# REDUCED KRONECKER COEFFICIENTS AND <br> COUNTER-EXAMPLES TO MULMULEY'S STRONG SATURATION CONJECTURE SH <br> WITH AN APPENDIX BY KETAN MULMULEY 

Emmanuel Briand, Rosa Orellana, and Mercedes Rosas


#### Abstract

We provide counter-examples to Mulmuley's strong saturation conjecture (strong SH) for the Kronecker coefficients. This conjecture was proposed in the setting of Geometric Complexity Theory to show that deciding whether or not a Kronecker coefficient is zero can be done in polynomial time. We also provide a short proof of the \#Phardness of computing the Kronecker coefficients. Both results rely on the connections between the Kronecker coefficients and another family of structural constants in the representation theory of the symmetric groups, Murnaghan's reduced Kronecker coefficients. An appendix by Mulmuley introduces a relaxed form of the saturation hypothesis $\mathbf{S H}$, still strong enough for the aims of Geometric Complexity Theory.


Keywords. Geometric complexity theory, Kronecker coefficients, saturation properties, quasipolynomials.

Subject classification. 05E05; 03D15; 20 G 05.

## 1. Introduction

A major unsolved problem in group representation theory is raised by the tensor product of irreducible representations of a symmetric group $\mathfrak{S}_{n}$ : Provide a (positive) combinatorial interpretation for the multiplicities of its decomposition into irreducible representations (the Kronecker coefficients $g_{\mu, \nu}^{\lambda}$ ). Recently,
the Kronecker coefficients started being examined also under the angle of computational complexity. The problems considered are:

Kron: (Computation problem) Given labels $\lambda, \mu, \nu$, compute the Kronecker coefficient $g_{\mu, \nu}^{\lambda}$.

ZeroKron: (Decision problem) Given labels $\lambda, \mu$ and $\nu$, decide whether $g_{\mu, \nu}^{\lambda}$ is positive or zero.

The labels $\lambda, \mu, \nu$ of the Kronecker coefficients are integer partitions (finite, nonincreasing sequences of positive integers) and the complexity of these problems is measured with respect to their bitlength.

A family of related coefficients, much better understood, are the LittlewoodRichardson coefficients $c_{\mu, \nu}^{\lambda}$ (the analogues of the Kronecker coefficients for representations of the complex linear groups $G L_{n}(\mathbb{C})$ ). Narayanan (2006) showed that computing the Littlewood-Richardson coefficients is a \#P-complete problem, which implies that there is no polynomial-time algorithm to perform this task, unless $P=N P$. On the other hand, deciding the positivity of the Littlewood-Richardson coefficients can be done in polynomial time (De Loera \& McAllister 2006; Knutson \& Tao 2001; Mulmulev \& Sohoni 2005), as a consequence of the saturation property established by Knutson \& Tao (1999):

$$
\begin{equation*}
c_{\mu, \nu}^{\lambda}>0 \quad \Leftrightarrow \quad c_{N \mu, N \nu}^{N \lambda}>0 \text { for all positive integers } N \text {, } \tag{1.1}
\end{equation*}
$$

where $N \lambda$ is just the partition $\left(N \lambda_{1}, N \lambda_{2}, \ldots, N \lambda_{k}\right)$ if $\lambda=\left(\lambda_{1}, \lambda_{2}, \ldots, \lambda_{k}\right)$, and likewise for $N \mu$ and $N \nu$.

The problem of determining whether or not Kron is also in \#P is open (Question 2.1 in Mulmuley 2007b). Bürgisser \& Ikenmeyer (2008) showed that Kron is \#P-hard, and GapP-complete.

That ZeroKron is in P is an open conjecture that lies at the heart of a detailed plan, Geometric Complexity Theory, that Ketan Mulmuley and Milind Sohoni elaborated to prove that $\mathrm{P} \neq \mathrm{NP}$ over the complex numbers: an arithmetic, non-uniform version of $\mathrm{P} \neq \mathrm{NP}$ (See the series of papers Mulmulev \& Sohoni 2001, 2008, 2005, 2007; Mulmuley \& Naravanan 2007; Mulmulev 2007a, 2008b. c, referred to as GCT1-8 below). Indeed, Mulmuley proposed in GCT6 a variant of the strategy used to show that the positivity of the Littlewood-Richardson coefficients can be decided in polynomial time, that would imply that ZeroKron is also in $P$.

Mulmuley conjectured in GCT6 (versions 1-3) that the following two hypotheses hold:
(i) A positivity hypothesis PH1, that says that the Kronecker coefficients $g_{N \mu, N \nu}^{N \lambda}$ for $N \in \mathbb{N}^{*}$ count the integral points in the dilations $N \mathcal{P}$ of a polytope $\mathcal{P}=\mathcal{P}(\lambda, \mu, \nu)$ whose non-emptiness can be decided in polynomial time. (Note that PH1 implies that Kron is in \#P).
(ii) A saturation hypothesis $\mathbf{S H}$, that reduces the test that $\mathcal{P}(\lambda, \mu, \nu)$ contains an integral point (integer programming) to a test of non-emptiness (linear programming). Since it is known that the verbatim translation of the saturation property of the Littlewood-Richardson coefficients (1.1) does not hold for the Kronecker coefficients, Mulmuley proposed a variant of it, see Section 2, and conjectured that it holds for the Kronecker coefficients (SH).

Together, hypotheses SH and PH1 imply that ZeroKron is in P (See Theorem 1.4.1 in GCT6).

The main result of this paper shows that the situation is more complicated than expected: $\mathbf{S H}$, as formulated in GCT6, versions $1-3$, does not hold for the Kronecker coefficients. Theorem 2.4 provides infinitely many counterexamples. They belong to the family of the Kronecker coefficients $g_{\mu, \nu}^{\lambda}$ where $\mu$ and $\nu$ have at most 2 parts and $\lambda$ has at most 3 parts. They are, actually, all the counter-examples in this family (see Section 4.2).

After a first version of this paper was published on the preprint server ArXiv, Mulmuley (2008a) proposed a new, weaker saturation conjecture $\mathbf{S H}$, still strong enough for the aims of Geometric Complexity Theory. This correction is appended to the present paper. In what follows, we will refer to the disproved saturation hypothesis, stated in GCT6, versions 1-3, as the strong saturation hypothesis, strong SH.

This work is organized as follows. Theorem 2.4 is formally proved inSection 3 after some preliminaries (Section 2). In Section 4 we explain how the counterexamples were obtained: we were able to check exhaustively strong SH for all Kronecker coefficients indexed by two two-row shapes (the Kronecker coefficients $g_{\mu, \nu}^{\lambda}$ where $\mu$ and $\nu$ have at most two terms) thanks to new explicit formulas for them. Previously known formulas, due to Remmel \& Whitehead (1994) and Rosas (2001) were not suitable for this study. The new formulas were obtained by considering another family of structural constants related to representations of the symmetric groups introduced long time ago by Murnaghan (1938) and called Reduced Kronecker coefficients by Klyachko (2004). They are defined precisely in Section 2.2. In Section 5 we point out the possible relevance of the reduced Kronecker coefficients in the complexity issues about Kronecker coefficients. As an illustration, a very short and simple proof of the \#P-hardness of Kron is presented. The paper ends with Mulmuley's appendix proposing a relaxed version of the hypothesis strong $\mathbf{S H}$.

## 2. Preliminaries and Main Result

2.1. Preliminaries on Kronecker coefficients.. A partition is a finite nonincreasing sequence of positive integers $\lambda=\left(\lambda_{1}, \lambda_{2}, \ldots, \lambda_{k}\right)$. We allow ourselves, when convenient, to represent also $\lambda$ by the sequences obtained by appending trailing zeros: $\lambda=\left(\lambda_{1}, \lambda_{2}, \ldots, \lambda_{k}, 0, \ldots, 0\right)$. The (non-zero) terms $\lambda_{i}$ of $\lambda$ are usually called its parts. The length (number of parts) $k$ is denoted with $\ell(\lambda)$. The sum of the parts of $\lambda$ is called weight of $\lambda$ and denoted with $|\lambda|$.

For $N$ and $d$ positive integers, the partition $(N, N, \ldots, N)$ having $d$ parts all equal to $N$ is denoted with $\left(N^{d}\right)$. Partitions can be added: $\lambda+\mu=\left(\lambda_{1}+\right.$ $\left.\mu_{1}, \lambda_{2}+\mu_{2}, \ldots\right)$ and stretched: for $N$ positive integer, $N \lambda=\left(N \lambda_{1}, N \lambda_{2}, \ldots\right)$.

