Phase Diagram for the Constrained Integer Partitioning Problem.

C. Borgs[*]   J. T. Chayes[*]   S. Mertens[†]   B. Pittel[‡§]

February 24, 2003

Abstract

We consider the problem of partitioning n integers into two subsets of given cardinalities such that the discrepancy, the absolute value of the difference of their sums, is minimized. The integers are i.i.d. random variables chosen uniformly from the set $\{1, \ldots, M\}$. We study how the typical behavior of the optimal partition depends on n, M and the bias s, the difference between the cardinalities of the two subsets in the partition. In particular, we rigorously establish this typical behavior as a function of the two parameters $\kappa := n^{-1} \log_2 M$ and $b := |s|/n$ by proving the existence of three distinct "phases" in the κb-plane, characterized by the value of the discrepancy and the number of optimal solutions: a "perfect phase" with exponentially many optimal solutions with discrepancy 0 or 1; a "hard phase" with minimal discrepancy of order $Me^{-\Theta(n)}$; and a "sorted phase" with an unique optimal partition of order Mn, obtained by putting the $(s + n)/2$ smallest integers in one subset. Our phase diagram covers all but a relatively small region in the κb-plane. We also show that the three phases can be alternatively characterized by the number of basis solutions of the associated linear programming problem, and by the fraction of these basis solutions whose ± 1-valued components form optimal integer partitions of the subproblem with the corresponding weights. We show in particular that this fraction is one in the sorted phase, and exponentially small in both the perfect and hard phases, and strictly exponentially smaller in the hard phase than in the perfect phase. Open problems are discussed, and numerical experiments are presented.

[*]Microsoft Research, 1 Microsoft Way, Redmond, WA 98052

[†]Institut für Theoretische Physik, Otto-von-Guericke Universität, D-39016 Magdeburg, Germany

[‡]Department of Mathematics, Ohio State University, Columbus, Ohio 43210

1 Introduction

Phase transitions in random combinatorial problems have been the subject of much recent attention. The random optimum partitioning problem is the only NP-hard problem for which the existence of a sharp phase transition has been rigorously established, as have many detailed properties of the transition ([3], see [4] for a short overview). Here we study a constrained version of the random optimum partitioning problem, and extend some of the results of [3] to that case.

The integer optimum partitioning problem is a classic problem of combinatorial optimization in which a given set of n integers is partitioned into two subsets in order to minimize the absolute value of the difference between the sum of the integers in the two subsets, the so-called *discrepancy*. Notice that for any given set of integers, the discrepancies of all partitions have the same parity, namely that of the sum of the n integers. We call a partition *perfect* if its discrepancy is 0, when this sum is even, or 1, when this sum is odd. The decision question is whether there exists a perfect partition. In the uniformly random version, an instance is a given a set of n i.i.d. integers drawn uniformly at random from $\{1, 2, \ldots, M\}$. We will sometimes use the notation $m = \log_2 M$; notice that each of the random integers has m binary bits. Previous work had established a sharp transition as a function of the parameter $\kappa := m/n$, characterized by a dramatic change in the probability of a perfect partition. For M and n tending to infinity in the limiting ratio $\kappa = m/n$, the probability of a perfect partition tends to 0 for $\kappa < 1$, while the probability tends to 1 for $\kappa > 1$. This result was suggested by the work of one of the authors [17] and proved in a paper by the three other authors [3]. See [12] for a beautiful introduction to the optimum partitioning phase transition and some of its properties.

Here we consider a constrained variant of the problem in which we require that the two subsets have given cardinalities; we say that the difference of the two cardinalities is the *bias*, s, of the partition. We establish the phase diagram of the random constrained integer partitioning problem as a function of the two parameters $\kappa := m/n$ and $b := |s|/n$. In the language of statistical physics, b would be called the magnetization, and the problem considered here, where b is constrained to assume a particular value, would be called the "microcanonical" integer partitioning problem. Microcanonical problems are known to be much more difficult than their unconstrained analogues, particularly in the case of random systems.

Let us first review previous rigorous and nonrigorous work on the random optimum partitioning problem. A good deal of rigorous work has been done for the unconstrained random partitioning problem with random numbers drawn from a compact interval in $\mathbb{R}$, which can be interpreted informally as the limiting case of $m \gg n$. Karmarkar and Karp [14] gave a linear time algorithm for a suboptimal solution with a typical discrepancy of order at most $O(n^{-c \log n})$ for some constant $c > 0$. Confirming a conjecture by Karmakar and Karp, Yakir [5] proved that the expected discrepancy delivered by this algorithm is indeed $n^{-\theta(\log n)}$. The optimum solution was studied by Karmarkar, Karp, Lueker and Odlyzko [15] who proved that the typical minimum discrepancy is much smaller, with the median of order $\theta(2^{-n} n^{1/2})$. More recently, Lueker [16] proved exponential bounds for the expected minimum discrepancy. Loosely speaking, these results correspond to m far

exceeding n, and hence $\kappa \to \infty$, thus well above the phase transition of the unconstrained problem which occurs for $\kappa = 1$.

There have also been (nonrigorous) studies of optimum partitioning in the theoretical physics and artificial intelligence communities, where the possibility of a phase transition was examined. Fu [9] noted that the minimum discrepancy is analogous to the ground state energy of an infinite-range, random antiferromagnetic spin model, but concluded incorrectly that the model did not have a phase transition. Gent and Walsh [10] studied the problem numerically and introduced the parameter $\kappa = m/n$. They noticed that the number of perfect partitions falls off dramatically at a transition point estimated to be close to $\kappa = 0.96$. Ferreira and Fontanari studied the random spin model of Fu, and used statistical mechanical methods to get estimates of the optimum partition [7] and to evaluate the average performance of simple heuristics [8]. Ferreira and Fontanari [7] also considered the constrained optimum partitioning problem, noted that the constrained problem is analogous to putting the random antiferromagnet in an external field, and observed that the problem becomes much easier when the bias parameter b satisfies $b > \sqrt{2} - 1$.

Returning to the unconstrained problem, one of the authors of this paper used statistical mechanical methods and the parameterization of Gent and Walsh to derive a compelling, but nonrigorous argument for a phase transition at $\kappa = 1$, and also derived many of the properties of the transition [17]. In a later work, this author [18] analyzed Fu's model by using a heuristic approximation known in statistical mechanics as Derrida's random energy model [6], and obtained the limiting distribution of the k-th smallest discrepancy.

Motivated by the statistical mechanics analysis in [17] and [18], the other three authors of this paper undertook an extensive rigorous study of the random integer partitioning problem [3]. They established the existence of a transition at $\kappa_c = 1$ below which the probability of a perfect partition tends to one with n and m, and above which it tends to zero, and also gave the finite-size scaling window of the transition: namely, in terms of the more detailed parametrization $m = \kappa_n$ with $\kappa_n = 1 - \log_2 n/(2n) + \lambda_n/n$, the probability of a perfect partition tends to 1, 0, or a computable λ-dependent constant strictly between 0 and 1, depending on whether λ_n tends to $-\infty$, ∞, or $\lambda \in (-\infty, \infty)$, respectively. The work also calculated the distribution of the number of perfect partitions, the distribution of the minimum discrepancy, and the joint distribution of the k smallest discrepancies, which give the entropy, the ground state energy and the bottom of the energy spectrum, respectively. In particular, the paper [3] provided a rigorous justification of the Derrida-type approximation both inside and above the scaling window, insofar as the joint distribution of k (finite) smallest discrepancies is concerned.

The location of the phase transition for the unconstrained problem immediately yields a one-dimensional phase diagram as a function of κ: For $\kappa \in (0, \kappa_c)$ with $\kappa_c = 1$, the system is in a "perfect phase" in which the probability of a perfect partition tends to 1 as M and n tend to infinity in the fixed function κ. For $\kappa \in (\kappa_c, \infty)$, the probability of a perfect partition tends to 0, and moreover, there is an unique optimal partition. We call this the "hard phase," since for $\kappa > \kappa_c$, it is presumably computationally difficult to find the optimal partition.

In this work, we consider the constrained optimum partitioning problem with bias s and extend the phase diagram to the two-dimensional κb-plane. See Figure 1. In addition to the extensions of the perfect and hard phases, we establish the existence of a new phase which we call the "sorted phase."
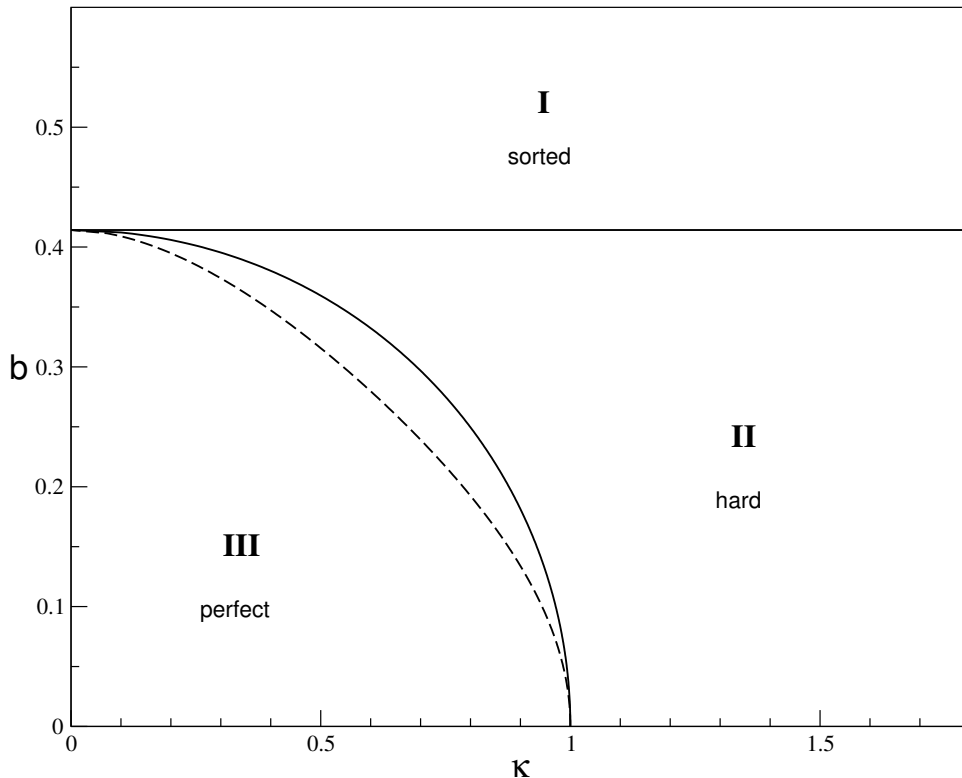

Figure 1: Phase diagram of the constrained integer partitioning problem.

The sorted phase is easy to understand. One way to meet the bias constraint is to take the $(s + n)/2$ smallest integers and put them in one subset of the partition.[1] It is not difficult to see that the resulting "sorted partition" is optimal if the total weight of this subset is at least half of the sum of all n integers. We define the sorted phase as the subset of the κb-plane where the sorted partition is optimal. We prove that the sorted phase is given by the condition

$$b > b_c := \sqrt{2} - 1, \tag{1.1}$$

see region III in Figure 1. Moreover, we show that the minimal discrepancy in this phase is of the order Mn. The region $b > \sqrt{2} - 1$ is precisely where Ferreira and Fontanari [7] observed that the corresponding statistical mechanical problem becomes "self-averaging."

Our analysis of the perfect and hard phases for $b < b_c$ is much more difficult. In this region, we use integral representations for the number of partitions with a given

---

[1]Note that the task of finding this partition is even easier than the task of sorting the n integers, which would take, on average, $\theta(n \log n)$ comparisons. Instead, the $(s + n)/2$ smallest integers can be found in strictly linear time in n.

discrepancy and bias; these representations generalize those used in [3]. The asymptotic analysis of the resulting two-dimensional random integrals leads to saddle point equations for a saddle point described in terms two real parameters η and ζ. For discrepancies of order $o(M)$ (including, in particular, the case of perfect partitions), the saddle point equations determining ζ and η are:

$$\int\limits_0^1 x \tanh(\zeta x + \eta) \, dx = 0,$$

$$\int\limits_0^1 \tanh(\zeta x + \eta) \, dx = -b. \tag{1.2}$$

The solution (ζ, η) of these equations can be used to define the two convex curves in Figure 1. To this end, let[2]

$$L(\zeta, \eta) := b\eta + \int\limits_0^1 \log(2\cosh(\zeta x + \eta)) \, dx \tag{1.3}$$

$$\rho(\zeta, \eta) := 1 - \frac{\tanh(\zeta + \eta) - \tanh(\eta)}{2\zeta}. \tag{1.4}$$

For (ζ, η) a solution of (1.2), we then define

$$\kappa_-(b) := -\log_2 \rho(\zeta, \eta),$$
$$\kappa_c(b) := \frac{1}{\log 2} L(\zeta, \eta). \tag{1.5}$$

From bottom to top, the two convex curves joining $(0, b_c)$ and $(1, 0)$ in Figure 1 are then given by $\kappa = \kappa_-(b)$ and $\kappa = \kappa_c(b)$.

In this paper, we prove that, in the region $\kappa < \kappa_-(b)$, with probability tending to one as n tends to infinity (or, more succinctly, with high probability, w.h.p.) there exist perfect partitions; see region I in Figure 1. Moreover the number of perfect partitions is about $2^{(\kappa_c - \kappa)n}$ in this "perfect phase." We also prove that w.h.p. there are no perfect partitions in the region $b < b_c$ and $\kappa > \kappa_c(b)$. As in the unconstrained problem, we call this the "hard phase." Our results leave open the question of what happens in the narrow region $\kappa_- < \kappa < \kappa_c$, and also whether the optimal partition is unique in the hard phase; see the final section for a discussion of this and other open questions.

