SUPPLEMENTARY MATERIALS: DERIVING DIFFERENTIAL APPROXIMATION RESULTS FOR K CSPS FROM COMBINATORIAL DESIGNS *

JEAN-FRANÇOIS CULUS† AND SOPHIE TOULOUSE‡

Notations. For a positive integer j, we denote by e^j the jth canonical vector (of dimension depending on the context).

SM1. Functions families $\mathcal{E}_q$ and $\mathcal{O}_q$ introduced in subsection 1.5.

SM1.1. Function decomposition.

Let q, k be two positive integers. Analogously to the concept of even and odd functions, any function $P : (\Sigma_q, +)^k \to \mathbb{R}$ can be decomposed into the sum of a function of $\mathcal{E}_q$ and a function of $\mathcal{O}_q$. Namely, we associate with P the function $P_E := 1/q \times \sum_{a=0}^{q-1} P_{\mathbf{a}}$, which is defined on Σ_q^k by:

$$P_E(y) = \textstyle\sum_{a=0}^{q-1} P(y_1 + a, \ldots, y_k + a)/q, \qquad y_1, \ldots, y_k \in \Sigma_q \tag{SM1.1}$$

For example, expression $\sum_{a=0}^{q-1} AllZeros^{k,q}(y_1 + a, \ldots, y_k + a)$ evaluates 1 *iff*

$$y_1 + a \equiv \ldots \equiv y_k + a \equiv 0 \bmod q$$

holds for some $a \in \{0, \ldots, q-1\}$, what occurs *iff* $y_1, \ldots, y_k$ are all equal. Otherwise, it evaluates 0. Thus when P is $AllZeros^{k,q}$, P_E is $1/q \times AllEqual^{k,q}$.

P_E by construction is stable under the shift by a same quantity $a \in \Sigma_q$ of all its variables, while $P - P_E$ by construction satisfies that $\sum_{a=0}^{q-1}(P - P_E)_{\mathbf{a}}$ is the constant function zero. Observe that function $P - P_E$ actually can be decomposed into the sum of the $q-1$ functions $(P - P_{\mathbf{a}})/q$, $a \in \Sigma_q$ that all belong to $\mathcal{O}_q$, and have a mean value of zero.

Definitions (1.3) of $\mathcal{E}_q$ and (1.4) of $\mathcal{O}_q$ precisely state that $P \in \mathcal{E}_q$ *iff* $P_E = P$, and $P \in \mathcal{O}_q$ *iff* P_E is constant (in which case P_E necessarily is the constant function r_P).

SM1.2. Restrictions $\mathsf{CSP}(\mathcal{O}_\mathsf{q})$ and $\mathsf{CSP}(\mathcal{E}_\mathsf{q})$ of $\mathsf{CSP}{-}\mathsf{q}$.

$\mathsf{CSP}(\mathcal{O}_\mathsf{q})$ is remarkable in that it is trivially approximable within differential factor of $1/q$ (see subsections 2.1 and 4.1), but **NP − hard** to approximate within any constant factor greater than $1/q$, and this even for $\mathsf{E3\,CSP}(\mathcal{O}_\mathsf{q})$ [SM8].

Regarding $\mathsf{CSP}(\mathcal{E}_\mathsf{q})$, we observe that, given a positive integer k, we can interpret any function P on Σ_q^k as a $(k+1)$-ary function of $\mathcal{E}_q$. Namely, we associate with P the function P^E which is defined on Σ_q^{k+1} by:

$$\begin{aligned} P^E(y_0, y_1, \ldots, y_k) &:= P_{-\mathbf{y_0}}(y_1, \ldots, y_k) \\ &= P(y_1 - y_0, \ldots, y_k - y_0), \quad y_0, y_1, \ldots, y_k \in \Sigma_q \end{aligned} \tag{SM1.2}$$

For example, consider the function $AllZeros^{k,q}$. Given $y_0, y_1, \ldots, y_k \in \Sigma_q$, we have:

$$(y_1 - y_0 \equiv \ldots \equiv y_k - y_0 \equiv 0 \bmod q) \quad \textit{iff} \quad (y_1 = \ldots = y_k = y_0)\,.$$

Thus when $P = AllZeros^{k,q}$, $P^E = AllEqual^{k+1,q}$.

---

*Submitted to the editors June 8, 2024. Prelimary versions of this work have been communicated or published in conferences [SM5, SM4, SM3].

†MEMIAD, UA, Crec Saint-Cyr, France (jean-francois.culus@st-cyr.terre-net.defense.gouv.fr).

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

TABLE SM1
Linear programs for orthogonal arrays and balanced t-wise independent measures.

$\rho(\nu,q,t) = \begin{cases} \max_{P:\Sigma_q^\nu \to [0,1], R} P(\mathbf{0}) \\ s.t. \quad \text{(SM2.1)–(SM2.3)} \\ \quad\quad R = 1 \end{cases}$	$F(\nu,q,t) = \begin{cases} \min_{P:\Sigma_q^\nu \to \mathbb{N}, R} R \\ s.t. \quad \text{(SM2.1)–(SM2.3)} \\ \quad\quad R \geq 1 \end{cases}$
$R(\nu,q,t) = \begin{cases} \min_{P:\Sigma_q^\nu \to \mathbb{N}, R} R \\ s.t. \quad \text{(SM2.1)–(SM2.3)} \\ \quad\quad P(\mathbf{0}) \geq \rho(\nu,q,t) \times R \\ \quad\quad R \geq 1 \end{cases}$	$R^*(\nu,q,t) = \begin{cases} \max_{P:\Sigma_q^\nu \to \mathbb{N}} P(\mathbf{0}) \\ s.t. \quad \text{(SM2.1)–(SM2.3)} \\ \quad\quad R = F(\nu,q,t) \end{cases}$

We derive from transformation (SM1.2) a differential approximation preserving reduction (f,g) (see subsection 3.1) from $\mathsf{k\,CSP{-}q}$ to $\mathsf{(k+1)CSP}(\mathcal{E}_\mathsf{q})$ that induces no loss on the approximation guarantee. Given an instance I of $\mathsf{k\,CSP{-}q}$, algorithm f introduces an auxiliary variable z_0, and substitutes for each constraint $P_i(x_{i_1},\ldots,x_{i_{k_i}})$ of the input instance the new constraint $P_i(x_{i_1}-z_0,\ldots,x_{i_{k_i}}-z_0)$. Algorithm $g(I,.)$ then associates with a solution $(x,z_0)=(x_1,\ldots,x_n,z_0)$ of $f(I)$ the solution $x-\mathbf{z_0}=(x_1-z_0,\ldots,x_n-z_0)$ of I. By definition of $f(I)$, this solution performs on I the same objective value as (x,z_0) on $f(I)$.