The irreducible (finite-dimensional, complex) representations $V_{\lambda}\left(\mathfrak{S}_{n}\right)$ of the symmetric group $\mathfrak{S}_{n}$ are indexed by the partitions $\lambda$ of weight $n$. Given two irreducible representations $V_{\mu}\left(\mathfrak{S}_{n}\right)$ and $V_{\nu}\left(\mathfrak{S}_{n}\right)$, one can form their tensor product and decompose it into irreducible representations. Such a decomposition takes the form:

$$
V_{\mu}\left(\mathfrak{S}_{n}\right) \otimes V_{\nu}\left(\mathfrak{S}_{n}\right) \cong \bigoplus_{\lambda \text { s.t. }|\lambda|=n} g_{\mu, \nu}^{\lambda} V_{\lambda}\left(\mathfrak{S}_{n}\right)
$$

where $g_{\mu, \nu}^{\lambda} V_{\lambda}\left(\mathfrak{S}_{n}\right)$ means "the direct sum of $g_{\mu, \nu}^{\lambda}$ copies of $V_{\lambda}\left(\mathfrak{S}_{n}\right)$ ". Each multiplicity $g_{\mu, \nu}^{\lambda}$ is uniquely determined by $\lambda, \mu, \nu$. By considering all symmetric groups $\mathfrak{S}_{n}$ this defines an infinite family of integers $g_{\mu, \nu}^{\lambda}$ indexed by triples of partitions fulfilling $|\lambda|=|\mu|=|\nu|$. They are the Kronecker coefficients.

The Kronecker coefficients can also be interpreted in the setting of representations of the general linear group (this is, actually, the relevant interpretation in Geometric Complexity Theory). The irreducible (finite-dimensional, polynomial) representations $V_{\lambda}\left(G L_{k}(\mathbb{C})\right)$ of $G L_{k}(\mathbb{C})$ are indexed by the partitions $\lambda$ with length at most $k$. The irreducible representations of the Cartesian product $G L_{m}(\mathbb{C}) \times G L_{n}(\mathbb{C})$ are just the tensor products $V_{\mu}\left(G L_{m}(\mathbb{C})\right) \otimes V_{\nu}\left(G L_{n}(\mathbb{C})\right)$. The Kronecker coefficient $g_{\mu, \nu}^{\lambda}$ is the multiplicity of $V_{\mu}\left(G L_{m}(\mathbb{C})\right) \otimes V_{\nu}\left(G L_{n}(\mathbb{C})\right)$ in $V_{\lambda}\left(G L_{m n}(\mathbb{C})\right)$, seen as a representation of $G L_{m}(\mathbb{C}) \times G L_{n}(\mathbb{C})$ through the Kronecker product of matrices. This follows from Schur-Weyl duality (see Kraft \& Procesi 1996). A simple consequence is that $g_{\mu, \nu}^{\lambda}$ can be positive only if $\ell(\lambda) \leq \ell(\mu) \ell(\nu)$. Another consequence is provided by the following lemma.

Lemma 2.1. Let $\mu, \nu, \lambda$ be partitions with $\ell(\mu) \leq m, \ell(\nu) \leq n$ and $\ell(\lambda) \leq m n$. Below we write $\lambda$ as a sequence of exactly mn terms, by appending trailing zeros if necessary: $\lambda=\left(\lambda_{1}, \lambda_{2}, \ldots, \lambda_{m n-1}, \lambda_{m n}\right)$, and likewise for $\mu$ ( $m$ terms) and $\nu$ ( $n$ terms). Set $k=\lambda_{m n}, k_{1}=m k$ and $k_{2}=n k$. If $\mu_{m}<k_{2}$ or $\nu_{n}<k_{1}$ then
$g_{\mu, \nu}^{\lambda}=0$. Else,

$$
\begin{equation*}
g_{\mu, \nu}^{\lambda}=g_{\left(\mu_{1}-k_{2}, \mu_{2}-k_{2}, \ldots, \mu_{m}-k_{2}\right)\left(\nu_{1}-k_{1}, \nu_{2}-k_{1}, \ldots, \nu_{n}-k_{1}\right)}^{\left(\lambda_{1}-k, \lambda_{2}-k, \ldots, \lambda_{m n-1} .-.\right.} . \tag{2.2}
\end{equation*}
$$

Proof. Let $m, n$ be positive integers and let $\lambda$ be a partition with length at most $m n$. As representations of $G L\left(\mathbb{C}^{m}\right) \times G L\left(\mathbb{C}^{n}\right)$ :

$$
V_{\lambda}\left(G L\left(\mathbb{C}^{m} \otimes \mathbb{C}^{n}\right)\right) \cong \bigoplus_{\substack{\ell(\mu) \leq m \\ \ell(\nu) \leq n}} g_{\mu, \nu}^{\lambda} V_{\mu}\left(G L\left(\mathbb{C}^{m}\right)\right) \otimes V_{\nu}\left(G L\left(\mathbb{C}^{n}\right)\right)
$$

For any vector space $U$ of dimension $d$, let $\operatorname{det} U=V_{\left(1^{d}\right)}(G L(U))$ be its determinant representation (remember that $\left(1^{d}\right)$ stands for the partition $(1,1, \ldots, 1)$ with $d$ parts, all equal to 1$)$. That is, the one dimensional representation of $G L(U)$ such that $g(u)=\operatorname{det}(g) u$ for all $g \in G L(U)$. We have $V_{\lambda+\left(1^{d}\right)}(G L(U)) \cong$ $\operatorname{det}(U) \otimes V_{\lambda}(G L(U))$. This fact, together with the isomorphism:

$$
\operatorname{det}\left(\mathbb{C}^{m} \otimes \mathbb{C}^{n}\right) \cong \operatorname{det}\left(\mathbb{C}^{m}\right)^{\otimes n} \otimes \operatorname{det}\left(\mathbb{C}^{n}\right)^{\otimes m}
$$

implies the following decomposition:

$$
V_{\lambda+\left(1^{m n}\right)}\left(G L\left(\mathbb{C}^{m} \otimes \mathbb{C}^{n}\right)\right) \cong \bigoplus_{\substack{\ell(\mu) \leq m \\ \ell(\nu) \leq n}} g_{\mu, \nu}^{\lambda} V_{\mu+\left(n^{m}\right)}\left(G L\left(\mathbb{C}^{m}\right)\right) \otimes V_{\nu+\left(m^{n}\right)}\left(G L\left(\mathbb{C}^{n}\right)\right)
$$

From this we obtain the invariance relation:

$$
g_{\mu+\left(n^{m}\right), \nu+\left(m^{n}\right)}^{\lambda+\left(1^{m n}\right)}=g_{\mu, \nu}^{\lambda} .
$$

Moreover, we easily see that $g_{\mu \nu}^{\lambda}$ can be positive only when $\mu_{m} \geq n \lambda_{m n}=k_{2}$ and $\nu_{n} \geq m \lambda_{m n}=k_{1}$.

The simplest non-trivial, meaningful family of Kronecker coefficients $g_{\mu, \nu}^{\lambda}$ closed under stretching (that is, under the map that sends the triple $\lambda, \mu, \nu$ into $N \lambda, N \mu, N \nu)$ is the family of coefficients $g_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{1}, \lambda_{4}\right)}$. But in view of (2.2) its study can be reduced to the study of the coefficients $g_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{3}\right)}$.
2.2. Reduced Kronecker Coefficients. Let us introduce another family of constants, closely related to the Kronecker coefficients, which will play an important role in this paper.

For any partition $\lambda=\left(\lambda_{1}, \lambda_{2}, \ldots, \lambda_{k}\right)$ and integer $n$, denote with $(n-|\lambda|, \lambda)$ the sequence obtained by prepending $n-|\lambda|$ to $\lambda$, i.e. $(n-|\lambda|, \lambda)=(n-$
$\left.|\lambda|, \lambda_{1}, \lambda_{2}, \ldots, \lambda_{k}\right)$. This is a partition when $n \geq|\lambda|+\lambda_{1}$. Murnaghan (1938) established that for any three partitions $\alpha, \beta, \gamma$, the sequence with general term $g_{(n-|\alpha|, \alpha)(n-|\beta|, \beta)}^{(n-|\alpha|, \gamma)}$ is stationary. Let $\bar{g}_{\alpha, \beta}^{\gamma}$ be its limit. Following Klyachko (2004) we call these constants $\bar{g}_{\alpha, \beta}^{\gamma}$ the reduced Kronecker coefficients.

Upper bounds for the index when the sequences with general term

$$
g_{(n-|\alpha|, \alpha)(n-|\beta|, \beta)}^{(n-|\gamma|, \gamma)}
$$

become stationary are discussed by Briand et al. (In preparation-a); Brion (1993); Vallejo (1999).

### 2.3. Saturation Hypotheses and counter-examples to the hypothesis

 strong SH. The verbatim translation of the saturation property (1.1) that holds for the Littlewood-Richardson coefficients is known not to hold for the Kronecker coefficients. The simplest counter-example may be $g_{(1,1)(1,1)}^{(1,1)}=0$ but $g_{(2,2)(2,2)}^{(2,2)}=1$. Indeed,$$
g_{(N, N),(N, N)}^{(N, N)}=\left\{\begin{array}{lc}
0 & \text { for odd } N \\
1 & \text { for even } N
\end{array}\right.
$$

Many more such counter-examples exist.
To present an alternative saturation property we consider the stretching function $\widetilde{g}_{\mu, \nu}^{\lambda}$ (where $\mu, \nu, \lambda$ are partitions of the same weight) defined by:

$$
\widetilde{g}_{\mu, \nu}^{\lambda}: \quad N \in \mathbb{N}^{*} \longmapsto g_{N \mu, N \nu}^{N \lambda} .
$$

Mulmuley proved (GCT6, Theorem 1.6.1.b) that $\widetilde{g}_{\mu, \nu}^{\lambda}$ is always a quasipolynomial, i.e. a function of the form:

$$
F: \quad N \in \mathbb{N}^{*} \longmapsto\left\{\begin{array}{ccc}
F_{1}(N) & \text { if } N \equiv 1 & \bmod k,  \tag{2.3}\\
F_{2}(N) & \text { if } N \equiv 2 & \bmod k, \\
\vdots & \vdots & \\
F_{k}(N) & \text { if } N \equiv k & \bmod k
\end{array}\right.
$$

where $k$ is a positive integer and $F_{1}, F_{2}, \ldots, F_{k}$ are polynomials (see Stanley 1997, Section 4.4 as a reference on quasipolynomials). A quasipolynomial is said to be saturated (GCT6, def. 1.2.4) when it has the property:

$$
F(1)=0 \Rightarrow F_{1} \text { vanishes identically. }
$$

We are now ready to state Mulmuley's strong saturation hypothesis strong SH for the Kronecker coefficients (GCT6, versions 1-3):

Strong SH: The stretching quasipolynomials $\widetilde{g}_{\mu, \nu}^{\lambda}$ of the Kronecker coefficients are saturated.