We are also able to prove that these phase transitions correspond to qualitative changes in the solution space of the associated linear programming problem (LPP). In the actual optimum partitioning problem, each integer is put in one subset or the other. The relaxed version is defined by allowing any fraction of each integer to be put in either of the two partitions. Using our theorems on the typical behavior of integer partitioning problem and

---

[2]It turns out the solutions of the saddle point equations 1.2 are just the stationary points of the function $L(\zeta, \eta)$

some general properties of the LPP, we show the following. In the sorted phase, i.e. for $b > b_c = \sqrt{2} - 1$, w.h.p. the LPP has a unique solution given by the sorted partition itself. For $b < b_c$, i.e. in the perfect and hard phases, w.h.p. the relaxed minimum discrepancy is zero, and the total number of optimal basis solutions is exponentially large, of order $2^{k_c(b)n + O_p(n^{1/2})}$. Finally, in the perfect and hard phases, we consider the fraction of these basis solutions whose integer-valued components form an optimal integer partition of the subproblem with the corresponding subset of the weights. We show that this fraction is exponentially small. Moreover, except for the crescent-shaped region between $\kappa = \kappa_-(b)$ and $\kappa = \kappa_c(b)$, we show that the fraction is strictly exponentially smaller in the hard phase than in the perfect phase. This fraction thus represents some measure of the algorithmic difficulty of the problem, see Remark 8.1.

The outline of the paper is as follows. In the next section, we define the problem in detail, and precisely state our main results. In Section 3, we introduce our integral representation and show how it leads to the relevant saddle point equations. We also give a brief heuristic derivation of some of the phase boundaries. Section 4 contains a proof of existence and properties of the solution of the saddle point equations for $b < b_c$. In Section 5, we establish an asymptotic formula for the number of partitions with given discrepancy and bias in the perfect phase. As a corollary, we obtain both the existence of exponentially many perfect partitions for $\kappa < \kappa_-(b)$, and a theorem on the distribution of the bias in the unconstrained problem for $\kappa < 1$. The analysis of the hard phase is done in Section 6. In Section 7, we prove that the sorted partitions are optimal for $b > b_c$. We also show why the sorted phase boundary coincides with the boundary for existence of solutions of the saddle point equations. In Section 8, we formulate the relaxed version of the optimum partitioning problem, and establish our results on the space of basis solutions of the LPP. Finally, in Section 9, we discuss open problems and a few numerical experiments addressing some of these problems.

2   Statement of Main Results

Let $X_1, \ldots, X_n$ be n independent copies of a generic random variable which is distributed uniformly on $\{1, \ldots, M\}$. We are interested in the case when M grows exponentially with n, and define κ as the exponential rate, i.e.

$$\kappa = \frac{1}{n} \log_2 M. \tag{2.1}$$

To avoid trivial counterexamples, we will always assume that κ stay bounded away from both 0 and ∞ as $n \to \infty$. We will use $\mathbb{P}$ and $\mathbb{E}$, with or without subindex n, to denote the probability measure and the expectation induced by $\mathbf{X} = (X_1, \ldots, X_n)$.

A partition of integers into two disjoint subsets is coded by an n-long binary sequence $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$, $\sigma_j \in \{-1, 1\}$; so the subsets are $\{j : \sigma_j = 1\}$ and $\{j : \sigma_j = -1\}$. Obviously $\boldsymbol{\sigma}$ and $-\boldsymbol{\sigma}$ are the codes of the same partition. Given a partition $\boldsymbol{\sigma}$, we define

its *discrepancy* (or energy), $d(\mathbf{X}, \boldsymbol{\sigma})$, and *bias* (or magnetization), $s(\boldsymbol{\sigma})$, as

$$d(\mathbf{X}, \boldsymbol{\sigma}) = |\boldsymbol{\sigma} \cdot \mathbf{X}|, \text{ with } \boldsymbol{\sigma} \cdot \mathbf{X} = \sum_{j=1}^{n} \sigma_j X_j, \tag{2.2}$$

$$s(\boldsymbol{\sigma}) = \boldsymbol{\sigma} \cdot \mathbf{e} = |\{j : \sigma_j = 1\}| - |\{j : \sigma_j = -1\}|. \tag{2.3}$$

Here $\mathbf{e}$ is the vector $(1, \ldots, 1)$. Clearly $s(\boldsymbol{\sigma})$ is an integer in $\{-n, \ldots, n\}$, so let $s \in \{-n, \ldots, n\}$ and define the bias density

$$b = \frac{|s|}{n} \tag{2.4}$$

so that $b \in [0, 1]$. Note that by symmetry it suffices to consider $s(\boldsymbol{\sigma}) \in \{0, \ldots, n\}$, so we will often take a non-negative integer $s \in \{0, \ldots, n\}$, in which case $s = bn$. We define an *optimum partition* as a partition $\boldsymbol{\sigma}$ that minimizes the discrepancy $d(\mathbf{X}, \boldsymbol{\sigma})$ among all the partitions with bias equal to s, and a *perfect partition* as a partition $\boldsymbol{\sigma}$ with $|d(\mathbf{X}, \boldsymbol{\sigma})| \leq 1$.

Theorems B, C and D below describe our main results on the phases labelled I, II, and III in Figure 1 in the introduction. In the statement of these theorems we will use the parameters $\zeta, \eta, \kappa_c(b)$ and $\kappa_-(b)$ defined in (1.2) – (1.5). Before getting to principal results, we must begin with an existence statement for the parameters ζ, η.

Theorem A *Let $b < b_c$, where $b_c = \sqrt{2} - 1$. Then the saddle point equations (1.2) have a unique solution $(\zeta, \eta) = (\zeta(b), \eta(b))$.*

This theorem is proved in Section 4.

Let

$$Z_n(\ell, s) = Z_n(\ell, s; \mathbf{X}) \tag{2.5}$$

denote the random number of partitions $\boldsymbol{\sigma}$ with $\boldsymbol{\sigma} \cdot \mathbf{X} = \ell$ and $\boldsymbol{\sigma} \cdot \mathbf{e} = s$. Since $s(\boldsymbol{\sigma})$ has the same parity as n, and $d(\mathbf{X}, \boldsymbol{\sigma})$ has the same parity as $\sum_{j=1}^{n} X_j$, we will only consider values of s which have the same parity as n, and values of ℓ which have the same parity as $\sum_{j=1}^{n} X_j$. In the theorems in this section and in much of the rest of the paper, we will not state these restrictions explicitly.

Our central goal is to use the saddle point solution in order to bound the $Z_n(\ell, s)$ for various given values of ℓ and s. To formulate our results in a compact, yet unambiguous form, we use a shorthand $a_n < a$ ($a_n > a$, resp.) instead of $\limsup a_n < a$ ($\liminf a_n > a$, resp.), even when the n-dependence of a_n is only implicit, as in $\kappa = n^{-1} \log_2 M$ and $b = |s/n|$. We will also use the notation $f_n = O_p(g_n)$ and $f_n = o_p(h_n)$ if f_n/g_n is bounded in probability and f_n/h_n goes to zero in probability, respectively. Also, as is customary, we will say that an event happens with high probability (w.h.p.) if the probability of this event approaches 1 as $n \to \infty$. In all our statements n, M, s and ℓ will be integers with $n \geq 1$, $M \geq 1$ and $s \geq 0$. Our main results in the perfect phase are summarized in the next theorem and remark.

Theorem B *Let $\ell = o(Mn^{1/2}), b < b_c$ and $\kappa < \kappa_-(b)$. Then w.h.p. $Z_n(\ell, s) \geq 1$ and*

$$Z_n(\ell, s) = 2^{[\kappa_c(b) - \kappa]n} e^{S_n n^{1/2} + o(n^{1/2})}, \tag{2.6}$$

where S_n converges in probability to a Gaussian with mean zero and variance $\sigma^2 = Var(\log(2\cosh(\zeta U + \eta)))$, with U uniformly distributed on $[0,1]$. Consequently, w.h.p., there exist exponentially many perfect partitions, with $\ell = 0$ if $\sum_j X_j$ is even, and $|\ell| = 1$ if $\sum_j X_j$ is odd.

Remark 2.1 *Under the conditions of Theorem B, we actually prove a much more accurate estimate. Namely, we show that there are 2×2 positive definite matrices R and K with deterministic entries, and a constant $q < 1$ such that, with probability $1 - O(q^{\log^2 n})$,*

$$Z_n(\ell, s) = \exp\left(\zeta\frac{\ell}{M} + \eta s + \sum_{j=1}^n \log(2\cosh(\zeta X_j/M + \eta))\right) \frac{\exp(-\frac{1}{4}\boldsymbol{\tau}_n R^{-1}\boldsymbol{\tau}'_n)}{\pi M n\sqrt{det\ R}}(1 + o(1)).$$

(2.7)

Here $\boldsymbol{\tau}_n$ is a two-dimensional random vector which converges in probability to a Gaussian vector $\boldsymbol{\tau}$ with zero mean and covariance matrix K. See Theorem 5.1 in Section 5.1.

We also prove a corollary relating the distribution of the bias in the unconstrained problem to the distribution of the bias between heads and tails in fair coin flips; see Subsection 5.2.

The proof of Theorem B and Remark 2.1 is given in Section 5.

Note that the above expression for $Z_n(\ell, s)$ is much more complicated than its analogue in the unconstrained case, see equation (2.6) in [3]. Both the sum in the first exponent and the entire second exponent represent fluctuations which were not present in the unconstrained case, and which make the analysis of the perfect phase much more difficult here; see also Remark 2.4 below.

Our next theorem, which describes our main results on the hard phase, has two parts: The first shows that there are no perfect partitions above $\kappa = \kappa_c(b)$, and the second gives a bound on the number of optimum partition for $\kappa > \kappa_-$. To state the theorem, let $d_{opt} = d_{opt}(n; s)$ denote the discrepancy of the optimal partition, and let $Z_{opt} = Z_{opt}(n; s)$ denote the number of optimal partitions.

Theorem C *Let $b < b_c$.*

a) *If $\kappa > \kappa_c(b)$, then there exists a $\delta > 0$ such that with probability $1 - O(e^{-\delta \log^2 n})$ there are no perfect partitions, and moreover*

$$d_{opt} \geq 2^{n[\kappa - \kappa_c(b)] - O_p(n^{1/2})}.$$

(2.8)

b) *If $\kappa > \kappa_-(b)$ and $\varepsilon > 0$, then there exists a constant $\delta > 0$ such that*

$$d_{opt} \leq 2^{n[\kappa - \kappa_-(b) + \varepsilon]},$$

(2.9)

and

$$Z_{opt} \leq 2^{n[\kappa_c(b) - \kappa_-(b) + \varepsilon]},$$

(2.10)

both with probability $1 - O(e^{-\delta \log^2 n})$.

This theorem is proved in Section 6. However, perhaps somewhat surprisingly, the proof of the upper bound in (2.9) runs parallel to the proof of Theorem B that established existence of perfect partitions for $\kappa < \kappa_-(b)$.

Remark 2.2 *We believe that the bound in* (2.8) *is actually sharp. If we* assume *that this is the case, in fact, even if we assume that the weaker bound*

$$d_{opt} = 2^{n(\kappa - \kappa_c + o_p(1))} \tag{2.11}$$

holds w.h.p. whenever $\kappa > \kappa_c$*, then we can significantly improve the upper bound* (2.10)*. Indeed, under the assumption* (2.11)*,* Z_{opt} *grows subexponentially with* n *whenever* $\kappa > \kappa_c(b)$*, see Remark 6.1 (iii).*

The optimum partition problem is much simpler for $b > b_c$. Our main result on the sorted phase is the following theorem, which is proved in Section 7.

Theorem D *Let* $b > b_c$*. Then w.h.p. the optimal partition is uniquely obtained by putting* $(s+n)/2$ *smallest integers* X_j *in one part, and the remaining* $(n-s)/2$ *integers into another part. W.h.p.,* d_{opt} *is asymptotic to* $\frac{Mn}{4}\left[(1+b)^2 - 2\right]$*, i.e., of order* Mn*.*

By this theorem, for b sufficiently large, the partition is determined by the decreasing order of weights X_j, but not by the actual values of X_j.

Until now, all our statements have been about the likely properties of the optimum partition $\boldsymbol{\sigma}$, whose components are allowed to assume only two values, -1 and $+1$. In an interesting twist, these results shed light on the likely properties of the related linear programming problem (LPP): find the minimum value of d subject to linear constraints

$$-d \le \sum_{j=1}^n \sigma_j X_j, \quad \sum_{j=1}^n \sigma_j X_j \le d,$$
$$\sum_{j=1}^n \sigma_j = s,$$
$$-1 \le \sigma_j \le 1, \quad (1 \le j \le n).$$

We denote this minimum value of d by d_{opt}^{LPP}. Our last theorem indicates that the LPP inherits the phase diagram of the optimum partition problem, and moreover provides, however incomplete, some way to rate the three regions according the algorithmic difficulty of the optimal partition problem. To make this precise, we define $F_n(\kappa, b)$ to be the fraction of basis solutions $\boldsymbol{\sigma}$ with the property that the ± 1-valued components σ_i form an optimal partition of the corresponding subproblem with weights X_i. Henceforth, we will call this the "optimal subpartition property."

Theorem E a) *If* $b > b_c$*, then w.h.p. the sorted partition is a unique solution of the LPP, and thus* $d_{opt}^{LPP} = \Theta(Mn)$ *and* $F_n(\kappa, b) = 1$*.*

   Let $b < b_c$*.*

   b) *Then w.h.p.* $d_{opt}^{LPP} = 0$*. In addition, w.h.p. there are* $2^{[\kappa_c(b) + o(1)]n}$ *basis solutions, each having either none or exactly two components* $\sigma_i \neq \pm 1$*.*

c) W.h.p. $F_n(\kappa, b) = 2^{-[\kappa+o(1)]n}$ *for* $\kappa < \kappa_-(b)$, *and* $2^{-[\kappa_c(b)+o(1)]n} \leq F_n(\kappa, b) \leq 2^{-[\kappa_-(b)+o(1)]n}$ *for* $\kappa > \kappa_-(b)$.