Examples of this reduction are provided in [SM10, SM6], when functions P_i are either the disjunction on k boolean variables, or its generalization to q-ary alphabets. Precisely, $\mathsf{NAE\,Sat{-}q}$ and $\mathsf{Sat{-}q}$ are the q-ary CSPs in which a constraint requires that a set of literals are not all equal for the former problem, are not all zero for the latter problem, where a literal ℓ_j is either the variable x_j or its shift x_j+a by some constant integer $a\in[q-1]$ (*e.g.* see [SM2]). Then we have $\mathsf{k\,Sat{-}q} \leq_D^1 \mathsf{(k+1)NAE\,Sat{-}q}$ [SM10, SM6]. Moreover, in Property 4.3 of subsection 4.2, we analyse reduction (f,g), when applied to $\mathsf{2\,CSP{-}2}$, with respect to the differential ratio reached at local optima w.r.t. $\tilde{B}^1$ and solutions of optimal value over any subset $\tilde{B}^1(x)$ of solutions.

Considering that $\mathsf{(k+1)CSP}(\mathcal{E}_\mathsf{q})$ is a special case of $\mathsf{(k+1)CSP{-}q}$, this reduction somehow indicates that $\mathsf{(k+1)CSP}(\mathcal{E}_\mathsf{q})$ can be viewed as an intermediate problem between $\mathsf{k\,CSP{-}q}$ and $\mathsf{(k+1)CSP{-}q}$.

SM2. Computation of optimum designs of sections 2 and 3. We explain how we computed the arrays and the values of Tables 4 to 7, 9, and 10.

SM2.1. Orthogonal arrays and difference schemes. Let $q\geq 1$, $t\geq 1$, $\nu\geq t$ be three integers. To model orthogonal arrays of strength t with ν columns on symbol set Σ_q, we associate with each $u\in\Sigma_q^\nu$ a variable $P(u)$ that represents either the number of occurrences or the frequency of u in the array, depending on whether we model the array itself or the measure it induces on Σ_q^ν. These variables therefore have domain $\mathbb{N}$ or $[0,1]$, depending on the context. We use an additional variable R to represent either the number of rows in the array (in which case R must be ≥ 1), or the overall frequency of words from Σ_q^ν in the array (in which case R must be 1). To prevent symmetries, we only consider arrays in which the all-zeros row is of maximum frequency. Accordingly, variables $P(u)$, $u\in\Sigma_q^\nu$ and R shall always satisfy:

$$\text{(SM2.1)} \qquad \sum_{u\in\Sigma_q^\nu} P(u) = R$$

$$\text{(SM2.2)} \qquad P(\mathbf{0}) \geq P(u), \qquad u\in\Sigma_q^\nu$$

$$\text{(SM2.3)} \qquad \sum_{u\in\Sigma_q^\nu : u_J = v} P(u) = R/q^t, \qquad J\subseteq[\nu], |J| = t, v\in\Sigma_q^t$$

(SM2.3) ensures that the array induces a balanced t-wise independent distribution over Σ_q^ν. When the variables are integer, depending on the optimization goal, we consider the additional constraint $R \geq 1$ so as to forbid the trivial solution $R = P(u) = 0, u \in \Sigma_q^\nu$.

We considerer two optimization criterions: the number of rows (that we aim at minimizing), and the maximal frequency of a word (that we aim at maximizing). We are more specifically interested in:

1. computing $\rho(\nu, q, t)$, which can be achieved by solving the top left linear program in continuous variables of Table SM1;
2. minimizing the number of rows in an array that realizes $\rho(\nu, q, t)$, which can be done by solving the bottom left program of Table SM1 with the parameter ρ set to $\rho(\nu, q, t)$;
3. computing $F(\nu, q, t)$, which can be achieved by solving the top right program of Table SM1;
4. maximizing the maximal frequency in an $OA(F(\nu, q, t), \nu, q, t)$, which can be done by solving the bottom right program of Table SM1.

Due to numerical approximations, the value found for $\rho(\nu, q, t)$ could be inaccurate. When this happens, we compute $R(\nu, q, t)$ with a wrong value for $\rho(\nu, q, t)$. Let M refer to the array obtained when computing $R(\nu, q, t)$. Let R_M and R_M^* represent the number of rows and the multiplicity of the row of all-zeros in M, respectively. M indeed achieves $\rho(\nu, q, t)$ *iff* in any orthogonal array of strength t with ν columns on symbol set Σ_q, the highest frequency of a row is at most R_M^*/R_M. Equivalently, there is no such OA in which the highest frequency of a row is strictly greater than R_M^*/R_M. We deduce that M achieves $\rho(\nu, q, t)$ provided that the linear program below admits no feasible solution:

$$\begin{cases} \max_{P:\Sigma_q^\nu \to \mathbb{N}, R} 0 & \\ s.t. & \text{(SM2.1)–(SM2.3)} \\ \quad R_M \times P(\mathbf{0}) & \geq R_N^* \times R + 1 \end{cases}$$

Hence, to increase our confidence in the optimality of the arrays we have computed for $\rho(\nu, q, t)$, we additionally have solved this problem.