Observe that Strong SH implies that for any three partitions $\lambda, \mu, \nu$ of the same weight,

$$
g_{\mu, \nu}^{\lambda}=0 \Rightarrow g_{N \mu, N \nu}^{N \lambda}=0 \text { for infinitely many positive integers } N .
$$

Hence, the following theorem provides an infinite family of counter-examples to Strong SH. (Its proof is provided in the next section.)

Theorem 2.4. Let $i, j, k$ be integers such that $i>j>0$ and $k>2 i+j$. Let

$$
\alpha=(k, k), \quad \beta=(k+1, k-1), \quad \gamma=(2 k-2 i-2 j, 2 i, 2 j)
$$

Then:

$$
g_{N \alpha, N \beta}^{N \gamma}=N / 2+\left\{\begin{array}{cc}
1 & \text { for even } N  \tag{2.5}\\
-1 / 2 & \text { for odd } N
\end{array}\right.
$$

In particular, $g_{\alpha, \beta}^{\gamma}=0$ and $g_{N \alpha, N \beta}^{N \gamma}>0$ for all $N>1$.
The smallest counter-example in this family is $\widetilde{g}_{(6,6)(7,5)}^{(6,4,2)}$.
Remark 2.6. All counter-examples $\widetilde{g}_{\mu, \nu}^{\lambda}$ to Strong SH with $\ell(\mu) \leq 2, \ell(\nu) \leq$ 2 , and $\ell(\lambda) \leq 3$ are given by Theorem 2.4, up to permutation of $\mu$ and $\nu$. This follows from the calculations in Briand et al. (2008, In preparation-b) reported in Section 4.2. All triples $(\mu, \nu, \lambda)$ corresponding to these counter-examples are contained in a codimension 2 affine subspace of the space of parameters, namely the subspace defined by $\mu_{2}=\nu_{2}+1, \mu_{1}=\mu_{2}$. In addition, they shall fulfill congruences: $\lambda_{2} \equiv \lambda_{3} \equiv 0 \bmod 2$. Under these conditions, it is not surprising that these counter-examples escaped the sampling taken in GCT6, Section 6.2, as an experimental verification of Strong SH.

Remark 2.7. Strikingly, the family of Kronecker coefficients $g_{\mu, \nu}^{\lambda}$ with $\mu=$ $(k, k)$, which comprises the counter-examples of Theorem 2.4, has been independently studied in the recent preprint by Brown et al. (2008) motivated by questions in mathematical physics.
2.4. The Positivity Hypothesis PH2, and counter-examples. A quasipolynomial $F$ is said to be positive when the coefficients of all polynomials $F_{i}$ in (2.3) are nonnegative (GCT6, def. 1.2.2). Mulmuley (2007a) conjectured:

Strong PH2: The stretching quasipolynomials $\widetilde{g}_{\mu, \nu}^{\lambda}$ of the Kronecker coefficients are positive.

This conjecture was first proposed for the Littlewood-Richardson coefficients by King et al. (2004) and later for the generalized Littlewood-Richardson coefficients associated to the classical Lie groups of type $B, C$ and $D$ by De Loera \& McAllister (2006). The conjecture is still open for both cases.

Note that Strong PH2 implies straightforwardly Strong SH. The counterexamples to Strong SH provided by Theorem 2.4 are thus also counterexamples to Strong PH2 for Kronecker coefficients. The following is a counterexample to Strong PH2 that nevertheless fulfills Strong SH:

$$
g_{(10 N, 8 N)(11 N, 7 N)}^{(10 N, 6 N, 2 N)}=7 / 4 N^{2}+3 / 2 N+\left\{\begin{array}{cc}
1 & \text { for even } N, \\
-1 / 4 & \text { for odd } N .
\end{array}\right.
$$

There exist many more counter-examples to Strong PH2 than to Strong SH. Indeed, there are several full-dimensional rational convex polyhedral cones $\sigma_{i}$ of $\mathbb{R}^{5}$ such that for all $\left(\lambda_{1}, \lambda_{2}, \lambda_{3}, \mu_{2}, \mu_{3}\right) \in \sigma_{i} \cap \mathbb{Z}^{5}$ fulfilling $\lambda_{1} \equiv \lambda_{2} \equiv \lambda_{3} \equiv$ $\mu_{2}+\nu_{2}+1 \equiv 0 \bmod 2$, the quasipolynomial $\widetilde{g}_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{2}\right)}$ is not positive. (See Section 4.2.)

Remark 2.8. Although the Littlewood-Richardson coefficients are particular cases of Kronecker coefficients (see Section 5), no counter-example to Strong PH2 for the Littlewood-Richardson coefficients was obtained this way.
2.5. Relaxed saturation hypothesis SH and relaxed positivity hypothesis PH2. After a first version of this paper was released on the preprint server ArXiv, Mulmuley (2008a) gave new, weaker versions of the saturation hypothesis SH and of the positivity hypothesis PH2. These hypotheses are still strong enough for the aims of Geometric Complexity Theory. Mulmuley's note (Mulmuley 2008a) is appended to this paper.

The relaxed hypotheses PH2 and SH hold for the Kronecker coefficients indexed by two two-rows shapes. In particular, SH a) follows from Remark 2.6 in this case. For this family of Kronecker coefficients, the positivity index (see the appendix) is at most 1 (see Remark 4.10).

## 3. Proof of Theorem 2.4

The proof of Theorem 2.4 will rely on the following lemma, which is a slight simplification of Theorem 1 in Rosas 2001.

Lemma 3.1. Let $n$ be a natural integer. Let $\lambda, \mu, \nu$ be three partitions of $n$. Suppose that $\mu$ and $\nu$ have at most two parts and $\lambda$ has at most three parts. Suppose additionally that $\mu_{2} \geq \nu_{2}$. Then:

$$
\begin{equation*}
g_{\mu, \nu}^{\lambda}=\operatorname{Card}\left(\mathcal{R}_{+} \cap \mathcal{Z} \cap \mathcal{L}\right)-\operatorname{Card}\left(\mathcal{R}_{-} \cap \mathcal{Z} \cap \mathcal{L}\right) \tag{3.2}
\end{equation*}
$$

where:

$$
\begin{aligned}
\mathcal{Z} & =\left\{(x, y) \in \mathbb{R}^{2} \mid x+y \leq \mu_{2}+\nu_{2}+1 \text { and } y-x \geq \mu_{2}-\nu_{2}+1\right\} \\
\mathcal{L} & =\left\{(x, y) \in \mathbb{Z}^{2} \mid x+y \equiv \mu_{2}+\nu_{2}+1 \quad \bmod 2\right\}
\end{aligned}
$$

and $\mathcal{R}_{+}$and $\mathcal{R}_{-}$are the following two rectangles of $\mathbb{R}^{2}$ :

$$
\begin{aligned}
& \mathcal{R}_{+}=\left[\lambda_{3} ; \lambda_{2}\right] \times\left[1+\lambda_{2} ; 1+\lambda_{2}+\lambda_{3}\right], \\
& \mathcal{R}_{-}=\left[\lambda_{3} ; \lambda_{2}\right] \times\left[2+\lambda_{1} ; 2+\lambda_{1}+\lambda_{3}\right] .
\end{aligned}
$$

Proof. When $\lambda_{1} \geq \lambda_{2}+\lambda_{3}$, this is a direct application of Theorem 1 of Rosas (2001). When $\lambda_{1}<\lambda_{2}+\lambda_{3}$, the same theorem states that:

$$
g_{\mu, \nu}^{\lambda}=\operatorname{Card}\left(\mathcal{R}_{+}^{\prime} \cap \mathcal{Z} \cap \mathcal{L}\right)-\operatorname{Card}\left(\mathcal{R}_{-}^{\prime} \cap \mathcal{Z} \cap \mathcal{L}\right)
$$

with
$\mathcal{R}_{+}^{\prime}=\left[\lambda_{3} ; \lambda_{2}\right] \times\left[1+\lambda_{2} ; 1+\lambda_{1}\right] \quad$ and $\quad \mathcal{R}_{-}^{\prime}=\left[\lambda_{3} ; \lambda_{2}\right] \times\left[2+\lambda_{2}+\lambda_{3} ; 2+\lambda_{1}+\lambda_{3}\right]$.
In Formula (3.2) the points of $\mathcal{Z}$ that lie in $\mathcal{R}_{+} \cap \mathcal{R}_{-}$have no contribution, thus (3.2) is equivalent to:

$$
\begin{equation*}
g_{\mu, \nu}^{\lambda}=\operatorname{Card}\left(\left(\mathcal{R}_{+} \backslash \mathcal{R}_{-}\right) \cap \mathcal{Z} \cap \mathcal{L}\right)-\operatorname{Card}\left(\left(\mathcal{R}_{-} \backslash \mathcal{R}_{+}\right) \cap \mathcal{Z} \cap \mathcal{L}\right) \tag{3.3}
\end{equation*}
$$

We observe that $\mathcal{R}_{+} \backslash \mathcal{R}_{-}$has the same integral points as $\mathcal{R}_{+}^{\prime}$. Similarly $\mathcal{R}_{-} \backslash \mathcal{R}_{+}$ has the same integral points as $\mathcal{R}_{-}^{\prime}$. Thus Formula (3.3) is true, and so is Formula (3.2) even when $\lambda_{1}<\lambda_{2}+\lambda_{3}$.