Remark 2.3 *(i) If one assume that the number of optimal partitions Z_{opt} in the hard phase grows subexponentially with probability at least $1 - o(n^{-2})$ (see Remark 2.2 for a motivation of this assumption), our upper bound on the fraction $F_n(\kappa, b)$ in the hard phase can be improved to match the lower bound, yielding $F_n(\kappa, b) = 2^{-n[\kappa_c(b)+o(1)]}$ in the hard phase, see Remark 8.1 (i).*

(ii) If, on the other hand, the asymptotics of Theorem 5.1 hold up to κ_c, more precisely, if one assumes that for $b < b_c$ and $\kappa < \kappa_c(b)$

$$Z_n(\ell, s) = 2^{n[\kappa_c(b)-\kappa+o(1))]} \tag{2.12}$$

holds with probability least $1 - o(n^{-2})$, then a bound of the form $F_n(\kappa, b) = 2^{-n[\kappa+o(1)]}$ can be extended to all $\kappa < \kappa_c$, see Remark 8.1 (ii).

We close this section with a few additional remarks and an additional theorem on the expected number of perfect partitions. We start with a discussion of Theorem B.

Remark 2.4 *While (2.6) has only been proved for $\kappa < \kappa_-(b)$,* an upper bound *of the same form can be shown to hold for all κ, see Theorem 6.1. Due to the random fluctuations of the Gaussian term, this upper bound is of order $e^{-\Theta(n^{1/2})}$ with positive probability as soon as $\kappa \geq \kappa_c(b) - O(n^{-1/2})$, so that in this regime, there are no perfect partitions with probability bounded away from zero. Note, however, that as $b \to 0$, the variance $\sigma^2 = Var(\log(2\cosh(\zeta U + \eta)))$ of the Gaussian term tends to zero.*

We expect that for all $b \in (0, b_c)$ fluctuations of this kind persist around the true threshold, whether it is actually equal to $\kappa_c(b)$, or whether it is some other value $\tilde{\kappa}_c(b) < \kappa_c(b)$. For the constrained partition problem with $b \in (0, b_c)$, we therefore expect a scaling window of width at least $n^{-1/2}$ in which the probability of perfect partitions lies strictly between 0 and 1. This is to be contrasted with the unconstrained case, where we had a very narrow scaling window of width $\Theta(n^{-1})$ about the transition point κ_c, see [3].

Next let us consider the statements of Theorem C. Here again the situation is much more complicated than in the unconstrained case. By Theorem B and the lower bound in Theorem Ca, the minimum discrepancy changes from being at most one to being exponentially large as κ crosses the interval $[\kappa_-, \kappa_c]$. However, we also prove (see Section 6.2) that the *expected* number of perfect partitions remains exponentially large until κ reaches a value strictly exceeding κ_c. This is the content of the following theorem and remark.

Theorem F *Let $\ell \in \{-1, 0, 1\}$ and $b \in (0, 1)$. Then*

$$\lim_{n\to\infty} \left[n^{-1} \log \mathbb{E}(Z_n(\ell, s)) - R(\kappa, b) \right] = 0 \tag{2.13}$$

where

$$R(\kappa, b) = H((1+b)/2) + \lambda b + \log(\lambda^{-1} \sinh \lambda) - \kappa \log 2, \tag{2.14}$$

with $H(u) = u \log(1/u) + (1-u)\log(1/(1-u))$, and λ satisfying $\coth \lambda = \lambda^{-1} - b$.

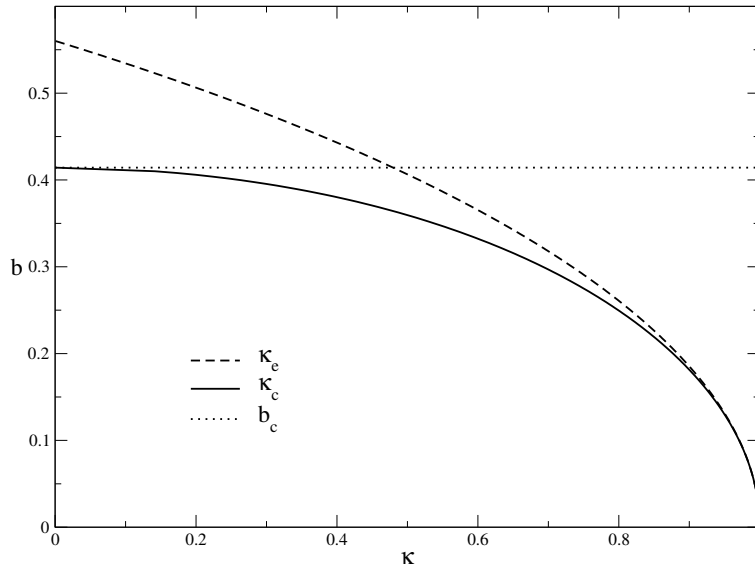Figure 2: The curves $\kappa = \kappa_c(b)$, $\kappa = \kappa_e(b)$ and $b = b_c$.

Remark 2.5 *Graphing the curve $R(\kappa, b) = 0$, i.e.*

$$\kappa = \kappa_e(b) := \frac{H((1+b)/2) + \lambda b + \log(\lambda^{-1} \sinh \lambda)}{\log 2}, \tag{2.15}$$

we see that it lies strictly above $\kappa = \kappa_c(b)$, except at the only common point $\kappa = 1, b = 0$, see Fig. 2. In particular, the curve intersects the b-axis at $b = 0.56 \cdots > b_c = 0.41 \ldots$. Thus for the points (κ, b) between the curves $\kappa = \kappa_c(b)$ and $\kappa = \kappa_e(b)$, the expected number of perfect partitions grows exponentially, while w.h.p. there are no perfect partitions at all. This complex behavior did not manifest itself in the unconstrained optimum partitioning problem [3].

We close this section with a discussion of the results of Theorem E.

Remark 2.6 *Clearly, the fraction $[F_n(\kappa, b)]^{-1}$ is the expected number of times one has to generate a uniformly random basis solution of the LPP to get a basis solution with the optimal subpartition property. In absence of a better candidate, $[F_n(\kappa, b)]^{-1}$ seems to be a possible measure of algorithmic difficulty of the integer partition problem. Our theorem says that w.h.p. this measure is lowest for the sorted phase ($b > b_c$) where $[F_n(\kappa, b)]^{-1} = 1$), next lowest for the perfect phase ($b < b_c$ and $\kappa < \kappa_-(b)$) where $[F_n(\kappa, b)]^{-1} = 2^{\kappa n + o(n)}$, and indeed hardest in the hard phase ($b < b_c$ and $\kappa > \kappa_c(b)$) where $[F_n(\kappa, b)]^{-1} \geq 2^{(\kappa_-(b) + o(1))n}$.*

If we make the additional assumptions of Remark 2.3, we have that $[F_n(\kappa, b)]^{-1} = 2^{\kappa n + o(n)}$ for $b < b_c$ and $\kappa < \kappa_c(b)$, while $[F_n(\kappa, b)]^{-1} = 2^{\kappa_c n + o(n)}$ for $\kappa > \kappa_c$. This gives an easy-hard-easy picture along any curve $b = b(\kappa)$, $\kappa \geq 0$, that crosses the lines $\kappa = \kappa_c(b)$ and $b = b_c$, provided that $b(\kappa)$ is strictly increasing in κ. Indeed, at a point (κ, b) on such a curve $[F_n]^{-1}$ grows exponentially in $n\kappa$, as long as $\kappa < \kappa_c(b(\kappa))$, i.e. until the curve $b = b(\kappa)$ intersects $\kappa = \kappa_c(b)$. For larger values of κ, $[F_n]^{-1}$ grows at the exponential rate

$n\kappa_c(b(\kappa)) < n\kappa$. *Once the curve* $b = b(\kappa)$ *crosses the horizontal line* $b = b_c$, *the problem becomes even easier with* $[F_n]^{-1} = 1$. *In fact, above this line, the problem becomes easy in the usual sense, since the rounded and the fractional problem are identical, and sorted partitions can be found in linear time.*

3 Preliminaries and Outline of Proof Strategy

In this section, we define our notation, review the heuristics of the proof, and point out why naive extensions of the unconstrained analysis of [3] fail in the constrained case.

3.1 Sorted Partitions

We first discuss our strategy to prove that in region III, the optimal partition is sorted and has discrepancy of order Mn. To this end, we consider n weights $X_1, \ldots, X_n$, chosen uniformly at random from $\{1, \ldots, M\}$, and reorder them in such a way that their sizes are increasing, $X_{\pi(1)} \leq X_{\pi(2)} \leq \cdots \leq X_{\pi(n)}$, where $\pi(1), \ldots, \pi(n)$ is a suitable permutation of $1, \ldots, n$. Since M is assumed to grow exponentially with n, we have, in particular, $n^2 = o(M)$, which implies that w.h.p. no two weights are equal. So w.h.p. the permutation π is unique and $X_{\pi(1)} < X_{\pi(2)} < \cdots < X_{\pi(n)}$.

Given a bias $s > 0$, (with $s \equiv n \pmod 2$), we need to find an optimum partition that puts $k = (s + n)/2$ integers in one part, and the remaining $n - k$ integers into another part. One such feasible partition is obtained if we select the k smallest integers for the first part; we call it the sorted partition. It is coded by the $\boldsymbol{\sigma}$, with $\sigma_{\pi(i)} = 1$ for $i \leq k$ and $\sigma_{\pi(i)} = -1$ for $i > k$. If the total weight of $(n - k)$ largest weights is, at most, the total weight of k smallest weights, then it is intuitively clear that the sorted partition is optimal. More precisely: if

$$\delta_s(\boldsymbol{X}) = \sum_{j=1}^{k} X_{\pi(j)} - \sum_{j=k+1}^{n} X_{\pi(j)} \geq 0 \tag{3.1}$$

then the sorted partition is the unique, optimal partition, and the minimal discrepancy is

$$d_{opt} = \delta_s(\boldsymbol{X}). \tag{3.2}$$

See Section 6.3 for a formal proof.[3]

To determine the phase boundary of the phase III, we thus have to determine the region of the phase diagram in which w.h.p. the sorted partition meets the condition (3.1). Leaving the probabilistic technicalities out of our heuristic discussion, let us replace the condition (3.1) by its mean version, namely $\mathbb{E}(\delta_s(\mathbf{X})) \geq 0$. Consider an arbitrary $b \in (0, 1]$. Let $x_0 = (1 + b)/2$ and $M_0 = \lfloor x_0 M \rfloor$. For a typical set of weights $X_1, \ldots, X_n$, let us consider the sorted partition with $\sigma_j = 1$ for $X_j \leq M_0$, and $\sigma_j = -1$ for $X_j > M_0$. Since the probability that $X_j \leq M_0$ is equal to $\tilde{x}_0 = M_0/M = x_0 + O(M^{-1})$, we get that

---

[3]If $\delta_s(\boldsymbol{X}) = -1$, the sorted partition is still optimal (it is, in fact, perfect). But in general, it is not the unique optimum partition.

the expected number of weights X_j with $X_j \leq M_0$ is $n\tilde{x}_0$, implying that the expected bias is $2n\tilde{x}_0 - n = nb + O(n/M)$. The expected discrepancy can be calculated in a similar manner, giving the expression

$$
\begin{aligned}
\mathbb{E}\bigg[\sum_j X_j \mathbb{I}\Big(X_j \leq \lfloor x_0 M \rfloor\Big) &- \sum_j X_j \mathbb{I}\Big(X_j > \lfloor x_0 M \rfloor\Big) \bigg] \\
&= \frac{n}{M}\bigg[M_0(1 + M_0) - \frac{M(1+M)}{2} \bigg] \\
&= \Big[x_0^2 - \frac{1}{2} + O(M^{-1}) \Big] Mn \\
&= \bigg[\Big(\frac{b+1}{2}\Big)^2 - \frac{1}{2} + O(M^{-1}) \bigg] Mn.
\end{aligned}
\tag{3.3}
$$

So, $\mathbb{E}(\delta_s(\mathbf{X}))$ is large positive, of order Mn, iff $(b+1)^2/4 - 1/2 > 0$, or equivalently $b > b_c = \sqrt{2} - 1$. In Section 6.3 we prove the condition $b > b_c$ is both necessary and sufficient for $\delta_s(\mathbf{X})$ to be, w.h.p., positive, of order Mn. In language of statistical mechanics, we show that, for $b > b_c$, $\delta_s(\mathbf{X})$ is "self-averaging," i.e. its distribution is sharply concentrated around $\mathbb{E}(\delta_s(\mathbf{X}))$.

Remark 3.1 *On the heuristic level presented here, the above arguments can easily be generalized to an arbitrary distribution for the weights $X_1, \ldots, X_n$, as long as these weights are independent copies of a generic (discrete) variable X with a reasonably well behaved probability distribution. Assuming, e.g., that the variable X/M has a limiting distribution with density μ, one obtains that the critical value of b is given by $b_c = b_c(\mu) = 2 \int_0^{x_0} \mu(x)\, dx - 1$, where x_0 is determined by the equation $\int_0^{x_0} x\mu(x)\, dx = \int_{x_0}^{\infty} x\mu(x)\, dx$. However, we have not tried to extend all our results to this more general μ-density case.*

3.2 Integral Representations

Let us now turn to the much more difficult region $b < b_c$. Without loss of generality, we may take $s \geq 0$, so that $b = s/n$.