The case of difference schemes is rather similar. First, in order to avoid symmetries, we associate a variable $P(u)$ only to the words $u \in \Sigma_q^\nu$ with a zero first coordinate. Second, rather than constraints (SM2.3), we consider for all $J \subseteq [\nu]$ with $|J| = t$ and all $v \in \{0\} \times \Sigma_q^{t-1}$ the constraint:

$$\text{(SM2.4)} \qquad \textstyle\sum_{a=0}^{q-1} \sum_{u \in \{0\} \times \Sigma_q^{\nu-1} : u_J = v + \mathbf{a}} P(u) = R/q^{t-1}$$

SM2.2. Designs of section 3. Let $k \geq 2$, $p \geq k$, $q > p$ be three integers. Let $\mathcal{U}$ be the set of words $u \in \Sigma_q^q$ with at most p distinct coordinates. In order to compute $\gamma(q, p, k)$ and to exhibit pairs of arrays that achieve $\gamma(q, p, k)$, we consider variables $P(u)$, $u \in \mathcal{U}$, $Q(u)$, $u \in \Sigma_q^q$ and R, so as to model the array Ψ (or frequencies in array Ψ), the array Φ (or frequencies in array Φ) and the number of rows in these arrays (or the overall frequency of words of Σ_q^q in these arrays, which equals 1), respectively. These variables must satisfy that R coincides with $\sum_{u \in \mathcal{U}} P(u)$, and:

$$\text{(SM2.5)} \qquad \textstyle\sum_{u \in \mathcal{U} : u_J = v} P(u) = \sum_{u \in \Sigma_q^q : u_J = v} Q(u), \qquad J \subseteq \Sigma_q, |J| = k, v \in \Sigma_q^k$$

The case of families $\Gamma_E(R, R^*, q, p, k)$ is rather similar. First, we eliminate symmetrical solutions by restricting the variables $P(u)$ and $Q(u)$ to words u of Σ_q^q such that $u_0 = 0$. Secondly, instead of the constraints (SM2.5), we consider for all $J \subseteq \Sigma_q$ with $|J| = k$ and all $v \in \{0\} \times \Sigma_q^{k-1}$ the constraint:

$$\sum_{a=0}^{q-1} \sum_{u \in \mathcal{U}: u_0 = 0 \wedge u_J = v + \mathbf{a}} P(u) = \sum_{a=0}^{q-1} \sum_{u \in \Sigma_q^q: u_0 = 0 \wedge u_J = v + \mathbf{a}} Q(u) \tag{SM2.6}$$

For both problems, the goal is to maximize the ratio $Q(0, 1, \ldots, q-1)/R$. We handle the fractional objective function in the same way as for orthogonal arrays and difference schemes.

SM3. Proof of relations (2.15) and (2.16) of section 2.

SM3.1. Proof of relations (2.15). In subsection 2.5, we claim that Property 2.5 implies the following inequalities related to orthogonal arrays on Σ_q and difference schemes based on $(\mathbb{Z}_q, +)$:

$$\left\{ \begin{array}{llll} E(\nu, q, t) & \leq F(\nu - 1, q, t) & \leq 1/q \times F(\nu, q, t+1) & \leq E(\nu, q, t+1) \\ \rho_E(\nu, q, t) & \geq \rho(\nu - 1, q, t) & \geq q \times \rho(\nu, q, t+1) & \geq \rho_E(\nu, q, t+1) \end{array} \right. \tag{2.15}$$

We argue why that claim is correct.

Proof. First consider array $B(M)$. By definition (2.13) of $B(M)$, we have:

$$\sum_{a=0}^{q-1} \mu^{B(M)}(\mathbf{a}) \quad = \mu^{B(M)}(\mathbf{0}) \quad = \mu^M(\mathbf{0})$$

Item 2 of Property 2.5 therefore establishes the left-hand side inequalities of (2.15). Now consider array $C(M)$. Observe that a row M_r of M gives rise to a row of all-zeros in $C(M)$ *iff* $M_r^1 + a = \ldots = M_r^\nu + a = 0$ holds for some $a \in \Sigma_q$, what occurs *iff* the components of M_r are all equal. This lead to:

$$\mu^{C(M)}(\mathbf{0}) \quad = (\textstyle\sum_{a=0}^{q-1} R \times \mu^M(\mathbf{a}))/(qR) \quad = 1/q \times \sum_{a=0}^{q-1} \mu^M(\mathbf{a})$$

(where, for $a \in \Sigma_q$, $R\mu^M(\mathbf{a})$ counts the number of times $\mathbf{a}$ occurs as a row in M). Item 3 of Property 2.5 therefore establishes the right-hand side inequalities of (2.15). Finally consider array $A(M)$. If M is an $OA(R, \nu, q, t)$ with $t > 0$, then M is an $OA(R, \nu, q, 1)$ and thus, $M_r^\nu = 0$ holds for R/q indices $r \in [R]$. Hence, provided that M is an OA, we have:

$$\mu^{A(M)}(\mathbf{0}) \quad = (R \times \mu^M(\mathbf{0}))/(R/q) \quad = q \times \mu^M(\mathbf{0})$$

(where $R\mu^M(\mathbf{0})$ counts the number of rows of all-zeros in M). Item 1 of Property Property 2.5 therefore establishes the middle inequalities of (2.15). ∎

SM3.2. Proof of Property 2.6. Relations (2.16) are a straightforward consequence of relations (2.15) and Property 2.6 which states that, over a binary alphabet, difference schemes with ν factors of even strength $2t < \nu$ actually have strength $2t+1$.

Proof. The proof can be found in [SM7]. Let M be a $D_{2t}(R, \nu, 2)$ where t and ν are two positive integers such that $\nu > 2t$. Given a $(2t+1)$-cardinality subset $J = (j_1, \ldots, j_{2t+1})$ of $[\nu]$ and a vector $v \in \{0, 1\}^{2t+1}$, we denote by $R(J, v)$ the number of rows of M that coincide with v or $\bar{v}$ on their coordinates with index in J. That is, $R(J, v)$ counts the rows M_r of M satisfying either $M_r^J = v$ or $M_r^J = \bar{v}$.

