0378-3758(96)00007-9)
4. Chan, S.O.: Approximation Resistance from Pairwise-Independent Subgroups. *J. ACM* **63**(3), 27:1–27:32 (2016). <https://doi.org/10.1145/2873054>

Table 4. Comparison of arrays that maximize their highest frequency among those that achieve $F(\nu, q, k)$ (on the right) to arrays that minimize their number of rows among those that achieve $\rho(\nu, q, k)$ (on the left). In both cases, we indicate the ratio R^*/R of the highest number of occurrences of a word to the number of rows in the array. (These arrays were calculated by computer using linear programs.)

q	k	ν						ν					
		4	5	6	7	8	9	4	5	6	7	8	9
2	2	2/12	2/12	1/8	1/8	2/20	2/20	1/8	1/8	1/8	1/8	1/12	1/12
2	4	1/16	1/16	3/80	4/144	6/240		1/16	1/16	1/32	1/64	1/64	
	6	–	1/32	1/64	1/64	4/448	6/960	–	1/32	1/64	1/64	1/128	1/256
3	2	1/9	2/27	3/45	3/45			1/9	1/18	1/18	1/18		
4	2	1/16	1/16	7/160				1/16	1/16	1/32			

5. Culus, J.F., Toulouse, S.: 2 CSPs all are approximable within some constant differential factor. In: 5th Int. Symp. on Combinatorial Optimization (ISCO) (2018), to appear
6. Demange, M., Paschos, V.T.: On an approximation measure founded on the links between optimization and polynomial approximation theory. *Theor. Comput. Sci.* **158**(1–2), 117–141 (1996). [https://doi.org/10.1016/0304-3975\(95\)00060-7](https://doi.org/10.1016/0304-3975(95)00060-7)
7. Escoffier, B., Paschos, V.T.: Differential approximation of MIN SAT, MAX SAT and related problems. *EJOR* **181**(2), 620–633 (2007). <https://doi.org/10.1016/j.ejor.2005.04.057>
8. Feige, U., Mirrokni, V.S., Vondrák, J.: Maximizing Non-monotone Submodular Functions. *SIAM J. Comput.* **40**(4), 1133–1153 (2011). <https://doi.org/10.1137/090779346>
9. Garey, M., Johnson, D., Stockmeyer, L.: Some simplified NP-complete graph problems. *Theor. Comput. Sci.* **1**(3), 237–267 (1976). [https://doi.org/10.1016/0304-3975\(76\)90059-1](https://doi.org/10.1016/0304-3975(76)90059-1)
10. Håstad, J.: Some optimal inapproximability results. *J. ACM* **48**(4), 798–859 (2001). <https://doi.org/10.1145/502090.502098>
11. Håstad, J., Venkatesh, S.: On the Advantage over a Random Assignment. *Random Structures & Algorithms* **25**(2), 117–149 (2004). <https://doi.org/10.1002/rsa.20031>
12. Hedayat, A., Sloane, N.J.A., Stufken, J.: *Orthogonal Arrays, Theory and Applications*. Springer-Verlag New York (1999). <https://doi.org/10.1007/978-1-4612-1478-6>
13. Johnson, D.S.: Approximation algorithms for combinatorial problems. *J. of Computer and System Sciences* **9**(3), 256–278 (1974). [https://doi.org/10.1016/S0022-0000\(74\)80044-9](https://doi.org/10.1016/S0022-0000(74)80044-9)
14. Khot, S., Naor, A.: Linear Equations Modulo 2 and the $\$L_1\$$ Diameter of Convex Bodies. *SIAM J. Comput.* **38**(4), 1448–1463 (2008). <https://doi.org/10.1137/070691140>
15. MacWilliams, F.J., Sloane, N.J.A.: *The Theory of Error-Correcting Codes*. North Holland Publishing Co. (1977)
16. Nemirovski, A.S., Roos, C., Terlaky, T.: On maximization of quadratic form over intersection of ellipsoids with common center. *Math. Program.* **86**(3), 463–473 (1999). <https://doi.org/10.1007/s101070050100>
17. Nesterov, Y.: Semidefinite relaxation and nonconvex quadratic optimization. *Optimization Methods and Software* **9**(1–3), 141–160 (1998). <https://doi.org/10.1080/10556789808805690>