Let $Z_n(\ell, s) = Z_n(\ell, s; \mathbf{X})$ denote the total number of partitions $\boldsymbol{\sigma}$ such that $\boldsymbol{\sigma} \cdot \mathbf{X} = \ell$ and $\boldsymbol{\sigma} \cdot \mathbf{e} = s$. Guided by the results of [3], one might hope to prove that, as the parameter $\kappa = n^{-1} \log_2 M$ is varied, the model undergoes a phase transition between a region with exponentially many perfect partitions and a region with no perfect partitions. Since perfect partitions correspond to $\ell = 0$ or $\ell = \pm 1$, we will be mainly interested in $Z_n(\ell, s)$ for $|\ell| \leq 1$, while s will typically be chosen proportional to n.

A starting point in [3] was an integral (Fourier-inversion) type formula for $Z_n(\ell) = Z_n(\ell; \mathbf{X})$, the total number of $\boldsymbol{\sigma}$'s such that $\boldsymbol{\sigma} \cdot \mathbf{X} = \ell$, namely

$$
Z_n(\ell) = \frac{2^n}{\pi} \int_{x \in (-\pi/2, \pi/2]} \cos(\ell x) \prod_{j=1}^{n} \cos(x X_j)\, dx.
\tag{3.4}
$$

We need to derive a two-dimensional counterpart of that formula for $Z_n(\ell, s)$. To this end, let us first recall that by (2.3), $s = 2|\{j : \sigma_j = 1\}| - n$, so that a generic value s

of $s(\boldsymbol{\sigma})$ must meet the condition $n + s \equiv 0 \pmod 2$. In a similar way, we get that $\boldsymbol{\sigma} \cdot \mathbf{X}$ has the same parity as the sum $\sum_j X_j$. Keeping this in mind, we have that on the event $\{\sum_j X_j \equiv \ell \pmod 2\}$, for $n + s \equiv 0 \pmod 2$,

$$
\mathbb{I}(\boldsymbol{\sigma} \cdot \mathbf{X} = \ell, \, \boldsymbol{\sigma} \cdot \mathbf{e} = s) = \frac{1}{\pi^2} \iint_{x,y \in (-\pi/2, \pi/2]} e^{i(\boldsymbol{\sigma} \cdot \mathbf{X} - \ell)x} \, e^{i(\boldsymbol{\sigma} \cdot \mathbf{e} - s)y} \, dx dy, \tag{3.5}
$$

thus extending (4.6) in [3]. Multiplying both sides of the identity by 2^n, and summing over all $\boldsymbol{\sigma}$, we obtain

$$
\begin{aligned}
Z_n(\ell, s) &= \frac{2^n}{\pi^2} \iint_{x,y \in (-\pi/2, \pi/2]} e^{-i(\ell x + s y)} \prod_{j=1}^{n} \cos\big(x X_j + y\big) \, dx dy. \\
&= 2^n \, \mathbb{P}_{1/2}\Big(\boldsymbol{\sigma} \cdot \mathbf{X} = \ell, \, \boldsymbol{\sigma} \cdot \mathbf{e} = s \big| \mathbf{X}\Big),
\end{aligned} \tag{3.6}
$$

where $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$ is a sequence of i.i.d. Bernoulli random variables with probability of $\sigma_i = \pm 1$ equal to $1/2$.

We would like to estimate the asymptotics of the integral in (3.6), which is equivalent to proving a local limit theorem for the conditional probability in (3.6). In general, to compute – via local limit theorems – the probability that some random variable A takes the value a, it must be the case that the corresponding expectation of A is near a. Thus the analogue of the representation (3.6) for the unconstrained problem was well adapted to the analysis of perfect partitions. Indeed, in that case, we wanted to estimate $\mathbb{P}_{1/2}(|\boldsymbol{\sigma} \cdot \mathbf{X}| \le 1 | \mathbf{X})$, and we had $\mathbb{E}_{1/2}(\boldsymbol{\sigma} \cdot \mathbf{X} | \mathbf{X}) = 0$. However, in the constrained case, this strategy cannot be expected to work for $b > 0$, since $s = bn$ is very far from the expectation of $\boldsymbol{\sigma} \cdot \mathbf{e}$, namely $\mathbb{E}_{1/2}(\boldsymbol{\sigma} \cdot \mathbf{e} | \mathbf{X}) = 0$.

To resolve this substantial difficulty, we introduce a *two-parameter* family of distributions for σ_j as follows: Given $\xi, \eta \in \mathbb{R}$, let $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$ be a sequence of random variables such that, conditioned on $\mathbf{X}$, $\sigma_1, \ldots, \sigma_n$ are mutually independent, and

$$
\mathbb{P}(\sigma_j = 1 | \mathbf{X}) = P(\xi X_j + \eta), \qquad \mathbb{P}(\sigma_j = -1 | \mathbf{X}) = 1 - P(\xi X_j + \eta), \tag{3.7}
$$

where

$$
P(u) := \frac{e^{-u}}{2 \cosh u}. \tag{3.8}
$$

In terms of these random variables, $Z_n(\ell, s)$ can be rewritten as

$$
\begin{aligned}
Z_n(\ell, s) &= e^{n L_n(\xi, \eta; \mathbf{X})} \, \mathbb{P}\big(\boldsymbol{\sigma} \cdot \mathbf{X} = \ell, \, \boldsymbol{\sigma} \cdot \mathbf{e} = s | \mathbf{X}\big) \\
&= e^{n L_n(\xi, \eta; \mathbf{X})} \frac{1}{\pi^2} \iint_{x,y \in (-\pi/2, \pi/2]} e^{-i(\ell x + s y)} \mathbb{E}\big(\exp(i(x \boldsymbol{\sigma} \cdot \mathbf{X} + y \boldsymbol{\sigma} \cdot \mathbf{e})) | \mathbf{X}\big) \, dx dy,
\end{aligned} \tag{3.9}
$$

where

$$
L_n(\xi, \eta; \mathbf{X}) := \frac{\ell \xi}{n} + \frac{s \eta}{n} + \frac{1}{n} \sum_{j=1}^{n} \log(2 \cosh(\xi X_j + \eta)). \tag{3.10}
$$

Indeed, fix $\xi, \eta \in \mathbb{R}$. Then $Z_n(\ell, s)$ can be rewritten as

$$
\begin{aligned}
Z_n(\ell, s) &= \sum_{\boldsymbol{\tau} \in \{-1,+1\}^n} \mathbb{I}(\boldsymbol{\tau} \cdot \mathbf{X} = \ell, \, \boldsymbol{\tau} \cdot \mathbf{e} = s) \\
&= \sum_{\substack{\boldsymbol{\tau}:\boldsymbol{\tau}\cdot\mathbf{X}=\ell,\\ \boldsymbol{\tau}\cdot\mathbf{e}=s}} e^{\xi(\ell - \boldsymbol{\tau}\cdot\mathbf{X}) + \eta(s - \boldsymbol{\tau}\cdot\mathbf{e})} = e^{\xi\ell + \eta s} \sum_{\substack{\boldsymbol{\tau}:\boldsymbol{\tau}\cdot\mathbf{X}=\ell,\\ \boldsymbol{\tau}\cdot\mathbf{e}=s}} \prod_{j=1}^n e^{-(\xi X_j + \eta)\tau_j} \\
&= \left[e^{\xi\ell + \eta s} \prod_{j=1}^n (2\cosh(\xi X_j + \eta)) \right] \sum_{\substack{\boldsymbol{\tau}:\boldsymbol{\tau}\cdot\mathbf{X}=\ell,\\ \boldsymbol{\tau}\cdot\mathbf{e}=s}} \prod_{j'=1}^n P\Big((\xi X_{j'} + \eta)\tau_{j'}\Big) \qquad (3.11) \\
&= e^{nL_n(\xi,\eta;\mathbf{X})} \sum_{\substack{\boldsymbol{\tau}:\boldsymbol{\tau}\cdot\mathbf{X}=\ell,\\ \boldsymbol{\tau}\cdot\mathbf{e}=s}} \prod_{j=1}^n \mathbb{P}(\sigma_j = \tau_j | \mathbf{X}) \\
&= e^{nL_n(\xi,\eta;\mathbf{X})} \mathbb{P}(\boldsymbol{\sigma} \cdot \mathbf{X} = \ell, \boldsymbol{\sigma} \cdot \mathbf{e} = s | \mathbf{X}),
\end{aligned}
$$

since $P(-u) = 1 - P(u)$, see equation (3.8).

3.3 Saddle Point Equations and their Solution

Given ξ, η, we now face the problem of determining an asymptotic value of the *local* probability in (3.9). This will obviously be easier if the chosen parameters ℓ and s are among the more likely values of $\boldsymbol{\sigma} \cdot \mathbf{X}$ and $\boldsymbol{\sigma} \cdot \mathbf{e}$, respectively. A natural choice is to take ℓ and s equal to their expected values, that is

$$
\mathbb{E}(\sigma \cdot \mathbf{X} | \mathbf{X}) = \ell, \quad \mathbb{E}(\boldsymbol{\sigma} \cdot \mathbf{e} | \mathbf{X}) = s, \tag{3.12}
$$

or explicitly (using (3.8), (3.7))

$$
\begin{aligned}
\sum_{j=1}^n X_j \tanh(\xi X_j + \eta) &= -\ell, \\
\sum_{j=1}^n \tanh(\xi X_j + \eta) &= -s.
\end{aligned} \tag{3.13}
$$

Note that the equations (3.13) also arise naturally in an apparently different approach to estimate the integral in (3.6), the "method of steepest descent." In our context, this corresponds to a complex shift of the integration path, i.e., to changing the path of integration for x to the complex path from $-\pi/2 + i\xi$ to $-\pi/2 + i\xi$, and the path of integration for y to the complex path from $-\pi/2 + i\eta$ to $-\pi/2 + i\eta$, where ξ and η are determined by a suitable saddle point condition. For general ξ and η, this leads to (3.9), while the saddle point conditions turn our to be nothing but (3.13). In fact, this is how we first obtained (3.9) and (3.13).

Both approaches raise the question of uniqueness and existence of a solution to the saddle point equations(3.13). In this context, it is useful to realize that the conditions (3.13) can be rewritten as

$$
\frac{\partial L_n(\xi, \eta; \mathbf{X})}{\partial \xi} = 0, \quad \frac{\partial L_n(\xi, \eta; \mathbf{X})}{\partial \eta} = 0. \tag{3.14}
$$

Therefore any solution (ξ, η) is a stationary point of the strictly convex function $L_n(\xi, \eta; \mathbf{X})$. If a solution exists, it is therefore the unique *minimum* point of L_n. Using the first equation in (3.9), we see also that (ξ, η) *maximizes* the local probability $\mathbb{P}(\boldsymbol{\sigma} \cdot \mathbf{X} = \ell, \boldsymbol{\sigma} \cdot e = s | \mathbf{X})$, and hence makes it easier to do an asymptotic analysis. This observation justifies our choice of ξ, η.

In the actual proof, we modify this approach a little since the solution $\xi = \xi(\mathbf{X})$, $\eta = \eta(\mathbf{X})$ does not lend itself to a rigorous analysis of $\mathbb{P}(\boldsymbol{\sigma} \cdot \mathbf{X} = \ell, \boldsymbol{\sigma} \cdot e = s | \mathbf{X})$. Instead, we will resort to "suboptimal" $\xi = \zeta/M$, η, where ζ, η are nonrandom constants, and (ζ, η) is a solution of nonrandom equations, obtained by replacing the (scaled) sums in (3.13) with their weak-law limits, see equations (3.18) below. This way we will be able to establish an explicit asymptotic formula for $Z_n(\ell, s)$, which will ultimately lead us to determine the phase boundaries.

In Section 4, we will show that these deterministic equations have a (unique) solution $\zeta = \zeta(b)$, $\eta = \eta(b)$ iff $b < b_c = \sqrt{2} - 1$, the same b_c that determines the sorted phase. In other words, the threshold b_c plays two seemingly unrelated roles: both as a threshold value of b for solvability of the deterministic saddle point equations (3.18), and as a threshold for the sorted partition being optimal. On an informal level, the reason for the coincidence is as follows: For simplicity, suppose that the weights X_j are all distinct, so that $X_1 < \cdots < X_n$ after reordering. As b approaches the point where the solutions (ζ, η) to the saddle point equations (3.18) stop existing, these solutions actually diverge, one tending to $+\infty$ and the other to $-\infty$. According to equations (3.7) and (3.8), this in turn means that $\mathbb{P}(\sigma_j = 1 | \mathbf{X})$ tends to zero or one, depending on whether $j < j_o$ or $j > j_o$, where $j_o = |\{j : \sigma_j = -1\}|$ is the cutoff of the sorted partition for $\mathbf{X}$ with bias $s = nb_c$. Hence, the product measure $\mathbb{P}(\boldsymbol{\sigma} \cdot \mathbf{X} = \ell, \boldsymbol{\sigma} \cdot \mathbf{e} = s | \mathbf{X})$ tends to a delta function on the (unique) sorted partition which is the solution to the number partitioning problem for $\mathbf{X}$ at $b = b_c$. See Subsection 7.2 for details.