Consider such a pair (J, v) long with an index $s \in [2t+1]$. Observe that $R(J, v) + R(J, v + e^s)$ counts the number of rows M_r of M that satisfy:

$$\begin{array}{r} \left(M_r^{j_1}, \ldots, M_r^{j_{s-1}}, M_r^{j_{s+1}}, \ldots, M_r^{j_{2t+1}}\right) = (v_1, \ldots, v_{s-1}, v_{s+1}, \ldots, v_{2t+1}) \\ \vee \left(M_r^{j_1}, \ldots, M_r^{j_{s-1}}, M_r^{j_{s+1}}, \ldots, M_r^{j_{2t+1}}\right) = (\bar{v}_1, \ldots, \bar{v}_{s-1}, \bar{v}_{s+1}, \ldots, \bar{v}_{2t+1}) \end{array}$$

Since M is a $D_{2t}(R,\nu,2)$, it contains exactly $R/2^{2t-1}$ such rows. The following relation thus holds on M:

$$R(J,v)+R(J,v+e^s) \quad = R/2^{2t-1}, \qquad J\subseteq[\nu],\ |J|=2t+1,\ v\in\{0,1\}^{2t+1},\ s\in[2t+1] \tag{SM3.1}$$

From (SM3.1), we deduce:

$$\begin{aligned}
&\textstyle\sum_{s=1}^{2t+1} R\left(J,v+\sum_{i=1}^{s} e^i\right)\\
&\quad=\textstyle\sum_{s=1}^{t}\left(R(J,v+\sum_{i=1}^{2s-1} e^i)+R(J,v+\sum_{i=1}^{2s} e^i)\right)+R(J,\bar v)\\
&\quad=t\times R/2^{2t-1}+R(J,\bar v)\\
&\textstyle\sum_{s=1}^{2t+1} R\left(J,v+\sum_{i=1}^{s} e^i\right)\\
&\quad=R(J,v+e^1)+\textstyle\sum_{s=1}^{t}\left(R(J,v+\sum_{i=1}^{2s} e^i)+R(J,v+\sum_{i=1}^{2s+1} e^i)\right)\\
&\quad=R(J,v+e^1)+t\times R/2^{2t-1}
\end{aligned}$$

Since $R(J,\bar v)=R(J,v)$, we consequently have:

$$R(J,v) \quad = R(J,v+e^1) \quad = \left(R(J,v)+R(J,v+e^1)\right)/2$$

It thus again follows from (SM3.1) that $R(J,v)$ equals $R/2^{2t}$: the proof is complete. ∎

SM4. Approximability bounds of Tables 1 and 13 (introducing and concluding section).

In subsection 1.2, we claim that the 6-gadget of [SM8] reducing $\mathsf{E3\,Lin}-2$ to $\mathsf{E2\,Lin}-2$ implies a differential approximability upper bound of $7/8$ for $\mathsf{Bipartite\,E2\,Lin}-2$. Moreover, Table 13 reports approximability bounds for the restriction of $\mathsf{E2\,CSP}(\mathcal{I}_2^1)$ to bipartite instances, as well as for $\mathsf{E3\,CSP}(\mathcal{I}_2^2)$. We show that these statements are correct.

SM4.1. The gain and the differential approximation measures on bipartiate instances of $\mathsf{E2\,Lin}-2$.

First, on bipartie instances of $\mathsf{Bipartite\,E2\,Lin}-2$, approximating the optimum gain over a random assignment or approximating the optimum gain over a worst solution somehow reduce to the same:

Property SM4.1. A solution of a bipartite instance of $\mathsf{E2\,Lin}-2$ is g-gain approximate if and only if it is $(1/2+g/2)$-differential approximate.

Proof. Let I be an instance of $\mathsf{Bipartite\,E2\,Lin}-2$, and (L,R) be a 2-coloring of I. Any two solutions x and y such that $y_L=x_L$ and $y_R=\bar x_R$ satisfy $v(I,x)+v(I,y)=\sum_{i=1}^m w_i$. In particular, we have $\mathrm{opt}(I)+\mathrm{wor}(I)=\sum_{i=1}^m w_i = 2\times\mathbb{E}_X[v(I,X)]$. Equivalently:

$$\mathbb{E}_X[v(I,X)]-\mathrm{wor}(I) \quad = \mathrm{opt}(I)-\mathbb{E}_X[v(I,X)] \quad = \left(\mathrm{opt}(I)-\mathrm{wor}(I)\right)/2 \tag{SM4.1}$$

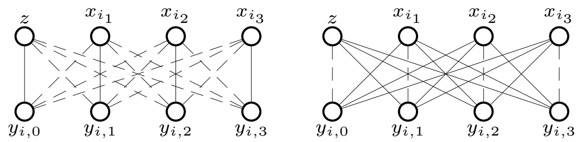
We deduce:

$$\frac{v(I,x)-\mathrm{wor}(I)}{\mathrm{opt}(I)-\mathrm{wor}(I)} \quad = \frac{v(I,x)-\mathbb{E}_X[v(I,X)]}{2\left(\mathrm{opt}(I)-\mathbb{E}_X[v(I,X)]\right)}+\frac{\mathbb{E}_X[v(I,X)]-\mathrm{wor}(I)}{2\left(\mathbb{E}_X[v(I,X)]-\mathrm{wor}(I)\right)}$$

The result is straightforward. ∎

In [SM1], Alon and Naor show that on instances of $\mathsf{Bipartite\,E2\,Lin}-2$, the optimum gain over a random assignment is approximable within a factor of $2\ln(1+\sqrt{2})/\pi$. According to Property SM4.1, equivalently, they show that $\mathsf{Bipartite\,E2\,Lin}-2$ is approximable within a differential factor of $1/2+\ln(1+\sqrt{2})/\pi$.

FIG. SM1. *6-gadget of [SM8] transforming each constraint ($x_{i_1} + x_{i_2} + x_{i_3} \equiv a_i \bmod 2$) of an instance I of* Max E3 Lin−2 *to a set of $XNOR^2$ (pictured in plain lines) and XOR^2 (pictured in dashed lines) constraints.*



gadget in case where $\alpha_{i,0} = 1$ gadget in case where $\alpha_{i,0} = 0$

SM4.2. Ek CSP($\mathcal{I}_2^{k-1}$) is Ek Lin−2. Second, over the boolean alphabet, given any positive integer k, the k-ary balanced $(k-1)$-wise independent boolean functions are functions of the form $aXNOR^k + b$ where a, b are any constant reals:

Property SM4.2. Let $k \geq 1$ be an integer. Then a function $P : \{0,1\}^k \to \mathbb{R}$ is balanced $(k-1)$-wise independent *iff* P coincides, up to an affine transformation, with $XNOR^k$.