Proof of Theorem 2.4. Let $n, \lambda, \mu$ and $\nu$ be as in the hypotheses of Lemma 3.1. The transformation $(x ; y) \mapsto\left(x ; 2 \mu_{2}+2-y\right)$ preserves the sets $\mathcal{Z}$
and $\mathcal{L}$. It also transforms $\mathcal{R}_{-}$into $\mathcal{R}_{-}^{\prime \prime}=\left[\lambda_{3} ; \lambda_{2}\right] \times\left[2 \mu_{2}-\lambda_{1}-\lambda_{3} ; 2 \mu_{2}-\lambda_{1}\right]$. As a consequence,

$$
g_{\mu, \nu}^{\lambda}=\operatorname{Card}\left(\mathcal{R}_{+} \cap \mathcal{Z} \cap \mathcal{L}\right)-\operatorname{Card}\left(\mathcal{R}_{-}^{\prime \prime} \cap \mathcal{Z} \cap \mathcal{L}\right)
$$

Since the points in the intersection $\mathcal{R}_{+} \cap \mathcal{R}_{-}^{\prime \prime}$ don't contribute to the above difference,

$$
g_{\mu, \nu}^{\lambda}=\operatorname{Card}\left(\left(\mathcal{R}_{+} \backslash \mathcal{R}_{-}^{\prime \prime}\right) \cap \mathcal{Z} \cap \mathcal{L}\right)-\operatorname{Card}\left(\left(\mathcal{R}_{-}^{\prime \prime} \backslash \mathcal{R}_{+}\right) \cap \mathcal{Z} \cap \mathcal{L}\right)
$$

We apply this to the case when $\mu=N \alpha, \nu=N \beta$ and $\lambda=N \gamma$, where $N$ is a positive integer and $\alpha, \beta$ and $\gamma$ are as in the theorem. Then

$$
\begin{aligned}
\mathcal{R}_{+} & =[2 N j ; 2 N i] \times[1+2 N i ; 1+2 N(i+j)] \\
\text { and } \mathcal{R}_{-}^{\prime \prime} & =[2 N j ; 2 N i] \times[2 N i ; 2 N(i+j)] .
\end{aligned}
$$

These two rectangles overlap nearly completely. The integral points of $\mathcal{R}_{+} \backslash \mathcal{R}_{-}^{\prime \prime}$ are those of the North Side of $\mathcal{R}_{+}$, which is $\mathcal{S}_{+}=[2 N j ; 2 N i] \times\{1+2 N(i+j)\}$. The integral points of $\mathcal{R}_{-}^{\prime \prime} \backslash \mathcal{R}_{+}$are those on the South Side of $\mathcal{R}_{-}^{\prime \prime}$, which is $\mathcal{S}_{-}=[2 N j ; 2 N i] \times\{2 N i\}$. It follows that:

$$
g_{N \alpha, N \beta}^{N \gamma}=\operatorname{Card}\left(\mathcal{S}_{+} \cap \mathcal{Z} \cap \mathcal{L}\right)-\operatorname{Card}\left(\mathcal{S}_{-} \cap \mathcal{Z} \cap \mathcal{L}\right)
$$

The hypotheses $i>j>0$ and $k>2 i+j$ imply that:

$$
\mathcal{S}_{+} \cap \mathcal{Z}=\mathcal{S}_{+}, \quad \mathcal{S}_{-} \cap \mathcal{Z}=\mathcal{S}_{-}^{\prime}=[2 N j ; 2 N i-N-1] \times\{2 N i\}
$$

We have now:

$$
g_{N \alpha, N \beta}^{N \gamma}=\operatorname{Card}\left(\mathcal{S}_{+} \cap \mathcal{L}\right)-\operatorname{Card}\left(\mathcal{S}_{-}^{\prime} \cap \mathcal{L}\right)
$$

Observe that for any horizontal segment $\mathcal{S}$ of positive length with integral end points (since $i>j>0$, the segments $\mathcal{S}_{+}$and $\mathcal{S}_{-}^{\prime}$ fall in this category),

$$
\operatorname{Card}(\mathcal{S} \cap \mathcal{L})= \begin{cases}\text { length }(\mathcal{S}) / 2+1 & \text { if both end points are in } \mathcal{L}, \\ \operatorname{length}(\mathcal{S}) / 2+1 / 2 & \text { if exactly one end point is in } \mathcal{L}, \\ \operatorname{length}(\mathcal{S}) / 2 & \text { if none of the end points is in } \mathcal{L} .\end{cases}
$$

Since $\mathcal{L}=\left\{(x, y) \in \mathbb{Z}^{2} \mid x+y \equiv N+1 \bmod 2\right\}$, we get

$$
\begin{aligned}
\operatorname{Card}\left(\mathcal{S}_{+} \cap \mathcal{L}\right) & = \begin{cases}N(i-j)+1 & \text { for even } N \\
N(i-j) & \text { for odd } N\end{cases} \\
\operatorname{Card}\left(\mathcal{S}_{-}^{\prime} \cap \mathcal{L}\right) & = \begin{cases}N(i-j)-(N+1) / 2+1 / 2 & \text { for even } N \\
N(i-j)-(N+1) / 2+1 & \text { for odd } N\end{cases}
\end{aligned}
$$

Formula (2.5) of Theorem 2.4 follows.

## 4. Kronecker coefficients from reduced Kronecker coefficients

The counter-examples of Theorem 2.4 were found by examining exhaustively the simplest non-trivial family of Kronecker coefficients: the Kronecker coefficients indexed by two two-row shapes, i.e. the coefficients $g_{\mu, \nu}^{\lambda}$ where $\mu$ and $\nu$ have at most two parts. By Equation (2.2), it is enough to consider those with $\ell(\lambda) \leq 3$, i.e. the coefficients $g_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{3}\right)}$. We give here an account of this investigation, which is presented with more detail by Briand et al. (2008, In preparation-b).
4.1. Quasipolynomial formulas for $g_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{3}\right)}$. We obtained a description (call it $\mathbf{D}$ ) of $g_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{3}\right)}$ as a piecewise quasipolynomial function of $\lambda_{1}$, $\lambda_{2}, \lambda_{3}, \mu_{2}, \nu_{2}$ (note that $\mu_{1}$ and $\nu_{1}$ are determined from these parameters by the condition $|\lambda|=|\mu|=|\nu|)$.

A (multivariate) quasipolynomial function is a function of the form:

$$
F: \mathbf{x} \in \mathbb{Z}^{m} \longmapsto\left\{\begin{array}{cc}
F_{1}(\mathbf{x}) & \text { if } \mathbf{x} \in C_{1} \\
F_{2}(\mathbf{x}) & \text { if } \mathbf{x} \in C_{2} \\
\vdots & \vdots \\
F_{k}(\mathbf{x}) & \text { if } \mathbf{x} \in C_{k}
\end{array}\right.
$$

where $C_{1}, C_{2}, \ldots, C_{k}$ are the cosets of a full-rank sublattice of $\mathbb{Z}^{m}$, and $F_{1}$, $F_{2}, \ldots, F_{k}$ are polynomials.

Well-known examples of piecewise quasipolynomial functions are the vector partition functions. Other examples are provided by the functions of $\mathbf{y} \in \mathbb{R}^{p}$ that count the integral points $\mathbf{x}$ in polytopes $\mathcal{P}(\mathbf{y}) \subset \mathbb{R}^{q}$ defined by a system of linear inequalities of the form

$$
\begin{equation*}
f_{i}(\mathbf{x}) \leq g_{i}(\mathbf{y}) \tag{4.1}
\end{equation*}
$$

where $f_{i}$ and $g_{i}$ are integral linear forms. See Brion \& Vergne 1997 for both families of examples. For these examples, the domains of quasipolynomiality are the maximal cells of a fan (a complex of convex rational polyhedral cones) subdividing a cone of $\mathbb{R}^{n}$ (outside the cone the function vanishes).

The explicit formulas obtained by Remmel \& Whitehead (1994) for the coefficients $g_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{3}, \lambda_{4}\right)}$ are quasipolynomials whose domains are the maximal cells of a polyhedral complex. But the number of domains is huge (see GCT6, Section 6.2), which makes these formulas unsuitable for checking conjectures

Strong PH2 and Strong SH. Note that in this description, the domains of quasipolynomiality are not cones.