3.4 Asymptotic behavior of $Z_n(\ell, s)$.

Proceeding with our heuristic discussion, let us simply assume that the equations (3.13) do have a solution $\xi = \xi(\mathbf{X}), \eta = \eta(\mathbf{X})$. Then we may hope that, with this choice of the parameters $\xi = \xi(\mathbf{X}), \eta = \eta(\mathbf{X})$, we have a reasonable chance to prove—at least for the likely values of $\mathbf{X}$—a local limit theorem for the *conditional* probability in (3.9), namely that w.h.p.

$$\mathbb{P}(\boldsymbol{\sigma} \cdot \mathbf{X} = \ell, \boldsymbol{\sigma} \cdot \mathbf{e} = s | \mathbf{X}) \sim \frac{2}{\pi\sqrt{\det Q}}, \tag{3.15}$$

where

$$Q = \begin{pmatrix} \mathrm{Var}(\boldsymbol{\sigma} \cdot X) & \mathrm{cov}(\boldsymbol{\sigma} \cdot \mathbf{X}, \boldsymbol{\sigma} \cdot \mathbf{e}) \\ \mathrm{cov}(\boldsymbol{\sigma} \cdot \mathbf{X}, \boldsymbol{\sigma} \cdot \mathbf{e}) & \mathrm{Var}(\boldsymbol{\sigma} \cdot \mathbf{e}) \end{pmatrix}. \tag{3.16}$$

Here the (co)variances are conditioned on $\mathbf{X}$, so, e.g., $Q_{11} = \mathrm{Var}(\boldsymbol{\sigma} \cdot \mathbf{X} | \mathbf{X})$. If (3.15) holds then by (3.11), w.h.p.,

$$Z_n(\ell, s) \sim e^{nL_n(\xi, \eta; \mathbf{X})} \frac{2}{\pi\sqrt{\det Q}} = e^{nL_n(\xi, \eta; \mathbf{X})} \frac{2}{\pi n M \sqrt{\det R^{(n)}}}, \tag{3.17}$$

where $R^{(n)}$ is the matrix with matrix elements $R_{11}^{(n)} = \frac{1}{nM^2}\mathrm{Var}(\boldsymbol{\sigma} \cdot X)$, $R_{12}^{(n)} = R_{21}^{(n)} = \frac{1}{nM}\mathrm{cov}(\boldsymbol{\sigma} \cdot \mathbf{X}, \boldsymbol{\sigma} \cdot \mathbf{e})$ and $R_{22}^{(n)} = \frac{1}{n}\mathrm{Var}(\boldsymbol{\sigma} \cdot \mathbf{e})$.

Note that, in the limit $M \to \infty$, X_j/M are independent, uniform random variables in $[0,1]$. We therefore expect that as $M, n \to \infty$ with $\kappa = n^{-1}log_2 M$ fixed, both $\zeta(\mathbf{X}) := M\xi(\mathbf{X})$ and $\eta(\mathbf{X})$ are close, in probability, to the deterministic ζ, η, defined as the roots of the averaged version of the "saddle point equations" (3.13), namely

$$
\begin{aligned}
\int_0^1 x \tanh(\zeta x + \eta)\, dx &= -\frac{\ell}{Mn}, \\
\int_0^1 \tanh(\zeta x + \eta)\, dx &= -b, \quad b = \frac{s}{n}.
\end{aligned}
\tag{3.18}
$$

Recall that, without loss of generality, we have taken $s \geq 0$, so $b \geq 0$.

Furthermore, approximating $\xi(\mathbf{X})$ and $\eta(\mathbf{X})$ by $M\zeta$ and η, respectively and using the bound $|d\cosh u/du| \leq 1$, it is easy to see that, because of the weak law of large numbers, w.h.p.

$$
\begin{aligned}
L_n(\xi(\mathbf{X}), \eta(\mathbf{X}); \mathbf{X}) &= \frac{1}{n}\sum_{j=1}^n \log\left(e^{\ell\xi(\mathbf{X})+s\eta(\mathbf{X})}2\cosh(\xi(\mathbf{X})X_j + \eta(\mathbf{X}))\right) \\
&\sim \frac{\ell}{Mn}\zeta + b\eta + \int_0^1 \log(2\cosh(\zeta x + \eta))\, dx,
\end{aligned}
\tag{3.19}
$$

and similarly for the matrix elements of $R^{(n)}$,

$$
R_{ij}^{(n)} \sim \int_0^1 x^{2-(i+j)}(1 - \tanh^2(\zeta x + \eta))\, dx.
\tag{3.20}
$$

Putting everything together, we thus may hope to prove that for $|\ell| \leq 1$ and M growing exponentially with n, (i.e. $\log_2 M \sim \kappa n$ for some n-independent κ), we have w.h.p.

$$
\begin{aligned}
\frac{1}{n}\log Z_n(\ell, s) &\sim \int_0^1 \log(2\cosh(\zeta x + \eta))\, dx + b\eta - \kappa \\
&= \kappa_c(b) - \kappa,
\end{aligned}
\tag{3.21}
$$

suggesting that for $\kappa < \kappa_c(b)$ there are exponentially many perfect partitions, while for $\kappa > \kappa_c(b)$ there are none.

However, this informal argument is too naive. Equation (3.21) could not possibly hold for $\kappa > \kappa_c(b)$. Indeed, $Z_n(\ell, s)$ is an integer, and thus cannot be asymptotically equivalent to an exponentially small, yet positive number. This means that a rigorous proof of (3.21) must be based on the condition $\kappa < \kappa_c(b)$. But our heuristic discussion

provides no clue as to how this condition might enter the picture. Furthermore, our attempts to find such a proof are stymied by mutual dependence of the random variables $\mathbb{P}(\sigma_j = 1|\mathbf{X})$, $(1 \leq j \leq n)$, a consequence of the fact that $(\xi(\mathbf{X}), \eta(\mathbf{X}))$ depends, in an unwieldy manner, on the whole $\mathbf{X}$. This complicated dependence of $(\xi(\mathbf{X}), \eta(\mathbf{X}))$ on $\mathbf{X}$ would have made it very hard to gain an insight into the random fluctuations of the sum in (3.19), even if we had found a proof.

Fortunately, once we have informally connected $(\xi(\mathbf{X}), \eta(\mathbf{X}))$ to (ζ, η) via $\xi(\mathbf{X}) = (1 + o_p(1))\zeta/M$, $\eta(\mathbf{X}) = (1 + o_p(1))\eta$, we may try to use the *suboptimal* parameters $(\zeta/M, \eta)$ instead. The corresponding random variables $\mathbb{P}(\sigma_j = 1|\mathbf{X})$ each depend on their own X_j, and are thus mutually independent. A key technical issue is whether the suboptimal parameters are good enough to get an asymptotic formula for the corresponding probability $\mathbb{P}(\boldsymbol{\sigma} \cdot \mathbf{X}, \boldsymbol{\sigma} \cdot \mathbf{X} = s|\mathbf{X})$, given that now the random equations (3.13) may hold only approximately. Our proof below shows that they are indeed sufficient. With those parameters, we will be able to get a sharp explicit approximation for $\log Z_n(\ell, s)$, at least in the range $\kappa < \kappa_-(b)$.

We prove the existence and uniqueness of the solution to (3.18) in the next section, and then use them in Section 5.1 to derive the asymptotics of $Z_n(\ell, s)$.

4 Solution of the Deterministic Saddle Point Equations

Based on the heuristic discussion of the last section, we *define* $\boldsymbol{\sigma}$ as the random sequence $(\sigma_1, \ldots, \sigma_n)$ such that, conditioned on $\mathbf{X}$, the σ_j are independent and

$$\mathbb{P}(\sigma_j = 1|\mathbf{X}) = P\left(\zeta\frac{X_j}{M} + \eta\right), \quad \mathbb{P}(\sigma_j = -1|\mathbf{X}) = 1 - P\left(\zeta\frac{X_j}{M} + \eta\right), \quad (4.1)$$

with $P(u)$ defined in (3.8), and (ζ, η) is a solution of the equations

$$
\begin{aligned}
\int_0^1 x \tanh(\zeta x + \eta)\, dx &= 0, \\
\int_0^1 \tanh(\zeta x + \eta)\, dx &= -b.
\end{aligned}
\tag{4.2}
$$

These are the equations (3.18), except that the right hand side of the first equation is set 0, since our focus is on $\ell \ll Mn$.

However, does such a solution exist? A key observation here is that the equations (4.2) mean that (ζ, η) is a stationary point of the function

$$L(\zeta, \eta) := b\eta + \int_0^1 \log(2\cosh(\zeta x + \eta))\, dx \tag{4.3}$$

which is the r.h.s. in (3.19), without the term $\zeta\ell/(Mn)$, i.e., the (weak) limit of the function $L_n(\xi(\mathbf{X}), \eta(\mathbf{X}); \mathbf{X})$ defined in (3.10). Since $L(\zeta, \eta)$ is strictly convex, it may have at most one stationary point, and this point is a global minimum. So a solution to (4.2) exists iff $L(\zeta, \eta)$ attains its global infimum.

Theorem 4.1 *Let $0 \leq b < b_c := \sqrt{2} - 1$. Then:*
(1) $L(\zeta, \eta)$ attains its infimum, hence there exists a unique solution $(\zeta, \eta) = (\zeta(b), \eta(b))$ of the equations (4.2).
(2) The minimizers $\zeta(b), \eta(b)$ are continuous functions, with $\zeta(b) > 0$, $\eta(b) < 0$ and $\zeta(b) + \eta(b) > 0$ whenever $0 < b < b_c$.
(3) $\hat{L}(b) := L(\zeta(b), \eta(b))$, the minimum of $L(\zeta, \eta)$, decreases with b. For $b \in (0, b_c)$, its derivative is $d\hat{L}(b)/db = \eta(b)$.
(4) $\lim_{b \to b_c} \zeta(b) = \infty$, $\lim_{b \to b_c} \eta(b) = -\infty$,

$$\lim_{b \to b_c} \frac{-\eta(b)}{\zeta(b)} = \frac{1}{\sqrt{2}}, \tag{4.4}$$

and $\lim_{b \to b_c} \hat{L}(b) = 0$.
(5) $\lim_{b \to 0} \zeta(b) = 0$, $\lim_{b \to 0} \eta(b) = 0$, and $\lim_{b \to 0} \hat{L}(b) = \log 2$.
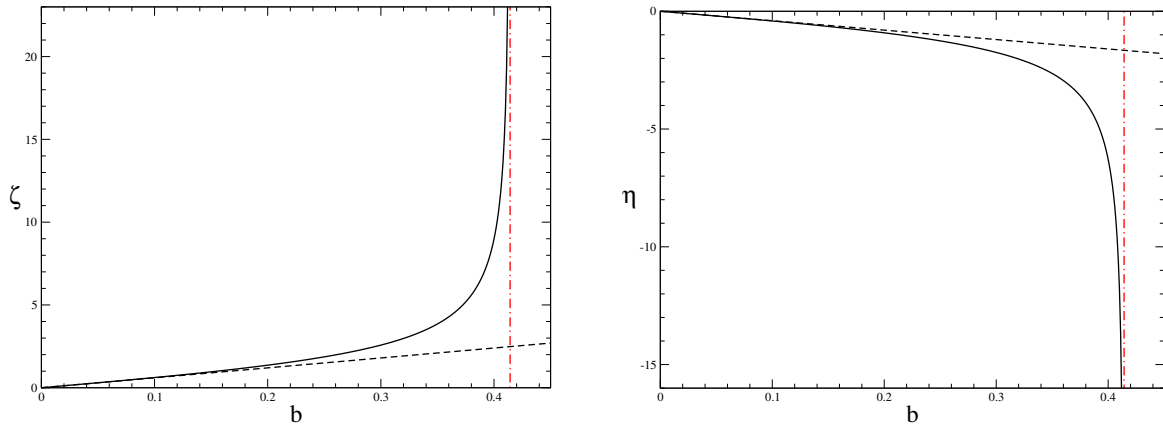

Figure 3: Numerical solution of eq. 4.2. The dashed lines are the linearized solutions $\zeta(b) = 6b + O(b^2)$ and $\eta(b) = -4b + O(b^2)$.

Proof of Theorem 4.1.
(1) Since $\log(2 \cosh u) \geq |u|$, we have

$$L(\zeta, \eta) \geq \mathcal{L}(\zeta, \eta), \tag{4.5}$$

where

$$\mathcal{L}(\zeta, \eta) = b\eta + \int_0^1 |\zeta x + \eta| \, dx. \tag{4.6}$$

It thus suffices to prove that

$$\liminf_{\|(\zeta,\eta)\|_\infty \to \infty} \mathcal{L}(\zeta,\eta) = \infty, \tag{4.7}$$

where $\|(\zeta,\eta)\|_\infty = \max\{|\zeta|, |\eta|\}$.

Since $\mathcal{L}$ is homogeneous, degree 1, and continuous, it suffices to prove that $\mathcal{L}(\zeta,\eta) > 0$ for all (ζ,η) such that $\|(\zeta,\eta)\|_\infty = 1$. To this end, we will first show that

$$\min_{\|(\zeta,\eta)\|_\infty = 1} \mathcal{L}(\zeta,\eta) = \min_{-1 \le \eta \le 0} \mathcal{L}(1,\eta). \tag{4.8}$$

Since $\mathcal{L}(\zeta,\eta) \ge \mathcal{L}(|\zeta|, -|\eta|)$, it suffices to consider $\eta \le 0$ and $\zeta \ge 0$. But $\eta \le 0$, $\zeta \ge 0$ and $\|(\zeta,\eta)\|_\infty = 1$ implies that either $\zeta = 1$ and $-1 \le \eta \le 0$ or $\eta = -1$ and $0 \le \zeta \le 1$. We thus have to show $\mathcal{L}(\zeta,\eta)$ is bounded below by the right hand side of (4.8) if $\eta = -1$ and $0 \le \zeta \le 1$. Indeed, under these conditions, $|\zeta x + \eta| = 1 - \zeta x \ge 1 - x = |x + \eta|$, implying that $\mathcal{L}(\zeta,\eta) \ge \mathcal{L}(1,-1)$, which is clearly bounded below by the right hand side of (4.8).