Proof. Consider two boolean vectors $u, v \in \{0,1\}^k$ such that $XNOR^k(u) = XNOR^k(v)$. We denote by $J = \{j_1, \ldots, j_\kappa\}$ the set of coordinate indices on which u and v differ. Thus v can be described as the vector $u + \sum_{r=1}^{\kappa} e^{j_r}$ where, by assumption $XNOR^k(u) = XNOR^k(v)$, κ is even. Therefore, we can write $P(v) - P(u)$ as:

$$\begin{aligned} P(v) - P(u) &= P\left(u + \textstyle\sum_{r=1}^{\kappa} e^{j_r}\right) - P(u) \\ &= \textstyle\sum_{s=1}^{\kappa/2} \left(P(u + \sum_{r=1}^{2s} e^{j_r}) - P(u + \sum_{r=1}^{2s-2} e^{j_r})\right) \end{aligned}$$

Let $s \in [\kappa/2]$. By assumption $P \in \mathcal{I}_k^{k-1}$, we can successively deduce from (1.2) that we have:

$$P(u + \textstyle\sum_{r=1}^{2s} e^{j_r}) \quad = 2r_P - P(u + \sum_{r=1}^{2s-1} e^{j_r}) \quad = P(u + \sum_{r=1}^{2s-2} e^{j_r})$$

We conclude that P takes the same value on all vectors u with $XNOR^k(u) = 1$ on the one hand, on all vectors u with $XNOR^k(u) = 0$ on the other hand. In other words, there exist two reals a, b such that P is the function $a \times XNOR^k + b \times XOR^k$ or, equivalently, $(a-b)XNOR^k + b$. ∎

In [SM9], Khot and Naor show that on instances of E3 Lin−2, the optimum gain over a random assignment is approximable within an expected factor of $\Omega(\sqrt{\ln n/n})$. According to Property SM4.2, the approximability bounds of [SM1] and [SM9] actually hold for respectively Bipartite E2 CSP($\mathcal{I}_2^1$) and E3 CSP($\mathcal{I}_2^2$).

SM4.3. Inapproximability bounds for Bipartite E2 Lin−2. Finally, the 6-gadget of [SM8] reducing E3 Lin−2 to E2 Lin−2 implies an approximability upper bound of 3/4 for the optimum gain over a random assignment on bipartite instances of E2 Lin−2:

PROPOSITION SM4.3. *If* Bipartite E2 Lin−2 *is approximable within some constant gain factor greater than* 3/4*, then* $\mathbf{P} = \mathbf{NP}$.

Proof. Consider an instance I of Max E3 Lin−2. The reduction of [SM8] first introduces $4m + 1$ auxiliary binary variables z and $y_{i_0}, y_{i_1}, y_{i_2}, y_{i_3}$, $i \in [m]$. It then generates for each constraint

$$x_{i_1} + x_{i_2} + x_{i_3} \equiv a_i \bmod 2$$

of I sixteen equations, all of weight $w_i/2$. These equations are depicted in Figure SM1. We denote by I' the resulting instance of $\mathsf{Max\,E2\,Lin}-2$, by $w(I)$ and $w(I')$ the sum of the constraint weights on respectively I and I'. Then the I' obviously is bipartite. Furthermore, we have [SM8]:

$$w(I') = 8w(I) \tag{SM4.2}$$

$$v(I,x) \geq v(I',(x,y,0)) - 5w(I), \qquad (x,y) \in \{0,1\}^{n+4m} \tag{SM4.3}$$

$$v(I,\bar{x}) \geq v(I',(x,y,1)) - 5w(I), \qquad (x,y) \in \{0,1\}^{n+4m} \tag{SM4.4}$$

$$\mathrm{opt}(I') = \mathrm{opt}(I) + 5w(I) \tag{SM4.5}$$

The reduction finally associates with a solution (x,y,z) of I' the solution x if $z=0$, $\bar{x}$ otherwise of I.

Assume that we can compute on I' a solution (x,y,z) which is ε-gain approximate, where ε is some positive constant. As solutions (x,y,z) and $(\bar{x},\bar{y},\bar{z})$ perform on I' the same objective value, we can assume without loss of generality that $z=0$. Consider then solution x of I. We successively observe:

$$\begin{aligned} v(I,x) &\geq v(I',(x,y,z)) - 5w(I) && \text{by (SM4.3)}\\ &\geq \varepsilon\,\mathrm{opt}(I') + (1-\varepsilon)\times w(I')/2 - 5w(I) && \text{by assumption on } (x,y,z)\\ &= \varepsilon\,(\mathrm{opt}(I) + 5w(I)) + (1-\varepsilon)4w(I) - 5w(I) && \text{by (SM4.2) and (SM4.5)}\\ &= \varepsilon\,\mathrm{opt}(I) - (1-\varepsilon)w(I) \end{aligned}$$

Now, for all constant $\delta > 0$, $\mathsf{Gap}_{(1-\delta,1/2+\delta)}\mathsf{CSP}(\{\mathsf{XNOR}^3,\mathsf{XOR}^3\})$ is **NP**-hard [SM8]. This means that, given an instance I of $\mathsf{Max\,E3\,Lin}-2$ verifying either $\mathrm{opt}(I) \geq (1-\delta)w(I)$ or $\mathrm{opt}(I) \leq (1/2+\delta)w(I)$, deciding which of these two cases occurs is **NP**-hard.