In the description $\mathbf{D}$ that we obtained, the domains of quasipolynomiality are the 74 maximal cells of a fan subdividing a cone $\mathcal{C}$. Note this suggests a stronger form of PH1: That $g_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{2}\right.}$ counts the integral points of polytopes $\mathcal{P}(\lambda, \mu, \nu)$ defined by a system of inequalities of the form (4.1).

Remark 4.2. This is the case for the Littlewood-Richardson coefficients: $c_{\mu, \nu}^{\lambda}$ counts the integral points of the Hive polytopes $\mathcal{H}(\lambda, \mu, \nu)$, defined by systems of inequalities of the form (4.1). See Buch 2000. See also Rassart 2004 for the corresponding piecewise quasipolynomial presentation. (It turns out to be piecewise polynomial.)

We don't know any family of polytopes whose integral points are counted by $g_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{3}\right)}$. But:
(i) The reduced Kronecker coefficients (see Section 2.2) indexed by two onerow shapes, have such an interpretation.
(ii) We are able to recover the Kronecker coefficients from the reduced Kronecker coefficients.

This is how we obtained $\mathbf{D}$.
We explain (i). Assume $\mu_{2} \geq \nu_{2}$. By fixing $\lambda_{2}, \lambda_{3}, \mu_{2}, \mu_{3}$ and making $|\lambda|=|\mu|=|\nu| \rightarrow \infty$ in Lemma 3.1, the rectangle $\mathcal{R}_{-}$goes outside $\mathcal{Z}$ while $\mathcal{R}_{+}$does not move. It follows that the reduced Kronecker coefficient $\bar{g}_{\left(\mu_{2}\right)\left(\nu_{2}\right)}^{\left(\lambda_{2}, \lambda_{3}\right)}=$ $\operatorname{Card}\left(\mathcal{R}^{+} \cap \mathcal{Z} \cap \mathcal{L}\right)$. The map

$$
(x, y) \longmapsto\left(\frac{y-x+r+s-1}{2}, \frac{-y-x+r+s+1}{2}\right)
$$

transforms the set $\mathcal{L}$ into $\mathbb{Z}^{2}$, and $\mathcal{R}_{+} \cap \mathcal{Z}$ into the set of solutions $(x, y)$ of the system:

$$
\left\{\begin{array}{l}
x \geq \mu_{2}  \tag{4.3}\\
y \geq 0 \\
\mu_{2}+\nu_{2}-\lambda_{2} \leq x+y \leq \mu_{2}+\nu_{2}-\lambda_{3} \\
\lambda_{2} \leq x-y \leq \lambda_{2}+\lambda_{3}
\end{array}\right.
$$

This yields the following result. Note that an equivalent result is given by Thibon (1991).

Proposition 4.4. Let $\mu_{2}, \nu_{2}, \lambda_{2}, \lambda_{3}$ be nonnegative integers with $\lambda_{2} \geq \lambda_{3}$. The Reduced Kronecker Coefficient $\bar{g}_{\left(\mu_{2}\right)\left(\nu_{2}\right)}^{\left(\lambda_{2}, \lambda_{3}\right)}$ counts the integral solutions $(x, y)$ of (4.3).

It follows a piecewise quasipolynomial description $\mathbf{D}_{0}$ for $\bar{g}_{\left(\mu_{2}\right)\left(\nu_{2}\right)}^{\left(\lambda_{2}, \lambda_{3}\right)}$. Its domain of quasipolynomiality are the 26 maximal cells of a fan subdividing a cone of $\mathbb{R}^{4}$.

We now explain (ii). There exists a simple formula to recover Kronecker coefficients from reduced Kronecker coefficients.

Theorem 4.5 (Briand et al. In preparation-b). Let $\ell_{1}$ and $\ell_{2}$ be positive integers. Let $\lambda, \mu, \nu$ be partitions of the same weight such that $\ell(\mu) \leq \ell_{1}, \ell(\nu) \leq \ell_{2}$ and $\ell(\lambda) \leq \ell_{1} \ell_{2}$. Then

$$
g_{\mu \nu}^{\lambda}=\sum_{i=1}^{\ell_{1} \ell_{2}-1}(-1)^{i+1} \bar{g}_{\bar{\mu}, \bar{\nu}}^{\lambda^{\dagger i}}
$$

where $\lambda^{\dagger i}$ is the partition obtained from $\lambda$ by incrementing the $i-1$ first terms and removing the $i-$ th term, that is:

$$
\lambda^{\dagger i}=\left(1+\lambda_{1}, 1+\lambda_{2}, \ldots, 1+\lambda_{i-1}, \lambda_{i+1}, \lambda_{i+2}, \ldots\right)
$$

and $\bar{\lambda}=\lambda^{\dagger 1}$.
In particular,

$$
\begin{equation*}
g_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{3}\right)}=\bar{g}_{\left(\mu_{2}\right)\left(\nu_{2}\right)}^{\left(\lambda_{2}, \lambda_{3}\right)}-\bar{g}_{\left(\mu_{2}\right)\left(\nu_{2}\right)}^{\left(\lambda_{1}+1, \lambda_{3}\right)}+\bar{g}_{\left(\mu_{2}\right)\left(\nu_{2}\right)}^{\left(\lambda_{1}+1, \lambda_{2}+1\right)} . \tag{4.6}
\end{equation*}
$$

Formula (4.6) allows us to deduce from the description $\mathbf{D}_{0}$ a piecewise quasipolynomial description for $g_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{1}\right.}$. Its domains of quasipolynomiality are the maximal cells of a polyhedral complex. But these cells are not cones. This is fixed to obtain the description $\mathbf{D}$ where the domain of quasipolynomiality are cones. The key observation for this is: The quasipolynomials attached to contiguous maximal cells in $\mathbf{D}_{0}$ coincide not only on their common border, but also on close parallel hyperplanes.

Remark 4.7. It is also possible, in principle, to derive a piecewise quasipolynomial presentation for $g_{\mu, \nu}^{\lambda}, \ell(\mu) \leq m, \ell(\nu) \leq n, \ell(\lambda) \leq m n$, from Klimyk's formula, for any $m, n$. This is explained in GCT6, section 4.5. Nevertheless, the domains of quasipolynomiality obtained this way are not cones.
4.2. Checking Strong PH2 and Strong SH for $g_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{3}\right)}$. We explain how we check when the stretching function $\widetilde{g}_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{3}\right)}$ is positive and/or saturated from the description $\mathbf{D}$. For each of the 74 maximal cells $\sigma$ in $\mathbf{D}$, the quasipolynomial formula on $\sigma$ has the form

$$
\begin{equation*}
g_{\left(\mu_{1}, \mu_{2}\right)\left(\nu_{1}, \nu_{2}\right)}^{\left(\lambda_{1}, \lambda_{2}, \lambda_{3}\right.}=1 / 4 Q_{\sigma}(\mathbf{x})+1 / 2 L_{\sigma}(\mathbf{x})+\Delta_{\sigma}(\mathbf{x}) \tag{4.8}
\end{equation*}
$$

where $Q_{\sigma}$ and $L_{\sigma}$ are integral homogeneous polynomials in the variable $\mathbf{x}=$ $\left(\lambda_{1}, \lambda_{2}, \lambda_{3}, \mu_{2}, \nu_{2}\right)$, respectively quadratic and linear. The function $\Delta_{\sigma}$ fulfills $\Delta_{\sigma}(0)=1$ and is constant on each coset of $\mathbb{Z}^{5}$ modulo the sublattice defined by $\mu_{2}+\nu_{2} \equiv \lambda_{1} \equiv \lambda_{2} \equiv \lambda_{3} \equiv 0 \bmod 2$.

Checking positivity is specially easy because in (4.8) the functions $Q_{\sigma}, L_{\sigma}$, $\Delta_{\sigma}$ are nonnegative on $\sigma$ for nearly all cells $\sigma$. Indeed:

- For all $\sigma$ and all integral points $\mathbf{x} \in \sigma$, one has $Q_{\sigma}(\mathbf{x})=\lim _{N \rightarrow \infty} g_{N \mu, N \nu}^{N \lambda} / N^{2}$, which is necessarily nonnegative.
- We check by direct inspection that for all cells $\sigma$ and all $\mathbf{x} \in \sigma$, one has $L_{\sigma}(\mathbf{x}) \geq 0$.
- By direct inspection, for all cells $\sigma$ except four, $\Delta_{\sigma}(\mathbf{x}) \geq 0$ for all $\mathbf{x} \in \sigma$. Let $A$ be the subset of $\mathbb{Z}^{5}$ defined by $\lambda_{1} \equiv \lambda_{2} \equiv \lambda_{3} \equiv \mu_{2}+\nu_{2}+1 \equiv 0$ $\bmod 2$. For three of the four exceptional cells, call them $\sigma_{1}, \sigma_{2}$ and $\sigma_{3}$, one has, for all integral points $\mathbf{x} \in \sigma_{i}$, that $\Delta_{\sigma_{i}}(\mathbf{x})=-1 / 4$ if $\mathbf{x} \in A$ and $\Delta_{\sigma_{i}}(\mathbf{x}) \geq 0$ else. For the fourth exceptional cell, call it $\sigma_{4}$, one has, for all integral points $\mathbf{x} \in \sigma_{4}$, that $\Delta_{\sigma_{4}}(\mathbf{x})=-1 / 2$ if $\mathbf{x} \in A$ and $\Delta_{\sigma_{4}}(\mathbf{x}) \geq 0$ else.