It remains to bound $\mathcal{L}(1,\eta)$ from below, for $-1 \le \eta \le 0$. Setting $\tilde{x} = -\eta$, we have

$$\mathcal{L}(1,\eta) = -b\tilde{x} + \int_0^1 |x - \tilde{x}|\, dx = \frac{1}{2} + \tilde{x}^2 - \tilde{x}(1 + b). \tag{4.9}$$

At $\tilde{x} = x_0 := (1 + b)/2$ the right hand side attains its minimum value $\frac{1}{2}[1 - (1+b)^2/2]$, which is bounded away form zero as $b < b_c = \sqrt{2} - 1$. Thus we have proved that for $b \in [0, \sqrt{2} - 1)$, and all ζ, η,

$$\mathcal{L}(\zeta,\eta) \ge c^*(b) \max\{|\zeta|, |\eta|\}, \tag{4.10}$$

where $c^*(b) = \frac{1}{2}[1 - (1+b)^2/2] > 0$. Therefore $\mathcal{L}(\zeta,\eta)$ attains its infimum, hence so does $L(\zeta,\eta)$. We conclude that (4.2) has a unique solution solution $(\zeta,\eta) = (\zeta(b),\eta(b))$.

(2) Suppose $\eta(b) \ge 0$. Using (4.2), and $y \tanh y > 0$ if $y \neq 0$, one can show easily that $\eta(b) > 0$ and $\zeta(b) < 0$. But such a point $(\zeta(b),\eta(b))$ cannot be a minimum point of $L(\zeta,\eta)$, since $L(\zeta(b),\eta(b)) > L(-\zeta(b),-\eta(b))$, due to the symmetry of $\cosh y$, and the fact that $b\eta(b) > -b\eta(b)$. Therefore $\eta = \eta(b) < 0$, and

$$\zeta + \eta = (\zeta x + \eta)|_{x=1} > 0. \tag{4.11}$$

Continuity will be proved along with (3), where we actually prove continuous differentiability.

(3) The equations (4.2) are an explicit form of $L_\zeta = 0$, $L_\eta = 0$. It is easy to show that the Jacobian matrix $\begin{pmatrix} L_{\zeta\zeta} & L_{\eta\zeta} \\ L_{\zeta\eta} & L_{\eta\eta} \end{pmatrix}$ is nonsingular. Therefore $\zeta(b)$, $\eta(b)$ are continuously differentiable, and consequently

$$\hat{L}_b(b) = \left[L_b(b,\eta,\zeta) + L_\zeta(b,\zeta,\eta)\zeta_b(b) + L_\eta(b,\zeta,\eta)\eta_b(b) \right]_{\zeta=\zeta(b),\eta=\eta(b)} \tag{4.12}$$

$$= L_b(b,\eta(b),\zeta(b)) = \eta(b) < 0. \tag{4.13}$$

Therefore $\hat{L}(b)$ decreases with b.

(4) Pick $\zeta > 0$, $x_0 \in (0,1)$, and set $\eta = -x_0\zeta$. Breaking the integral (4.3) into two parts, $x \in [0, x_0]$ and $x \in [x_0, 1]$, and using

$$\log(e^u + e^{-u}) = u + \log(1 + e^{-2u}), \tag{4.14}$$

we get:

$$
\begin{aligned}
L(\zeta, \eta) = &\frac{\zeta}{2}\left(2x_0^2 - 2x_0(1+b) + 1\right) \\
&+ \frac{1}{2\zeta} \int_0^{2\zeta x_0} \log(1 + e^{-u})\,du + \frac{1}{2\zeta} \int_0^{2\zeta(1-x_0)} \log(1 + e^{-u})\,du.
\end{aligned} \tag{4.15}
$$

At $x_0 = (1+b)/2$ the quadratic polynomial attains its minimum value $1 - (1+b)^2/2$, which is positive since $b < b_c$. With this x_0, choose $\zeta = \left(1 - \frac{(1+b)^2}{2}\right)^{-1/2}$. Then $\zeta \to \infty$ as $b \to b_c$, so that the integral terms add up to $O(\zeta^{-1})$, which is also the order of the first term. Hence $L(\zeta, \eta) \to 0$, and therefore $\lim_{b \to b_c} \hat{L}(b) \leq 0$. To see that $\lim_{b \to b_c} \hat{L}(b) = 0$, we just note that $\hat{L}(b) = \min_{\eta,\zeta} L(\zeta, \eta) \geq \min_{\eta,\zeta} \mathcal{L}(\zeta, \eta) = 0$.

To complete the proof, in (4.15) set $\zeta = \zeta(b)$ and $x_0 = -\eta(b)/\zeta(b)$, so that $\eta = \eta(b)$. (Note that $x_0 \in (0,1)$ as $\zeta(b) + \eta(b) > 0$.) Since the quadratic polynomial in (4.15) is non-negative if $b \leq b_c$, and $\max(x_0, 1 - x_0) \geq 1/2$, we have that

$$\lim_{b \to b_c} \hat{L}(b) \geq \liminf_{b \to b_c} \frac{1}{2\zeta(b)} \int_0^{\zeta(b)} \log(1 + e^{-u})\,du > 0, \tag{4.16}$$

if $\liminf_{b \to b_c} \zeta(b) < \infty$. So, since $\lim_{b \to b_c} \hat{L}(b) = 0$, we conclude that $\zeta(b) \to \infty$ as $b \to b_c$. But then, using (4.15) again,

$$0 = \lim_{b \to b_c} \frac{\zeta(b)}{2}\left[2x_0^2 - 2x_0(1+b) + 1\right] \implies \lim_{b \to b_c}\left[2x_0^2 - 2x_0(1+b) + 1\right] = 0 \tag{4.17}$$

$$\implies \lim_{b \to b_c} x_0 = \frac{1}{\sqrt{2}}, \tag{4.18}$$

the only root of $2x^2 - 2x\sqrt{2} + 1 = 0$.

(5) This statement is immediate from the fact that $\zeta(b)$, $\eta(b)$ are continuously differentiable on $(0, b_c)$ and the observation that for $b = 0$, $L(\zeta, \eta)$ attains its minimum value of $\log 2$ at $(\zeta, \eta) = (0, 0)$. ∎

Remark 4.1 *Theorem 4.1 can easily be generalized to the case of non-uniform i.i.d. random variables X_j provided X_j/M has a limiting density $\mu(x)$, $x \geq 0$. In that case, b_c is replaced by $b_c = b_c(\mu)$, as defined in Remark 3.1, i.e.*

$$b_c = 2\int_0^{x_0} \mu(x)\,dx - 1, \qquad \int_0^{x_0} x\mu(x)\,dx = \int_{x_0}^{\infty} x\mu(x)\,dx. \tag{4.19}$$

The counterpart of $L(\zeta, \eta)$ is obviously

$$L(\zeta, \eta) = b\eta + \int_0^\infty \log(2 \cosh(\zeta x + \eta)) \, \mu(x) \, dx. \tag{4.20}$$

Remarkably, this extension requires only obvious changes in the above proof. For instance, below is the proof of the item (1). Note that the surprising dual role of b_c, namely as both the point at which the saddle point equation stops having a solution and as the threshold for optimality of sorted partitions, still holds for $b_c(\mu)$. In fact, if correctly interpreted, this dual role persists deterministically *for any fixed instance $\{X_1, \ldots, X_n\}$, see Subsection 7.2.*

Proof of (1) for an arbitrary distribution μ: First, we write

$$L(\zeta, \eta) \geq \mathcal{L}(\zeta, \eta) = b\eta + \int_0^\infty |\zeta x + \eta| \, \mu(x) \, dx. \tag{4.21}$$

Second, we bound

$$\min_{\|(\zeta, \eta)\|_\infty = 1} \mathcal{L}(\zeta, \eta) \geq \min\left(\min_{-1 \leq \eta \leq 0} \mathcal{L}(1, \eta), \min_{0 \leq \zeta \leq 1} \mathcal{L}(\zeta, -1) \right). \tag{4.22}$$

Furthermore,

$$\mathcal{L}(\zeta, -1) = -b + M(\zeta^{-1}),,$$
$$M(y) := \int_0^y (1 - xy^{-1}) \mu(x) \, dx + \int_y^\infty (xy^{-1} - 1) \mu(x) \, dx.$$

Using 4.19, we see that

$$\min_{y \geq 0} M(y) = M(x_0) = b_c(\mu), \tag{4.24}$$

hence

$$\mathcal{L}(\zeta, -1) \geq -b + b_c(\mu) > 0, \tag{4.25}$$

for $b < b_c(\mu)$. Likewise, if $\eta < 0$, we set $\eta = -\tilde{x}$, and easily obtain

$$\mathcal{L}(1, \eta) = \tilde{x}\big(-b + M(\tilde{x})\big) \geq \tilde{x}(-b + b_c(\mu)) > 0, \tag{4.26}$$

for $b < b_c(\mu)$. ∎

5 The Perfect Phase

5.1 Asymptotic Enumeration of Partitions by Discrepancy and Bias

Now that we have proved existence of the solution (ζ, η) of (4.2) for $b < \sqrt{2} - 1$, we are justified in using the marginals (4.1). It is critically important that each $\mathbb{P}(\sigma_j = \pm 1 | \mathbf{X})$

depends only on its own X_j, so that they are mutually independent. This would not have been the case if we had used $(\xi(\mathbf{X}), \eta(\mathbf{X}))$, the solution of the random equations (3.13).

The corresponding version of (3.9) is

$$Z_n(\ell, s) = \exp\left(\zeta \frac{\ell}{M} + s\eta + \sum_{j=1}^{n} \log\left(2\cosh\left(\zeta \frac{X_j}{M} + \eta\right)\right)\right) I_n(\mathbf{X}). \tag{5.1}$$

Here $I_n(\mathbf{X})$ is the random integral

$$I_n(\mathbf{X}) = \frac{1}{\pi^2} \iint_{x,y \in (-\pi/2, \pi/2]} e^{-i(\ell x + sy)} f(x, y; \mathbf{X}) \, dx dy, \tag{5.2}$$

where

$$f(x, y; \mathbf{X}) := \mathbb{E}\left(\exp(i(x\boldsymbol{\sigma} \cdot \mathbf{X} + y\boldsymbol{\sigma} \cdot \mathbf{e}))|\mathbf{X}\right)$$
$$= \prod_{j=1}^{n}\left[p(X_j/M)e^{i\left(xX_j+y\right)} + q(X_j/M)e^{-i\left(xX_j+y\right)}\right], \tag{5.3}$$

with the shorthands $p(u)$ and $q(u)$ for $P(\zeta u + \eta)$ and $1 - P(\zeta u + \eta)$, where (ζ, η) is the solution of (4.2), and $P(\cdot)$ is given by (3.8). Now that the summands in (5.1) are simply i.i.d. random variables, the core of the problem is to determine the asymptotically likely behavior of $I_n(\mathbf{X})$.

Theorem 5.1 *Suppose that* $\limsup |s|/n < b_c$, $0 < \liminf \kappa$, $\limsup(\kappa - \kappa_-(b)) < 0$, $\ell = o(Mn^{1/2})$ *and* $n = o(M^2)$. *Then there is a constant* $\delta > 0$ *such that, with probability* $1 - O(e^{-\delta \log^2 n})$,

$$I_n(\mathbf{X}) = (1 + o(1)) \frac{1}{\pi Mn\sqrt{detR}} \exp\left(-\frac{1}{4}\boldsymbol{\tau}_n R^{-1} \boldsymbol{\tau}_n'\right). \tag{5.4}$$

Here

$$R = \begin{pmatrix} 2\mathbb{E}(U^2 p(U)q(U)) & 2\mathbb{E}(Up(U)q(U)) \\ 2\mathbb{E}(Up(U)q(U)) & 2\mathbb{E}(p(U)q(U)) \end{pmatrix}, \tag{5.5}$$

and $\boldsymbol{\tau}_n$ *is a two-dimensional random vector which converges in probability to a Gaussian vector* $\boldsymbol{\tau}$, *with mean zero and covariance matrix*

$$K = \begin{pmatrix} Var(U(p(U) - q(U))) & cov(U(p(U) - q(U)), p(U) - q(U)) \\ cov(U(p(U) - q(U)), p(U) - q(U)) & Var(p(U) - q(U)) \end{pmatrix}, \tag{5.6}$$

where U *is uniformly distributed on* $[0, 1]$. *Furthermore,* $\|\boldsymbol{\tau}_n\| \leq \log n$ *with probability at least* $1 - O(e^{-\delta log^2 n})$.

Consequently, with probability $1 - O(e^{-\delta \log^2 n})$, $Z_n(\ell, s) \geq 1$ *and*

$$\log Z_n(\ell, s) = n[L(\zeta, \eta) - \kappa \log 2] + n^{1/2} S_n + o(n^{1/2}), \tag{5.7}$$

where

$$S_n = \frac{1}{n^{1/2}} \sum_{j=1}^{n} \left(\log\left(2\cosh\left(\zeta \frac{X_j}{M} + \eta\right)\right) - \mathbb{E}\left[\log\left(2\cosh\left(\zeta \frac{X_j}{M} + \eta\right)\right)\right]\right) \tag{5.8}$$

is asymptotically Gaussian with zero mean and variance $\sigma^2 = Var(\log(2\cosh(\zeta U + \eta)))$.

Remark 5.1 *It is a consequence of Theorem 4.1 and Theorem 5.1 that for all $b \in [0, b_c)$,*

$$\kappa_-(b) \leq \kappa_c(b), \tag{5.9}$$

with

$$\kappa_-(0) = \kappa_c(0) = 1 \quad and \quad \kappa_-(b_c) = \kappa_c(b_c) = 0. \tag{5.10}$$

Indeed, let us assume that $\liminf(\kappa_-(b) - \kappa) > 0$. By Theorem 5.1, we then have that $n^{-1} \log Z_n(\ell, s) - [L(\zeta, \eta) - \kappa \log 2] \to 0$ in probability. In particular, since w.h.p. $Z_n(\ell, s) \geq 1$, we have $\liminf(L(\zeta, \eta) - \kappa \log 2) = \liminf(\kappa_c(b) - \kappa) \log 2 \geq 0$. So the condition $\liminf(\kappa_-(b) - \kappa) > 0$ implies that $\liminf(\kappa_c(b) - \kappa) \geq 0$, which proves (5.9). Since $\zeta(0) = \eta(0) = 0$, it follows from the definitions (1.3) – (1.5) that $\kappa_-(0) = \kappa_c(0) = 1$. Finally, by Theorem 4.1, we have $\hat{L}(b_c-) = 0$, or $\kappa_c(b_c-) = 1$. Numerical computations indicate that $\kappa_-(b) < \kappa_c(b)$ for $0 < b < b_c$, but the graphs of two functions remain surprisingly close to each other. Our limited attempts to prove this strict inequality have not succeeded.