Let $\delta > 0$, and consider such an instance I. The preceding observations indicate that, in case where $\mathrm{opt}(I) \geq (1-\delta)w(I)$, $v(I,x)$ satisfies:

$$v(I,x) \quad \geq \varepsilon \times (1-\delta)w(I) - (1-\varepsilon)w(I) \quad = w(I) \times ((2-\delta)\varepsilon - 1)$$

By contrast, if $\mathrm{opt}(I) \leq (1/2+\delta)w(I)$, then we have:

$$v(I,x) \quad \leq \mathrm{opt}(I) \quad \leq (1/2+\delta)w(I)$$

Eventually observe that $(2-\delta)\varepsilon - 1 > 1/2 + \delta$ *iff* $\delta < (2\varepsilon - 3/2)/(1+\varepsilon)$, while $(2\varepsilon-3/2)/(1+\varepsilon) > 0$ *iff* $\varepsilon > 3/4$. Hence, if $\varepsilon > 3/4$, then for small enough δ, we can decide whether $\mathrm{opt}(I) \geq (1-\delta)w(I)$ or $\mathrm{opt}(I) \leq (1/2+\delta)w(I)$ by comparing $v(I,x)$ to $(1/2+\delta)w(I)$: contradiction. ∎

According to Property SM4.1, Proposition SM4.3 equivalently indicates that $\mathsf{Bipartite\,E2\,Lin}-2$ is inapproximable within any constant differential factor greater than 7/8, unless $\mathbf{P} = \mathbf{NP}$.

SM5. Combinatorial designs of sections 3 and 4.

SM5.1. Proof of Theorem 3.8. Consider Algorithm 3.1. Our goal is to prove that, at the end of the algorithm, the difference $\mu_\Psi - \mu_\Phi$ of the frequencies of rows occurring in Ψ and Φ is balanced k-wise independent. To that end, we first establish a technical lemma.

Lemma SM5.1. *For three natural numbers a, b and $c \leq b$, we define:*

$$S(a,b,c) := \textstyle\sum_{r\geq 0}(-1)^r\binom{a}{r}\binom{b-r}{c-r} \tag{SM5.1}$$

These numbers satisfy the following identity:

$$S(a,b,c) = \binom{b-a}{c}, \qquad a,b,c \in \mathbb{N},\ b \geq a,\ c \leq b \tag{SM5.2}$$

Proof. By induction on integer b. Let $a \in \mathbb{N}$. For all $c \in \{0,\dots,a\}$, considering identity $\binom{a}{r}\binom{a-r}{c-r} = \binom{a}{c}\binom{c}{r}$, $r \in \mathbb{N}$, we have:

$$S(a,a,c) = \binom{a}{c} \times \sum_{r=0}^{c} (-1)^r \binom{c}{r}$$

We deduce that $S(a,a,c)$ equals 1 if $c = 0$ and 0 otherwise, just as the same as $\binom{0}{c}$. Identity (SM5.2) therefore is satisfied at rank (a,a,c) for all natural numbers $c \leq a$. Now suppose that it is satisfied at rank $(a,b-1,c)$ for all natural numbers $c \leq b-1$, where b is some integer greater than a. We consider rank (a,b,c) where $c \in \{0,\dots,b\}$. If $c = 0$, then $S(a,b,0) = (-1)^0\binom{a}{0}\binom{b}{0} = 1 = \binom{b-a}{0}$. If $c = b$, we have:

$$S(a,b,b) = \sum_{r=0}^{a} (-1)^r \binom{a}{r}\binom{b-r}{b-r} = \sum_{r=0}^{a} (-1)^r \binom{a}{r}$$

Thus $S(a,b,b)$ equals 1 if $a = 0$ and 0 otherwise, just as the same as $\binom{b-a}{b}$. Now assume $c > 0$ and $c < b$. In this case, we successively deduce:

$$\begin{aligned} S(a,b,c) &= \textstyle\sum_{r\geq 0} (-1)^r \binom{a}{r} \left(\binom{b-1-r}{c-r} + \binom{b-1-r}{c-1-r} \right) && \text{by Pascal's rule} \\ &= S(a,b-1,c) + S(a,b-1,c-1) && \text{according to (SM5.1)} \\ &= \binom{b-a-1}{c} + \binom{b-a-1}{c-1} && \text{by induction hypothesis} \end{aligned}$$

Thus $S(a,b,c) = \binom{b-a}{c}$, what completes the argument. ∎

We now prove that $\mu_\Psi - \mu_\Phi$ is balanced k-wise independent.

Proof. Consider a k-cardinality subset J of Σ_{q-1}. Since (Ψ,Φ) initially belongs to $\Gamma(R,R^*,q-1,k,k)$, subarrays

$$(\Psi_r^J \mid r \in [R]) \text{ and } (\Phi_r^J \mid r \in [R])$$

are the same multisets of rows. The same holds for subarrays

$$(\Psi_r^J \mid R < r \leq R + R^*\Delta) \text{ and } (\Phi_r^J \mid R < r \leq R + R^*\Delta),$$

due to the shape of the rows inserted by the construction. Therefore, it remains for us to show for all sequences $J = (j_1,\dots,j_{k-1})$ of $k-1$ pairwise distinct symbols from Σ_{q-1} and all $v \in \Sigma_q^k$ that subarrays (Ψ^J,Ψ^{q-1}) and (Φ^J,Φ^{q-1}) both coincide with v on the same number of rows. We consider three cases:

- $v \notin \{j_1,q-1\} \times \dots \times \{j_{k-1},q-1\} \times \{0,q-1\}$: by construction, given $M \in \{\Psi,\Phi\}$, $(M_r^J, M_r^{q-1}) = v$ might not occur unless $r \leq R$ and $(M_r^J, M_r^{q-1}) = (M_r^J, M_r^0)$. Subarrays (Ψ^J,Ψ^{q-1}) and (Φ^J,Φ^{q-1}) therefore both coincide with v on the same number of rows, due to the initial assumption on (Ψ,Φ).
- $(v_1,\dots,v_{k-1}) = J$ and $v_k \in \{0,q-1\}$. If $v_k = q-1$, then the R^* occurrences of row $(0,1,\dots,q-1)$ in Φ, and the R^* occurrences of row $(\alpha(J),q-1)$ in Ψ, are the only rows of the two arrays that coincide with v on their indices in $(J,q-1)$. Otherwise (thus $v_k = 0$), let X be the number of rows Φ_r of Φ that initially satisfy $(\Phi_r^J,\Phi_r^0) = v$. In array Φ, the rows Φ_r that satisfy $(\Phi_r^J,\Phi_r^{q-1}) = v$ are all but R^* of the rows Φ_r with $r \in [R]$ that initially satisfy $(\Phi_r^J,\Phi_r^0) = v$, and the rows $(\alpha(J),0)$. The number of such rows therefore is $(X - R^*) + R^* = X$. In array Ψ, the rows Ψ_r that satisfy $(\Psi_r^J,\Psi_r^{q-1}) = v$ are precisely the rows that initially satisfy $(\Psi_r^J,\Psi_r^0) = v$. Since $\mu_\Psi - \mu_\Phi$ is initially balanced k-wise independent, Ψ contains X such rows.
- $v \in \{j_1,q-1\} \times \dots \times \{j_{k-1},q-1\} \times \{0,q-1\}$ and $(v_1,\dots,v_{k-1}) \neq J$. Since $(v_1,\dots,v_{k-1})$ has at least one coordinate equal to $q-1$, given $M \in \{\Psi,\Phi\}$,