Therefore, the counter-examples to Strong PH2 correspond to $\mathbf{x} \in A \cap\left(\sigma_{1} \cup\right.$ $\left.\sigma_{2} \cup \sigma_{3} \cup \sigma_{4}\right)$.

Since Strong PH2 implies Strong SH, we look for the counter-examples to Strong SH among the counter-examples to Strong PH2.

For $\mathbf{x} \in A \cap \sigma_{i}, i \in\{1,2,3\}$, the coefficient $g_{\mu, \nu}^{\lambda}$ is zero if and only if $Q_{\sigma_{i}}(\mathbf{x}) / 4+L_{\sigma_{i}}(\mathbf{x}) / 2=1 / 4$, which is equivalent to $Q_{\sigma_{i}}(\mathbf{x})-1=L_{\sigma_{i}}(\mathbf{x})=0$ (because $Q_{\sigma_{i}}$ and $L_{\sigma_{i}}$ are integral). But $L_{\sigma_{i}}(\mathbf{x})=0$ is found to be incompatible with $\mathbf{x} \in A$. Hence, the cells $\sigma_{1}, \sigma_{2}, \sigma_{3}$ provide no counter-example to Strong SH.

For $\mathbf{x} \in A \cap \sigma_{4}$, the coefficient $g_{\mu, \nu}^{\lambda}$ is zero if and only if $Q_{\sigma_{4}}(\mathbf{x}) / 4+L_{\sigma_{4}}(\mathbf{x}) / 2=$ $1 / 2$, which is equivalent to $Q_{\sigma_{4}}(\mathbf{x})-2=L_{\sigma_{4}}(\mathbf{x})=0$ or $Q_{\sigma_{4}}(\mathbf{x})=L_{\sigma_{4}}(\mathbf{x})-1=0$. The case $Q_{\sigma_{4}}(\mathbf{x})-2=L_{\sigma_{4}}(\mathbf{x})=0$ is discarded because $L_{\sigma_{4}}(\mathbf{x})=|\lambda|-\mu_{2}-\nu_{2}$, whose vanishing is incompatible with $\mathbf{x} \in A$. On the contrary, $L_{\sigma_{4}}(\mathbf{x})=1$
is compatible with $\mathbf{x} \in A$. Last $Q_{\sigma_{4}}$ factorizes as $\left(|\lambda|-2 \mu_{2}\right)\left(|\lambda|-2 \nu_{2}\right)$. The counter-examples to Strong $\mathbf{S H}$ in $\sigma_{4}$ are thus given by $\mathbf{x} \in A$ and $|\lambda|=\mu_{2}+\nu_{2}+1=2 \mu_{2}$. These are the counter-examples given in Theorem 2.4.

Remark 4.9. The reduced Kronecker coefficients $\bar{g}_{\left(\mu_{2}\right)\left(\mu_{2}\right)}^{\left(\lambda_{2}, \lambda_{3}\right)}$ fulfill Hypothesis Strong PH2, and thus also satisfy Strong SH. (SeeBriand et al. In preparation-b).

Remark 4.10. Let $\mu, \nu$ be partitions with at most two parts. Let $\lambda$ be a partition with at most three parts. Let $\mathbf{x}=\left(\lambda_{1}, \lambda_{2}, \lambda_{3}, \mu_{2}, \nu_{2}\right)$. Then

$$
\widetilde{g}_{\mu, \nu}^{\lambda}(N+1)=N^{2} / 4 Q_{\sigma}(\mathbf{x})+N / 2\left(L_{\sigma}(\mathbf{x})+Q_{\sigma}(\mathbf{x})\right)+g_{\mu, \nu}^{\lambda} .
$$

Remember that for all cells $\sigma$ the polynomials $Q_{\sigma}$ and $L_{\sigma}$ are nonnegative on $\sigma$. This shows that for the Kronecker coefficients indexed by two two-row shapes, the positivity index (see the appendix) is always at most 1 .

## 5. On the complexity of computing the Kronecker Coefficients

In this section we review the proof of the \#P-hardness of Kron given by Bürgisser \& Ikenmeyer (2008), and related results. Next we propose a new, very simple proof using known properties of the reduced Kronecker coefficients. This further underlines the relevance of the reduced Kronecker coefficients in computational complexity issues related to representation-theoretical structural constants.

The class \#P is a class of counting problems introduced by Valiant (1979) in his study of the complexity of computing the permanent (see also Arora \& Barak 2009, Ch. 17). It consists of all functions $f:\{0,1\}^{*} \rightarrow \mathbb{N}$ such that there exists a Turing machine $M$ working in polynomial time, and a polynomial $p$ such that for all $n \in \mathbb{N}$ and all $x \in\{0,1\}^{n}$,

$$
f(x)=\operatorname{Card}\left\{y \in\{0,1\}^{p(n)} \mid M \text { accepts }(x, y)\right\} .
$$

A counting problem, corresponding to $g:\{0,1\}^{*} \rightarrow \mathbb{N}$, is \#P-hard if for every function $f$ in $\# \mathrm{P}$, there exists a polynomial-time Turing reduction from $f$ to $g$ (i.e. $f$ is computed in polynomial time by a Turing Machine that has access to an oracle for $g$ ). The problem is \#P-complete if it is \#P-hard and belongs to \#P. Parsimonious reductions are a special kind of polynomial-time Turing reductions. Given two functions $f, g:\{0,1\}^{*} \rightarrow \mathbb{N}$, one says that $f$ reduces parsimoniously to $g$ (notation: $f \leq_{\text {par }} g$ ) if there exists a function
$\varphi:\{0,1\}^{*} \rightarrow\{0,1\}^{*}$, computable in polynomial time, such that $f(x)=g(\varphi(x))$ for all $x \in\{0,1\}^{*}$.

Let $\lambda$ and $\mu$ be two partitions of length at most $n$. The Kostka number $K_{\lambda, \mu}$ is the dimension of the weight space of weight $\mu$ in the irreducible representation $V_{\lambda}\left(G L_{n}(\mathbb{C})\right)$. Consider the following three problems:

LRCoeff: Given partitions $\lambda, \mu, \nu$ such that $|\lambda|=|\mu|+|\nu|$, compute the Littlewood-Richardson coefficient $c_{\mu, \nu}^{\lambda}$.

Kostka: Given partitions $\lambda$ and $\mu$, compute the Kostka number $K_{\lambda, \mu}$.
KostkaSub: Given partitions $\lambda$ and $\mu$, with $\ell(\lambda) \leq 2$, compute the Kostka number $K_{\lambda, \mu}$.

Narayanan (2006) showed that LRCoEFF is \#P-complete as follows:

- LRCOEFF is in \#P because $c_{\mu, \nu}^{\lambda}$ counts the integral points of the Hive polytopes, which are described as the solution sets of systems of linear inequalities with size polynomial in the bitlength of $\lambda, \mu, \nu$ (that LRCoEFF is in \#P follows the same way from the Littlewood-Richardson rule, GCT3).
- He showed that KostkaSub $\leq_{p a r}$ Kostka $\leq_{p a r}$ LRCoeff and that a known \#P-complete problem (counting all contingency tables with two rows and prescribed column sums and row sums, see Dyer et al. 1997) reduces parsimoniously to KostkaSub.
Bürgisser \& Ikenmeyer (2008) showed that Kron is \#P-hard by exhibiting a reduction KostkaSub $\leq_{p a r}$ Kron based on combinatorial constructions (Kronecker Tableaux) due to Ballantine \& Orellana (2005/07). Their proof, yet elementary, requires careful attention to detail. We propose an alternative, very simple, proof of the \#P-hardness of Kron, relying on known properties of the reduced Kronecker coefficients. Consider the problem:

RKron: Given partitions $\lambda, \mu, \nu$, compute the reduced Kronecker coefficient $\bar{g}_{\mu, \nu}^{\lambda}$.

The \#P-hardness of Kron is a consequence of the \#P-hardness of LRCoEfF and the existence of the following reductions:

- LRCoeff $\leq_{\text {par }}$ RKron. This follows from an observation by Murnaghan (1955) proved by Littlewood (1958): For all partitions $\lambda, \mu, \nu$ such that $|\lambda|=|\mu|+|\nu|$, one has $c_{\mu, \nu}^{\lambda}=\bar{g}_{\mu, \nu}^{\lambda}$.
- RKron $\leq_{\text {par }}$ Kron. This follows from the existence of polynomial (even linear) bounds for the stabilization of the sequence of general term $g_{(n-|\alpha|, \alpha)(n-|\beta|, \beta)}^{(n-|\gamma|, \gamma)}$. For instance, by Vallejo (1999),

$$
\bar{g}_{\alpha, \beta}^{\gamma}=g_{(n-|\alpha|, \alpha)(n-|\beta|, \beta)}^{(n-|\gamma|, \gamma)}
$$

$$
\text { for all } n \geq|\alpha|+|\beta|+\alpha_{1}+\beta_{1}+2|\gamma| \text {. }
$$

In the progression of computation problems associated to the structural constants of the representation theory of the groups $G L_{n}(\mathbb{C})$ and $\mathfrak{S}_{n}$ :

$$
\text { KOSTKA } \leq_{p a r} \text { LRCOEFF } \leq_{p a r} \text { RKRON } \leq_{p a r} \text { KRON }
$$

(which can be continued further to the right with the structural constants of plethysm), the reduced Kronecker coefficients sit between the well-understood Littlewood-Richardson coefficients, and the still mysterious Kronecker coefficients. Understanding the reduced Kronecker coefficients may be a fruitful approach towards the understanding of the Kronecker coefficients. We introduced the reduced Kronecker coefficients in Section 2.2 as limits of sequences of Kronecker coefficients, but they can be defined directly as the structural constants for the Character Polynomials (see Macdonald 1995, I.7, ex. 13 and ex. 14).