Proof of Theorem 5.1: Pick a large, but fixed, $B > 0$. Split the integration into two parts, $|x| \leq B/M$ and $|x| > B/M$, and denote the corresponding integral $I_{n1}(\mathbf{X})$ and $I_{n2}(\mathbf{X})$, respectively. Consider $I_{n1}(\mathbf{X})$ first. Begin with

$$\left| p(X_j/M)e^{i(xX_j+y)} + q(X_j/M)e^{-i(xX_j+y)} \right|^2$$
$$= 1 - 2p_j q_j(1 - \cos(2(xX_j + y))) \tag{5.11}$$
$$\leq \exp\left(-2p_j q_j(1 - \cos(2(xX_j + y)))\right),$$

where we have introduced the abbreviations $p_j = p(X_j/M)$ and $q_j = q(X_j/M)$. Let

$$\mathcal{S}_n = \{j : X_j/M \leq \pi/(3B)\}. \tag{5.12}$$

Clearly, $j \in \mathcal{S}_n$ implies

$$2|xX_j + y| \leq 2\left(\frac{B}{M}X_j + \frac{\pi}{2}\right) \leq \frac{5\pi}{3} < 2\pi. \tag{5.13}$$

Now, there exist a constant $c_1 > 0$ such that

$$1 - \cos\alpha \geq c_1\alpha^2, \quad \alpha \in [-5\pi/3, 5\pi/3]. \tag{5.14}$$

Since

$$2p_j q_j = \frac{1}{2\cosh^2(\zeta X_j/M + \eta)} \geq \frac{1}{\max\{2\cosh^2(\eta), \, 2\cosh^2(\zeta + \eta)\}}, \tag{5.15}$$

we thus have shown that there exist a $c_2 > 0$ such that

$$|f(x, y; \mathbf{X})| \leq \exp\left(-c_2 \sum_{j \in \mathcal{S}_n} (xX_j + y)^2\right)$$
$$= \exp\left(-c_2(x^2 M_2 + 2xy M_1 + y^2 M_0)\right), \tag{5.16}$$

where

$$M_k = M_k(B) = \sum_{j \in \mathcal{S}_n} X_j^{(k)} = \sum_{j=1}^{n} X_j^{(k)}(B), \quad X_j^{(k)}(B) := X_j^k \mathbb{I}_{\{X_j/M \le \pi/(3B)\}}. \tag{5.17}$$

Since $X_j^{(k)}(B)$ are independent with $X_j^{(k)}(B)/\mathbb{E}[X_j^{(k)}(B)] = O(B)$, the event

$$A_n = \{M_k \in [0.99n\mathbb{E}(X^{(k)}(B)), \ 1.01n\mathbb{E}(X^{(k)}(B))], \ k = 0, 1, 2\} \tag{5.18}$$

has probability $1 - O(e^{-\delta_1 n})$ for some $\delta_1 > 0$, by, e.g., the Azuma-Hoeffding inequality.

We continue our computation on the event A_n. It is easy to see that

$$x^2 M_2 + 2xy M_1 + y^2 M_0 \ge c_3 n \big[(Mx)^2 + y^2\big], \quad c_3 > 0. \tag{5.19}$$

Set $r_n = n^{-1/2} \log n$. From (5.16) and (5.19), it follows that, for $c_4 = c_2 c_3$,

$$\iint_{\substack{\|(Mx,y)\| \ge r_n \\ |x| \le B/M}} |f(x, y; \mathbf{X})| \, dx dy \le \frac{1}{Mn} \left(\iint_{\|\mathbf{z}\| \ge \log n} e^{-c_4 \|\mathbf{z}\|^2} \, dz_1 dz_2 \right) = O\left((Mn)^{-1} e^{-c_4 \log^2 n}\right). \tag{5.20}$$

For $\|(Mx, y)\| \le r_n$, we expand and exponentiate:

$$p_j e^{i(xX_j+y)} + q_j e^{-i(xX_j+y)} =$$

$$= 1 + i(xX_j + y)(p_j - q_j) - \frac{1}{2}(xX_j + y)^2 + O(|xX_j|^3 + |y|^3)$$

$$= \exp\Big(i(xX_j + y)(p_j - q_j) - \frac{1}{2}(xX_j + y)^2$$

$$\qquad + \frac{1}{2}(xX_j + y)^2(p_j - q_j)^2 + O(|xX_j|^3 + |y|^3)\Big) \tag{5.21}$$

$$= \exp\Big(i(xX_j + y)(p_j - q_j)$$

$$\qquad - 2p_j q_j (x^2 X_j^2 + 2X_j xy + y^2) + O(|xX_j|^3 + |y|^3)\Big).$$

Therefore,

$$e^{-i(\ell x + sy)} f(x, y; \mathbf{X}) = e^{i(Mx)(T_{n1} - \ell/M) + iy(T_{n2} - s)} \times \exp(-(Mx, y)Q(Mx, y)' + O(nM^3|x|^3 + n|y|^3)), \tag{5.22}$$

where $(Mx, y)'$ denotes the transpose of (Mx, y), and

$$T_{n1} = \sum_j (X_j/M)(p_j - q_j),$$

$$T_{n2} = \sum_j (p_j - q_j), \tag{5.23}$$

$$Q_{11} = \sum_j (X_j/M)^2 2 p_j q_j,$$

$$Q_{12} = \sum_j (X_j/M) 2 p_j q_j \tag{5.24}$$

$$Q_{22} = \sum_j 2 p_j q_j.$$

Here T_{n1}, T_{n2} are sums of i.i.d. random variables, and it is easy to show that the random vector

$$\boldsymbol{\tau}_n = (\tau_{n1}, \tau_{n2}) := n^{-1/2}(T_{n1} - \mathbb{E}(T_{n1}), \, T_{n2} - \mathbb{E}(T_{n2})) \tag{5.25}$$

is asymptotically Gaussian, with zero means, and the covariance matrix $\{K_M(i,j)\}$, with

$$\begin{aligned}
K_M(1,1) &= \mathrm{Var}(U_M(p(U_M) - q(U_M))), \\
K_M(1,2) &= \mathrm{cov}(U_M(p(U_M) - q(U_M)), p(U_M) - q(U_M)), \\
K_M(2,2) &= \mathrm{Var}(p(U_M) - q(U_M)),
\end{aligned} \tag{5.26}$$

and U_M distributed uniformly on $\{1/M, \ldots, M/M\}$. Consequently

$$K_M = K + O(M^{-1}), \tag{5.27}$$

where K is defined like K_M, with U_M replaced by the $[0,1]$-uniform U, which is the matrix K defined in (5.6). We can use K as the limiting covariance matrix for $\boldsymbol{\tau}_n$. Also, again by Azuma-Hoeffding, for any $c > 0$,

$$\|\boldsymbol{\tau}_n\| \leq c \log n \tag{5.28}$$

with probability $1 - O(e^{-\delta_2 \log^2 n})$ for some $\delta_2 = \delta_2(c) > 0$. In addition,

$$\begin{aligned}
\mathbb{E}(T_{n1}) &= n\mathbb{E}\big[(X/M)(p(X/M) - q(X/M))\big] = n\mathbb{E}(U(p(U) - q(U))) + O(n/M) \\
&= O(n/M), \\
\mathbb{E}(T_{n2}) &= n\mathbb{E}\big[p(X/M) - q(X/M)\big] = n\mathbb{E}(p(U) - q(U)) + O(n/M) \\
&= s + O(n/M).
\end{aligned} \tag{5.29}$$

Using the equations (5.25) and (5.29), we obtain

$$\begin{aligned}
T_{n1} - \ell/M &= n^{1/2}\big(\tau_{n1} + O(n^{1/2}/M + |\ell|/(Mn^{1/2}))\big), \\
T_{n2} - s &= n^{1/2}\big(\tau_{n2} + O(n^{1/2}/M)\big).
\end{aligned}$$

Both remainder terms are $o(1)$ since $n^{1/2} = o(M)$ and $\ell = o(Mn^{1/2})$. Since Q_{ij} is a sum of n bounded i.i.d. random variables, $Q_{ij} = \mathbb{E}(Q_{ij}) + O(n^{1/2} \log n)$ with probability $1 - O(e^{-\delta_3 log^2 n})$ for some $\delta_3 > 0$. Approximating $\mathbb{E}(Q_{ij})$ as $\mathbb{E}(Q_{ij}) = n[R_{ij} + O(M^{-1})] = n[R_{ij} + o(n^{-1/2})]$, where

$$\begin{aligned}
R_{11} &= 2\mathbb{E}(U^2 p(U) q(U)), \\
R_{12} &= 2\mathbb{E}(U p(U) q(U)), \\
R_{22} &= 2\mathbb{E}(p(U) q(U)),
\end{aligned} \tag{5.30}$$

we get

$$Q = n(R + O(n^{-1/2} \log n)) \tag{5.31}$$

with probability $1 - O(e^{-\delta_3 \log^2 n})$.

Consequently, with probability $1 - O(e^{-\delta_3 \log^2 n})$,

$$\iint\limits_{\|(Mx,y)\| \le r_n} e^{-i(\ell x + sy)} f(x, y; \mathbf{X}) \, dxdy$$

$$= \iint\limits_{\|(Mx,y)\| \le r_n} \exp\big(i(Mn^{1/2}x)(\tau_{n1} + o(1)) + i(n^{1/2}y)(\tau_{n2} + o(1))\big)$$

$$\exp\big(-(Mx, y)Q(Mx, y)' + O(|Mx|^3 n + |y|^3 n)\big) \, dxdy$$

$$= \frac{1}{Mn}\left[\frac{\pi}{\sqrt{\det R}} \exp\left(-\frac{1}{4}\boldsymbol{\tau}_n R^{-1} \boldsymbol{\tau}_n'\right) + o(1)\right]. \tag{5.32}$$

Using (5.20) and (5.28), we see that the r.h.s. of (5.32) also gives the asymptotics of $I_{n1}(\mathbf{X})$, the integral over all (x, y) with $|x| \le B/M$.

Let us turn now to $I_{n2}(\mathbf{X})$. We want to show that for some $\delta > 0$ we have $I_{n2} = o(I_{n1})$ with probability $1 - O(e^{-\delta \log^2 n})$. First of all, by (5.2), (5.3) and the definition of $I_{n2}(\mathbf{X})$,

$$|I_{n2}(\mathbf{X})|^2 = \frac{1}{\pi^4} \iiiint\limits_{\substack{|x_1|, |x_2| \in [B/M, \pi/2] \\ y_1, y_2 \in (-\pi/2, \pi/2]}} e^{-i\ell(x_1 - x_2) - is(y_1 - y_2)} F(\mathbf{x}, \mathbf{y}; \mathbf{X}) \, d\mathbf{x}d\mathbf{y}, \tag{5.33}$$

where

$$F(\mathbf{x}, \mathbf{y}; \mathbf{X}) = f(x_1, y_1; \mathbf{X}) \overline{f(x_2, y_2; \mathbf{X})} \tag{5.34}$$

$$= \prod_{j=1}^{n} \big[p_j^2 e^{i(x_1' X_j + y_1')} + q_j^2 e^{-i(x_1' X_j + y_1')} \tag{5.35}$$

$$+ p_j q_j \big(e^{i(x_2' X_j + y_2')} + e^{-i(x_2' X_j + y_2')}\big)\big], \tag{5.36}$$

and

$$x_1' = x_1 - x_2, \; x_2' = x_1 + x_2; \quad y_1' = y_1 - y_2, \; y_2' = y_1 + y_2. \tag{5.37}$$

Therefore

$$\mathbb{E}(|I_{n2}(\mathbf{X})|^2) \le \frac{1}{\pi^4} \iiiint\limits_{\substack{|x_1|, |x_2| \in [B/M, \pi/2] \\ y_1, y_2 \in (-\pi/2, \pi/2]}} |F(\mathbf{x}, \mathbf{y})|^n \, d\mathbf{x}d\mathbf{y}, \tag{5.38}$$

where

$$F(\mathbf{x}, \mathbf{y}) = \frac{1}{M} \sum_j p^2(j/M) e^{i(x_1' j + y_1')} + \frac{1}{M} \sum_j q^2(j/M) e^{-i(x_1' j + y_1')}$$

$$+ \frac{1}{M} \sum_j p(j/M) q(j/M) \big(e^{i(x_2' j + y_2')} + e^{-i(x_2' j + y_2')}\big). \tag{5.39}$$

To proceed, we need the following lemma.

Lemma 5.1 *Let $g(u)$ be continuously differentiable on $[0,1]$. Then, for $x \notin 2\pi\mathbb{Z}$ and for all y,*

$$\left| \sum_{j=1}^{M} g(j/M) e^{i(xj+y)} \right| \le \frac{2\|g\| + \|g'\|}{|e^{ix} - 1|}, \tag{5.40}$$

where $\|g\| := \max\{|g(u)| : u \in [0,1]\}$, and $\|g'\| := \max\{|g'(u)| : u \in [0,1]\}$.