$(M_r^J, M_r^{q-1}) = v$ might not occur unless $r > R$. We thus count the number of rows of the form $(\alpha(H), v_k)$ that satisfy $\alpha(H)^J = (v_1, \ldots, v_{k-1})$. Let L refer to the set of indices $j_s \in J$ such that $v_s = j_s$. Then observe that $\alpha(H)^J = (v_1, \ldots, v_{k-1})$ provided that $L \subseteq H$ and $H \cap (J \backslash L) = \emptyset$. If $|L| = \ell$, the number of such subsets H of Σ_{q-1} of a given size $h \leq k-1$ is equal to $\binom{q-k}{h-\ell}$. The construction therefore generates for each natural number $h \leq k-1$ $R^* \times \binom{q-h-2}{k-h-1} \times \binom{q-k}{h-\ell}$ rows of the form $(\alpha(H), v_k)$ with $|H| = h$ that coincide with v on their coordinates in $(J, q-1)$. These rows are inserted in Ψ if either h has the same parity as $k-1$ and $v_k = q-1$, or h has not the same parity as $k-1$ and $v_k = 0$; otherwise, there are inserted in Φ. Hence, we have:

$$
\begin{aligned}
&|\{r \in [R + R^*\Delta] \mid \Psi_r^J = v\}| - |\{r \in [R + R^*\Delta] \mid \Phi_r^J = v\}| \\
&\quad = R^* \times \begin{cases} \sum_{h=\ell}^{k-1} (-1)^{k-1-h} \binom{q-k}{h-\ell} \binom{q-2-h}{k-1-h} & \text{if } v_k = q-1 \\ -\sum_{h=\ell}^{k-1} (-1)^{k-1-h} \binom{q-k}{h-\ell} \binom{q-2-h}{k-1-h} & \text{if } v_k = 0 \end{cases}
\end{aligned} \tag{SM5.3}
$$

By definition of L and the assumption $(v_1, \ldots, v_{k-1}) \neq J$, ℓ is some integer in $\{0, \ldots, k-2\}$. On the one hand, given any such ℓ, we have:

$$
\begin{aligned}
\sum_{h=\ell}^{k-1} (-1)^{k-1-h} \binom{q-k}{h-\ell} \binom{q-2-h}{k-1-h} &= \sum_{j=0}^{k-1-\ell} (-1)^{k-1-\ell-j} \binom{q-k}{j} \binom{q-2-\ell-j}{k-1-\ell-j} \\
&= (-1)^{k-1-\ell} \times S(q-k, q-2-\ell, k-1-\ell)
\end{aligned}
$$

On the other hand, according to identity (SM5.2), we have:

$$
S(q-k, q-2-\ell, k-1-\ell) \quad = \binom{k-2-\ell}{k-1-\ell} = \quad 0, \quad \ell \in \{0, \ldots, k-2\}
$$

We conclude that Ψ and Φ do satisfy that $\mu^\Psi - \mu^\Phi$ is balanced k-wise independent: the proof is now complete. ∎

SM5.2. Proof of identity (4.23). Let $k \geq 1$ and $\nu > k$ be two integers, and let (Ψ, Φ) be the pair of boolean $(T(\nu, k) + 1)/2 \times \nu$ arrays obtained by applying map σ_ν of Proposition 4.6 to the pair of arrays produced by Algorithm 3.2 on input (k, ν). We establish that (Ψ, Φ) can be described as follows:

- the word of all-ones occurs exactly once as a row in Φ;
- every $u \in \{0,1\}^\nu$ with a number $d \in \{0, \ldots, k\}$ of nonzero coordinates where $d \equiv k \bmod 2$ occurs exactly $\binom{\nu-1-d}{k-d}$ times as a row in Ψ;
- every $u \in \{0,1\}^\nu$ with a number $d \in \{0, \ldots, k\}$ of nonzero coordinates where $d \not\equiv k \bmod 2$ occurs exactly $\binom{\nu-1-d}{k-d}$ times as a row in Φ;
- any other ν-length boolean word occurs neither in Ψ nor in Φ.

Algorithm SM5.1 Construction for $\Delta\left((T(\nu, k) + 1)/2, \nu, k, k\right)$ given two positive integers k and $\nu > k$

$\Psi, \Phi \leftarrow \{\beta(k, [k])\}$
for $i = k+1$ **to** ν **do**
  Insert in Ψ and Φ a ith column of zeros
  Set the ith coefficient of the first row of Φ to 1
  for all $J \subseteq [i-1]$ with $|J| \leq k-1$ **do**
    Insert $\binom{i-2-|J|}{k-1-|J|}$ copies of $\beta(i, J \cup \{i\})$ in Ψ if $|J| \not\equiv k \bmod 2$, in Φ otherwise
    insert $\binom{i-2-|J|}{k-1-|J|}$ copies of $\beta(i, J)$ in Ψ if $|J| \equiv k \bmod 2$, in Φ otherwise
  end for
end for

Proof. For an integer $i \in \{k, \dots, \nu-1\}$ and a subset J of $[i]$, we denote by $\beta(i, J)$ the incidence vector of J viewed as a subset of $[i]$, i.e., the word of $\{0,1\}^i$ defined by:

$$\beta(i,J)_j = \begin{cases} 1 & \text{if } j \in J \\ 0 & \text{otherwise} \end{cases}, \qquad j \in [i]$$

In particular, $\beta(k,[k])$ and $\beta(\nu,[\nu])$ are the k-length and ν-length words of all-ones.