## Appendix:

## Erratum to the saturation hypothesis (SH) in "Geometric Complexity Theory VI", by Ketan Mulmuley

Hypotheses SH, PH2 and PH3 are corrected in this appendix by appropriate relaxation without affecting the overall approach of Geometric Complexity Theory (GCT).

Let $H=G L_{n}(\mathbb{C}) \times G L_{n}(\mathbb{C})$ and $\rho: H \rightarrow G=G L\left(\mathbb{C}^{n} \otimes \mathbb{C}^{n}\right)=G L_{n^{2}}(\mathbb{C})$ the natural embedding. Let $\lambda$ and $\mu$ be partitions of length at most $n$, and $\pi$ a partition of length at most $n^{2}$. By a partition $\lambda$, we mean a sequence $\lambda: \lambda_{1} \geq \lambda_{2} \geq \cdots \lambda_{k}>0$ of nonnegative integers, where $k$ is called the height or length of $\lambda$. Let $V_{\lambda}\left(G L_{n}(\mathbb{C})\right)$ and $V_{\mu}\left(G L_{n}(\mathbb{C})\right)$ be the Weyl modules of $G L_{n}(\mathbb{C})$ indexed by the partitions $\lambda$ and $\mu$, and $V_{\pi}(G)$ the Weyl module of $G$ indexed by $\pi$. Let $g_{\lambda, \mu}^{\pi}$ be the Kronecker coefficient. This is the multiplicity of the $H$-module $V_{\lambda}\left(G L_{n}(\mathbb{C})\right) \otimes V_{\mu}\left(G L_{n}(\mathbb{C})\right)$ in the $G$-module $V_{\pi}(G)$, considered as an $H$-module via the embedding $\rho$. Let $\tilde{g}_{\lambda, \mu}^{\pi}(n)=g_{n \lambda, n \mu}^{n \pi}$ be the associated stretching function, where $n$ is a positive integer. It is shown in GCT6 that it is a quasipolynomial.

Here we say that $f(n)$ is a quasipolynomial if there exist polynomials $f_{i}(n)$, $1 \leq i \leq l$, for some positive integer $l$, such that $f(n)=f_{i}(n)$ if $n=i$ modulo $l$. We say it is positive if the coefficients of $f_{i}(n)$ are nonnegative for all $i$. We say it is saturated if $f_{i}(n)>0$ for every $n \geq 1$ whenever $f_{i}(n)$ is not identically zero-this definition is slightly stronger than the one in GCT6. Positivity implies saturation.

It was conjectured in GCT6 that:
(SH) $\tilde{g}_{\lambda, \mu}^{\pi}(n)$ is saturated.
More strongly,
(PH2) $\tilde{g}_{\lambda, \mu}^{\pi}(n)$ is positive.
Theorem 2.4 and Section 2.4 give counter examples to SH and PH2 as stated. A similar phenomenon was also reported in GCT7; GCT8, where it was observed that the structural constants of the nonstandard quantum groups associated with the plethysm problem (of which the Kronecker problem is a special case) need not satisfy an analogue of PH2. But it was observed there that PH2 holds after a small adjustment. Specifically, define the positivity index $p(f)$ of a quasipolynomial $f(n)$ to be the smallest nonnegative integer such
that $f(n+p(f))$ is positive. The saturation index $s(f)$ is defined similarly. As per the experimental evidence in GCT7; GCT8, the positivity (and hence saturation) indices of the structural constants there are small, though not always zero; e.g. see Figures 30, 33, 35 in GCT8. The same can be expected here. This is also supported by the experimental evidence for the Kronecker coefficients indexed by two two-row shapes, where too it may be observed that the positivity index is small (see Section 2.5 and Remark 4.10).

This leads to the following relaxed forms of SH and PH2.
Hypothesis (SH). (a) The quasipolynomial $k(n)=\tilde{g}_{\lambda, \mu}^{\pi}(n)$ is almost saturated; i.e. $s(k)=O(\operatorname{poly}(h))$, where $h \leq n$ is the maximum of the heights of $\lambda, \mu$ and $\pi$. This means there exist nonnegative constants $a$ and $b$ (independent of $n, \lambda, \mu$ and $\pi$ ) such that $s(k) \leq a h^{b}$,
(b) The quasipolynomial $\tilde{g}_{\lambda, \mu}^{\pi}(n)$ is strictly saturated, i.e. the saturation index is zero, for almost all $\lambda, \mu, \pi$. Specifically, the density of the triples $(\lambda, \mu, \pi)$ of total bit length $N$ with nonzero $g_{\lambda, \mu}^{\pi}$ for which the saturation index is not zero is less than $1 / N^{c^{\prime \prime}}$, for any positive constant $c^{\prime \prime}$, as $N \rightarrow \infty$.

The stronger hypothesis than (a) is the following.
Hypothesis (PH2). The quasipolynomial $k(n)=\tilde{g}_{\lambda, \mu}^{\pi}(n)$ is almost positive. This means $p(k)=O($ poly $(h))$.

Let

$$
K(t)=K_{\lambda, \mu}^{\pi}(t)=\sum_{n \geq 0} \tilde{g}_{\lambda, \mu}^{\pi}(n) t^{n}
$$

It is shown in GCT6 that $K(t)$ is rational function that can be expressed in a positive form:

$$
\begin{equation*}
K(t)=\frac{h_{d} t^{d}+\cdots+h_{0}}{\prod_{i=0}^{k}\left(1-t^{a_{i}}\right)^{d_{i}}}, \tag{5.1}
\end{equation*}
$$

where (1) $h_{0}=1$, and $h_{i}$ 's are nonnegative integers, (2) $a_{i}$ 's and $d_{i}$ 's are positive integers, (3) $\sum_{i} d_{i}=d+1$, where $d$ is the degree of the quasipolynomial $\tilde{g}_{\lambda, \mu}^{\pi}(n)$. This positive form is not unique. But GCT6 also associates with $g_{\lambda, \mu}^{\pi}$ a unique positive form that is minimal in a certain sense. Let $\chi_{\lambda, \mu}^{\pi}=\max \left\{a_{i}\right\}$, where $a_{i}$ 's are the degrees occurring in this minimal form. We call it the modular index of $g_{\lambda, \mu}^{\pi}$.

The statement of PH3 in GCT6 should be replaced by the following one.

Hypothesis (PH3). The modular index $\chi_{\lambda, \mu}^{\pi}=O(\operatorname{poly}(h))$.
This is stated as Conjecture 1.6.2 (for the plethysm problem) in GCT6. Here the minimal positive form is not conjectured to be reduced as in GCT6. It can be shown that PH3 also implies $\mathbf{S H}$ (a).

The article GCT6 also suggests an approach to prove a good polynomial bound on the modular index (i.e. PH3) based on the theory of nonstandard quantum groups GCT4; GCT7; GCT8. This is also a natural approach to prove SH (a) (and also PH2) via PH3.

As a preliminary result, it can be verified that the hypothesis PH1 in GCT6, or rather its slightly strengthened form, implies weaker forms of PH2 and SH; specifically, that $p(k)$ (and hence $\mathrm{s}(\mathrm{k})$ ) is $O\left(2^{\operatorname{poly}(h)}\right)$. But this exponential bound is very weak and conservative.

The following is a relaxed version of the Kronecker (decision) problem in GCT6.

Problem (Relaxed Kronecker Problem). Given partitions $\lambda, \mu, \pi$ and a relaxation parameter $c>a h^{b}$, for the nonnegative constants $a$ and $b$ as in the statement of Hypothesis $\mathbf{S H}$ above, decide whether $g_{c \lambda, c \mu}^{c \pi}$ is positive.

Theorem. Assuming PH1 in GCT6 and SH here, the relaxed Kronecker problem can be solved in poly $(\langle\lambda\rangle,\langle\mu\rangle,\langle\pi\rangle,\langle c\rangle)$ time, where $\langle c\rangle$ denotes the bitlength of $c$. In particular, if the relaxation parameter $c$ is small 11, i.e., $O(\operatorname{poly}(h))$, then the time is polynomial in the bitlengths of $\lambda, \mu$ and $\pi$.

Furthermore, there exists a polynomial time algorithm for deciding nonvanishing of $g_{\lambda, \mu}^{\pi}$ that works correctly on almost all $\lambda, \mu$ and $\pi$; almost all has the same meaning here as in $\mathbf{S H}$.