Applying transformation σ_ν to the arrays Algorithm 3.2 produces on input (k,ν) reduces to run Algorithm SM5.1 on (k,ν). Table 12 illustrates the construction when $k \in \{2,3\}$.

In order to establish identity (4.23), we count the number of occurrences of each word of $\{0,1\}^\nu$ in the resulting arrays Ψ and Φ. In Algorithm SM5.1, Line 1 first inserts a single occurrence of row $\beta(k,[k])$ in both arrays. Lines 3 and 4 then extend these partial rows into the rows $\beta(\nu,[k])$ and $\beta(\nu,[\nu])$ in respectively Ψ and Φ. At a given iteration $i \in \{k+1,\dots,\nu\}$, Lines 6 and 7 generate rows of the form $\beta(i,J)$ where J is an at most k-cardinality subset of $[i]$ such that $|J| < k$ or $i \in J$; Line 3 then extends each such partial row $\beta(i,J)$ into the row $\beta(\nu,J)$.

Thus consider a subset J of $[\nu]$, and the associated word $\beta(\nu,J)$. In the light of the above observations, if $|J| = \nu$, then $\beta(\nu,J)$ occurs once, in Φ. If $J = [k]$, then $\beta(\nu,J)$ occurs once, in Ψ. If $|J| \in \{k+1,\dots,\nu-1\}$, then $\beta(\nu,J)$ does not occur in neither Ψ, nor Φ. Thus assume that $|J| \le k$ and $J \ne [k]$. We denote by i^* the value 0 if $J = \emptyset$, the greatest integer in J otherwise. If $i^* > k$, then occurrences of $\beta(\nu,J)$ originate from the insertion by Line 6 at iteration i^* of rows $\beta(i^*,J)$. If $i^* < \nu$, then for all $i \in \{\max\{i^*,k\}+1,\dots,\nu\}$, occurrences of $\beta(\nu,J)$ originate from the insertion by Line 7 of rows $\beta(i,J)$ at iteration i. In both cases, these rows occur in Ψ if $|J| \equiv k \bmod 2$; otherwise, they occur in Φ.

Hence, on the one hand, copies of $\beta(\nu,J)$ all occur in the same array. On the other hand, the precise number of times $\beta(\nu,J)$ occurs in Ψ or Φ is equal to:

$$\begin{cases} \binom{\nu-|J|-1}{k-|J|} & \text{if } i^* = \nu \\ \sum_{i=k+1}^{\nu} \binom{i-|J|-2}{k-|J|-1} & \text{if } i^* < k \\ \binom{i^*-|J|-1}{k-|J|} + \sum_{i=i^*+1}^{\nu} \binom{i-|J|-2}{k-|J|-1} & \text{otherwise} \end{cases}$$

Now we trivially have given any $t \in \{k+1,\dots,\nu-1\}$:

$$\sum_{i=t}^{\nu} \binom{i-|J|-2}{k-|J|-1} = \sum_{i=t}^{\nu} \left(\binom{i-|J|-1}{k-|J|} - \binom{i-|J|-2}{k-|J|} \right) = \binom{\nu-|J|-1}{k-|J|} - \binom{t-|J|-2}{k-|J|}$$

We deduce that each ν-length boolean word with $d \in \{0,\dots,k\}$ nonzero coordinates is generated $\binom{\nu-d-1}{k-d}$ times, and occurs in the same array as the all-ones vector *iff* $k-d$ is odd. The argument is complete. ∎

REFERENCES

[SM1] N. Alon and A. Naor, *Approximating the cut-norm via grothendieck's inequality*, SIAM Journal on Computing, 35 (2006), pp. 787–803, https://doi.org/10.1137/S0097539704441629.

[SM2] P. Austrin and E. Mossel, *Approximation resistant predicates from pairwise independence*, Computational complexity, 18 (2009), pp. 249–271, https://doi.org/10.1007/s00037-009-0272-6.

[SM3] J. Culus and S. Toulouse, *How far from a worst solution a random solution of a kcsp instance can be?*, in Combinatorial Algorithms - 29th International Workshop, IWOCA 2018, Singapore, July 16-19, 2018, Proceedings, C. S. Iliopoulos, H. W. Leong, and W. Sung, eds., vol. 10979 of Lecture Notes in Computer Science, Springer, 2018, pp. 374–386, https://doi.org/10.1007/978-3-319-94667-2_31.

[SM4] J.-F. Culus and S. Toulouse, *2 csps all are approximable within a constant differential factor*, in Combinatorial Optimization, J. Lee, G. Rinaldi, and A. R. Mahjoub, eds., vol. 10856 of Lecture Notes in Computer Science, Cham, 2018, Springer International Publishing, pp. 389–401, https://doi.org/10.1007/978-3-319-96151-4_33.

[SM5] J.-F. Culus, S. Toulouse, and F. Roupin, *Differential approximation of SNP optimization problems*, in International Symposium on Combinatorial Optimization (ISCO) 2012 (short paper), 2012.

[SM6] L. Engebretsen and V. Guruswami, *Is constraint satisfaction over two variables always easy?*, Random Structures & Algorithms, 25 (2004), pp. 150–178, https://doi.org/https://doi.org/10.1002/rsa.20026.

[SM7] A. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal Arrays: Theory and Applications*, Springer, 1999, https://doi.org/https://doi.org/10.1007/978-1-4612-1478-6.

[SM8] J. Håstad, *Some optimal inapproximability results*, J. ACM, 48 (2001), p. 798–859, https://doi.org/10.1145/502090.502098.

[SM9] S. Khot and A. Naor, *Linear equations modulo 2 and the \$l_1\$ diameter of convex bodies*, SIAM Journal on Computing, 38 (2008), pp. 1448–1463, https://doi.org/10.1137/070691140.

[SM10] J. Monnot, V. T. Paschos, and S. Toulouse, *Approximation polynomiale des problèmes NP-difficiles - Optima locaux et rapport différentiel*, Hermes Science, Paris, 2003.