This follows by a slight modification of the proof technique in GCT6.
The hypotheses SH, PH2 and PH3 associated with other decision problems in GCT6 can be relaxed in a similar fashion, and analogues of the above Theorem can be proven for the relaxed versions of those decision problems. SH and PH2 in GCT8 can also be relaxed similarly.

These relaxations do not affect the overall GCT approach to the fundamental lower bound problems in complexity theory, such as the $P$ vs. NP problem in characteristic zero. Because the final goal in GCT is to use the efficient algorithms for the decision problems such as the Kronecker problem above, or

[^0]rather the structure of these algorithms, to show that, for every input size $n$, there exists an obstruction $O_{n}$ that serves as a "proof-certificate" or "witness" of hardness of the explicit function under consideration. When saturation only holds in a relaxed sense, the bit length of the label of this final obstruction $O_{n}$ would get multiplied by a small (polynomial) factor. But this small blow up does not affect the overall approach.

The details of this relaxation would appear in the revised version of GCT6 under preparation.

## Acknowledgements

Emmanuel Briand is supported by a Juan de la Cierva fellowship (MICINN, Spain). Mercedes Rosas is supported by a Ramón y Cajal fellowship (MICINN, Spain). Both are also supported by Projects MTM2007-64509 (MICINN, Spain) and FQM333 (Junta de Andalucia).

## References

Sanjeev Arora \& Boaz Barak (2009). Computational complexity: a modern approach. Cambridge University Press.

Cristina M. Ballantine \& Rosa C. Orellana (2005/07). A combinatorial interpretation for the coefficients in the Kronecker product $s_{(n-p, p)} * s_{\lambda}$. Sém. Lothar. Combin. 54A, Art. B54Af, 29 pp. (electronic).

Emmanuel Briand, Rosa Orellana \& Mercedes Rosas (2008). Quasipolynomial formulas for the Kronecker coefficients indexed by two two-row shapes (extended abstract). arXiv:0812.0861v1. To appear in Discrete Mathematics and Theoretical Computer Science, DMTCS, Proceedings of FPSAC 2009.

Emmanuel Briand, Rosa Orellana \& Mercedes Rosas (In preparation-a). On the stability of the Kronecker product.

Emmanuel Briand, Rosa Orellana \& Mercedes Rosas (In preparation-b). Quasi-polynomial formulas for the Kronecker coefficients indexed by two two-row shapes.

Michel Brion (1993). Stable properties of plethysm: on two conjectures of Foulkes. Manuscripta Math. 4, 347-371.

Michel Brion \& Michèle Vergne (1997). Residue formulae, vector partition functions and lattice points in rational polytopes. J. Amer. Math. Soc. 10(4), 797833.

Andrew A.H. Brown, Stephanie Van Willigenburg \& Mike Zabrocki (2008). Expressions for Catalan Kronecker products. arXiv:0809.3469v1.

Anders Skovsted Buch (2000). The saturation conjecture (after A. Knutson and T. Tao). Enseign. Math. (2) 46(1-2), 43-60. With an appendix by William Fulton.

Peter Bürgisser \& Christian Ikenmeyer (2008). The complexity of computing Kronecker coefficients. In Proceedings of FPSAC 2008 (Formal Power Series and Algebraic Combinatorics). Valparaiso.

Jesús A. De Loera \& Tyrrell B. McAllister (2006). On the computation of Clebsch-Gordan coefficients and the dilation effect. Experiment. Math. 15(1), 7-19.

Martin Dyer, Ravi Kannan \& John Mount (1997). Sampling contingency tables. Random Structures Algorithms 10(4), 487-506.

Ron C. King, Christophe Tollu \& Frédéric Toumazet (2004). Stretched Littlewood-Richardson and Kostka coefficients. In Symmetry in physics, volume 34 of CRM Proc. Lecture Notes, 99-112. Amer. Math. Soc., Providence, RI.

Alexander Klyachko (2004). Quantum Marginal problem and representations of the symmetric group. ArXiv:quant-ph:0409113.

Allen Knutson \& Terence Tao (1999). The honeycomb model of $\mathrm{GL}_{n}(\mathbf{C})$ tensor products. I. Proof of the saturation conjecture. J. Amer. Math. Soc. 12(4), 10551090.

Allen Knutson \& Terence Tao (2001). Honeycombs and sums of Hermitian matrices. Notices Amer. Math. Soc. 48(2), 175-186.

Hanspeter Kraft \& Claudio Procesi (1996). Classical invariant theory, a primer. Lecture Notes, available at http://www.math.unibas.ch/~kraft/.
D. E. Littlewood (1958). Products and plethysms of characters with orthogonal, symplectic and symmetric groups. Canad. J. Math. 10, 17-32.
I. G. Macdonald (1995). Symmetric functions and Hall polynomials. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 2nd edition. With contributions by A. Zelevinsky, Oxford Science Publications.

Ketan D. Mulmuley \& Milind Sohoni (2001). Geometric complexity theory. I. An approach to the P vs. NP and related problems. SIAM J. Comput. 31(2), 496-526 (electronic). (GCT1).

Ketan D. Mulmuley \& Milind Sohoni (2008). Geometric complexity theory. II. Towards explicit obstructions for embeddings among class varieties. SIAM J. Comput. 38(3), 1175-1206. (GCT2).

Ketan D. Mulmuley \& Milind Sohoni (2005). Geometric complexity theory III: on deciding positivity of Littlewood-Richardson coefficients. ArXiv:0501076. (GCT3).

Ketan D. Mulmuley \& Milind Sohoni (2007). Geometric complexity theory IV: quantum group for the Kronecker Problem. ArXiv:0703110. (GCT4).

Ketan D. Mulmuley \& H. Narayanan (2007). Geometric complexity theory V: on deciding nonvanishing of a generalized Littlewood-Richardson coefficient. arXiv:0704.0213. (GCT5).

Ketan D. Mulmuley (2007a). Geometric complexity theory VI: the flip via saturated and positive integer programming in representation theory and algebraic geometry. Technical Report TR-2007-04, Computer Science Department, The University of Chicago. Available as arXiv:0704.0229 and at http://ramakrishnadas.cs.uchicago.edu. Revised version to be available here. (GCT6).

Ketan D. Mulmuley (2007b). On P vs NP, geometric complexity theory, and the flip I: a high-level view. Technical Report TR-2007-09, Computer Science Department, The University of Chicago. Also available as arXiv:0709.0748.

Ketan D. Mulmuley (2008b). Geometric complexity theory VII: Nonstandard quantum group for the plethysm problem. arXiv:0709.0749v1. (GCT7).

Ketan D. Mulmuley (2008c). Geometric complexity theory VIII: On canonical bases for the nonstandard quantum groups. arXiv:0709.0751v2. (GCT8).

Ketan D. Mulmuley (2008a). Erratum to the saturation hypothesis (SH) in "Geometric Complexity Theory VI". Technical report TR2008-10, Computer Science Department, University of Chicago. http://ramakrishnadas.cs.uchicago.edu.

Francis D. Murnaghan (1938). The Analysis of the Kronecker Product of Irreducible Representations of the Symmetric Group. Amer. J. Math. 60(3), 761-784.

Francis D. Murnaghan (1955). On the analysis of the Kronecker product of irreducible representations of $S_{n}$. Proc. Nat. Acad. Sci. U.S.A. 41, 515-518.

Hariharan Narayanan (2006). On the complexity of computing Kostka numbers and Littlewood-Richardson coefficients. Journal of Algebraic Combinatorics 24(3), 347-354.

Etienne Rassart (2004). A polynomiality property for Littlewood-Richardson coefficients. J. Combin. Theory Ser. A 107(2), 161-179.

Jeffrey B. Remmel \& Tamsen Whitehead (1994). On the Kronecker product of Schur functions of two row shapes. Bull. Belg. Math. Soc. Simon Stevin 1, 649-683.

Mercedes H. Rosas (2001). The Kronecker product of Schur functions indexed by two-row shapes or hook shapes. Journal of algebraic combinatorics 14(2), 153-173. Also at arXiv:math.CO/0001084.

Richard P. Stanley (1997). Enumerative combinatorics. Vol. 1, volume 49 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge. With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.

Jean-Yves Thibon (1991). Hopf algebras of symmetric functions and tensor products of symmetric group representations. Internat. J. Algebra Comput. 1(2), 207-221.

Leslie G. Valiant (1979). The complexity of computing the permanent. Theoret. Comput. Sci. 8(2), 189-201.

Ernesto Vallejo (1999). Stability of Kronecker products of irreducible characters of the symmetric group. Electronic journal of combinatorics 6(1), 1-7.

Emmanuel Briand
Departamento de Álgebra, Facultad de Matemáticas, Aptdo. de Correos 1160, 41080 Sevilla, Spain. ebriand@us.es

Mercedes Rosas
Departamento de Álgebra, Facultad de Matemáticas, Aptdo. de Correos 1160, 41080 Sevilla, Spain.
mrosas@us.es

Rosa Orellana
Dartmouth College, Mathematics Department, 6188 Kemeny Hall,
Hanover, NH 03755, USA.
Rosa.C.Orellana@dartmouth.edu


[^0]:    ${ }^{1}$ In this statement it even suffices even if the bitlength of $c$, rather than its value, is $O(\operatorname{poly}(h))$.