Proof of Lemma 5.1. First write

$$\sum_{j=1}^{M} g(j/M) e^{i(xj+y)} = \sum_{j=1}^{M} \frac{e^{i(x(j+1)+y)} - e^{i(xj+y)}}{e^{ix} - 1} g(j/M)$$

$$= \frac{1}{e^{ix} - 1} \left[-g(1/M) e^{i(x+y)} + g(M/M) e^{i(x(M+1)+y)} \right.$$

$$\left. - \sum_{j=1}^{M-1} (g((j+1)/M) - g(j/M)) e^{i(x(j+1)+y)} \right]. \tag{5.41}$$

Since each of the differences in the last sum has absolute value bounded by $M^{-1}\|g'\|$, while the first two terms are clearly bounded by $\|g\|$, we obtain (5.40). ∎

Returning to the proof of the theorem, we observe that since $|x_t| \le \pi/2$, we have $|x_t'| \le \pi$, $t = 1, 2$. Furthermore,

$$B/M \le |x_t| = 0.5|x_1' \pm x_2'|, \quad t = 1, 2, \tag{5.42}$$

implies that $\max\{|x_1'|, |x_2'|\} \ge B/M$. If $|x_1'| \ge B/M$, then applying Lemma 5.1 to the first two sums in (5.39), we obtain

$$|F(\mathbf{x}, \mathbf{y})| \le \frac{2}{M} \sum_{j} p(j/M) q(j/M) + O(B^{-1})$$

$$= 2 \int_0^1 p(u) q(u) \, du + O(B^{-1}). \tag{5.43}$$

If $|x_2'| \ge B/M$, then likewise

$$|F(\mathbf{x}, \mathbf{y})| \le \int_0^1 (p^2(u) + q^2(u)) \, du + O(B^{-1}). \tag{5.44}$$

And, if $\min\{|x_1'|, |x_2'|\} \ge B/M$, then

$$|F(\mathbf{x}, \mathbf{y})| = O(B^{-1}). \tag{5.45}$$

Since the right hand side of (5.43) is dominated by the right hand side of (5.44) (just use that $2pq \le p^2 + q^2$), we conclude that there is a constant c independent of B such that

$$|F(\mathbf{x}, \mathbf{y})| \le \rho + cB^{-1} \quad \text{or} \quad |F(\mathbf{x}, \mathbf{y})| \le cB^{-1}, \tag{5.46}$$

depending upon whether only one or both $|x'_t|$ exceeds B/M. Here

$$
\begin{aligned}
\rho &= \int_0^1 (p^2(u) + q^2(u))\, du = \int_0^1 \left(1 - \frac{1}{2}\cosh^{-2}(\zeta u + \eta)\right) du \\
&= 1 - \frac{\tanh(\zeta + \eta) - \tanh(\eta)}{2\zeta} \\
&= 2^{-\kappa_-(b)}.
\end{aligned}
\tag{5.47}
$$

We conclude then that

$$
\mathbb{E}(|I_{n2}(\mathbf{X})|^2) \le (c/B)^n + O\big(M^{-1}(\rho + c/B)^n\big).
\tag{5.48}
$$

Since $M\rho^n$ is exponentially small if $\limsup(\kappa - \kappa_-(b)) < 0$, we get that for B large enough, there exists a $\delta_4 > 0$ such that

$$
\mathbb{E}(|I_{n2}(\mathbf{X})|^2) \le e^{-\delta_4 n}(Mn)^{-2}.
\tag{5.49}
$$

On the other hand, $|I_{n1}(\mathbf{X})|^2 = (Mn)^{-2}e^{O(\log n^2)}$ with probability $1 - O(e^{-\delta_2 \log^2 n}) - O(e^{-\delta_3 \log^2 n})$ by (5.28) and (5.32). Thus $|I_{n2}(\mathbf{X})| = o(|I_{n1}(\mathbf{X})|)$ with probability at least $1 - O(e^{-\delta_5 \log^2 n})$, implying (5.4). To prove (5.7), we just note that the prefactor in (5.1) can be rewritten as

$$
\begin{aligned}
&\exp\left(\zeta\frac{\ell}{M} + s\eta + \sum_{j=1}^n \log\left(2\cosh\left(\zeta\frac{X_j}{M} + \eta\right)\right)\right) \\
&= \exp\left(\zeta\frac{\ell}{M} + s\eta + n^{1/2}S_n + n\int_0^1 \log\big(2\cosh(\zeta x + \eta)\big)dx + O(nM^{-1})\right) \\
&= \exp\left(nL(\zeta, \eta) + n^{1/2}S_n + O(nM^{-1}) + \zeta\ell/M\right),
\end{aligned}
\tag{5.50}
$$

while, with probability $1 - O(e^{-\delta \log^2 n})$,

$$
I_n(\mathbf{X}) = M^{-1}e^{O(\log^2 n)} = M^{-1}e^{o(n^{1/2})}.
\tag{5.51}
$$

∎

Remark 5.2 *As the reader may have noticed, the condition that ℓ has the same parity as $\sum_j X_j$ has not been used in the above proof. Thus the asymptotics stated in (5.4) hold for all ℓ with $\ell = o(Mn^{1/2})$, independent of the parity of ℓ. But this does* not *mean that the corresponding asymptotics hold for the number of partitions $Z_n(\ell, s)$, since (5.1) is valid only if the parity of ℓ is the same as that of $\sum_j X_j$. If this condition is violated, the left hand side of (5.1) is zero, while w.h.p., the random integral $I_n(\mathbf{X})$ is different from zero.*

Applied to the special case $|\ell| \le 1$, Theorem 5.1 asserts, roughly, that for every point (b, κ) such that $b < b_c$ and $\kappa < \kappa_-(b) < 1$, w.h.p. there are exponentially many perfect partitions. In fact, if in the right hand side of (5.1) the random integral $I_n(\mathbf{X})$ is replaced

by the leading term in (5.4), then the resulting product remains exponentially large within the narrow (crescent-shaped) region between $\kappa = \kappa_-(b)$ and $\kappa = \kappa_c(b)$. In principle, this may mean that the likely number of perfect partitions remains exponentially large in this extended region! An extensive numerical simulation (see Section 9) strongly suggests that the expected logarithm of the number of perfect partitions at every point of the region $\kappa < \kappa_c(b)$ is extremely well approximated by the expected logarithm of the above-mentioned product. Based on our experience with the unconstrained problem and these simulations, we expect that w.h.p. at least the weaker formula

$$\log Z_n(\ell, s) = n[L(\zeta, \eta) - \kappa \log 2 + o(1)]n, \tag{5.52}$$

cf.(5.7), remains valid in the whole region $\limsup(\kappa - \kappa_c(b)) < 0$.

5.2 Distribution of the Bias

Let us have a closer look at the case $|\ell| \leq 1$ and $s = o(n)$. A simple computation shows that

$$\zeta = 6\frac{s}{n} + O((s/n)^2), \quad \eta = -4\frac{s}{n} + O((s/n)^2), \tag{5.53}$$

so that

$$p(u) = P(\zeta u + \eta) = \frac{1}{2} + O(|s|/n), \tag{5.54}$$

and the entries of the covariance matrix K are of order $O(|s|/n)$. Furthermore

$$R = \begin{pmatrix} 1/6 + O(|s|/n) & 1/4 + O(|s|/n) \\ 1/4 + O(|s|/n) & 1/2 + O(|s|/n) \end{pmatrix}, \tag{5.55}$$

so that $\det R = 1/(48) + O(|s|/n)$, and (5.4) yields

$$I_n(\mathbf{X}) = (1 + o_p(1))\frac{4\sqrt{3}}{\pi M n}. \tag{5.56}$$

In addition, the exponential factor in the formula for $Z_n(\ell, s)$ becomes $2^n e^{S_n}$, where

$$\begin{aligned} S_n = &- 4\frac{s^2}{n} + O(|s|/(nM) + |s|^3/n^2) \\ &+ \frac{1}{2}\sum_{j=1}^n (\zeta X_j/M + \eta)^2 + O(s^4/n^3). \end{aligned} \tag{5.57}$$

By the central limit theorem and (5.53), the sum can be written as

$$\begin{aligned} &\zeta^2\left(n\mathbb{E}(U^2) + O_p(n^{1/2})\right) + 2\zeta\eta\left(n\mathbb{E}(U) + O_p(n^{1/2})\right) + \eta^2 n \\ =&4\frac{s^2}{n} + O(|s|^3/n^2) + O_p(s^2/n^{3/2}) \\ =&4\frac{s^2}{n} + o_p(1), \end{aligned} \tag{5.58}$$

uniformly for $|s| \leq n^{2/3}\omega^{-1}(n)$, where $\omega(n) \to \infty$, however slowly. Thus (5.57) simplifies to

$$S_n = -2\frac{s^2}{n} + o_p(1). \tag{5.59}$$

Using this formula and (5.56) we obtain

$$Z_n(\ell, s) = (1 + o_p(1))\frac{4\sqrt{3}}{\pi}\frac{2^n}{Mn}e^{-2s^2/n}, \tag{5.60}$$

uniformly for $|s| \leq n^{2/3}\omega^{-1}(n)$ and $|\ell| \leq 1$; and, of course, $s \equiv n(\mathrm{mod}\ 2)$, and $\ell \equiv \sum_j X_j\ (\mathrm{mod}\ 2)$. In [3] it was shown that, for $Mn^{1/2}/2^n \to 0$, $Y_n(\ell) = \sum_{s=-\infty}^{\infty} Z_{\ell,s}$, the total number of partitions[4] with $\boldsymbol{\sigma} \cdot \mathbf{X} = \ell$ is asymptotic, in probability, to $\frac{2^{n+1}\sqrt{3}}{M\sqrt{2\pi n}}$. Let s_n denote the bias of a perfect partition $\boldsymbol{\sigma}^{(n)}$ chosen uniformly at random from all perfect partitions. The formula for $Y_n(\ell)$ and (5.60) prove the following corollary of Theorem 5.1.

Corollary 5.1 *Assume that* $\limsup \frac{1}{n}\log_2 M < 1$. *Then*

$$\mathbb{P}(s_n = s | \mathbf{X}) = (1 + o_p(1))\frac{2\sqrt{2}}{\sqrt{\pi n}}e^{-2s^2/n} \tag{5.61}$$

uniformly for $|s| \leq n^{2/3}\omega^{-1}(n)$, *(*$s \equiv n(\mathrm{mod}\ 2)$*), and consequently*

$$\mathbb{P}\left(\frac{|s_n|}{\frac{n^{1/2}}{2}} \leq a \,\middle|\, \mathbf{X}\right) \Longrightarrow_p \sqrt{\frac{2}{\pi}}\int_0^a e^{-u^2/2}\,du. \tag{5.62}$$

Remark 5.3 *Thus the bias of the randomly selected (typical) perfect partition is exactly of order* $n^{1/2}$, *just like* t_n, *the bias of the sequence of* n *flips of a fair coin, i.e. the difference between number of heads and number of tails of a fair coin. However,*

$$\mathbb{P}\left(\frac{|t_n|}{n^{1/2}} \leq a\right) \Longrightarrow \sqrt{\frac{2}{\pi}}\int_0^a e^{-u^2/2}\,du, \tag{5.63}$$

i.e. in distribution the bias of the random perfect partition is, in the limit, half as large as the bias of the sequence of n *coin flips. Perhaps we should have anticipated some reduction of the typical bias, since perfect partitions are by definition those with the smallest discrepancy, which should favor smaller bias. In retrospect, the fact that most perfect partitions turn out to have small bias may be responsible for the greater mathematical tractability of the unconstrained problem.*

---

[4]Note that $Y_n(\ell)$ is equal to the total number of perfect partitions if $\ell = 0$, and equal to half the total number of perfect partitions if $\ell = 1$. In a similar way, $Z_n(\ell, s)$ is the total number of perfect partitions with bias s if $\ell = 0$, and half that number if $\ell = 1$.

6 The Hard Phase

6.1 Lower Bounds on the Minimal Discrepancy

Cautiously extrapolating the asymptotic formula in Theorem 5.1, we expect that w.h.p. there will be no perfect partitions in the domain where this expression tends to zero, that is where $\kappa > \kappa_c(b)$. Here we establish this result outside a small window of width $n^{-1/2}$ above κ_c.

Theorem 6.1 *Suppose that* $\limsup |s|/n < b$ *and that* $0 < \liminf \kappa \leq \limsup \kappa < \infty$. *Let* S_n *be the random variable defined in* (5.8), *let* ℓ_n *be a sequence of positive integers with* $\ell_n = o(Mn^{1/2})$ *and let* $|\ell| < \ell_n$. *Then, with probability at least* $1 - O(e^{-\log^2 n})$,

$$Z_n(\ell, s) \leq 2^{[\kappa_c(b)-\kappa]n} e^{n^{1/2}S_n} e^{\log^2 n + O(\ell/M)} \tag{6.1}$$

and

$$\sum_{\ell:|\ell|<\ell_n} Z_n(\ell, s) \leq \ell_n 2^{[\kappa_c(b)-\kappa]n} e^{n^{1/2}S_n} e^{\log^2 n + O(\ell_n/M)}. \tag{6.2}$$

If $(\kappa - \kappa_c(b))n^{1/2} \to \infty$, *we thus have*

$$d_{opt} \geq 2^{[\kappa-\kappa_c(b)-O_p(n^{-1/2})]n}, \tag{6.3}$$

so that w.h.p. there are no perfect partitions.

Remark 6.1 *(i) The proof of* (6.3) *can be generalized to show that there is a constant* $\delta > 0$ *such that, with probability* $1 - O(e^{-\delta \log^2 n})$,

$$d_{opt} \geq \lfloor 2^{[\kappa-\kappa_c(b)-n^{-1/2}\log n]n} \rfloor. \tag{6.4}$$

For $\kappa - \kappa_c(b) \geq 1 + n^{-1/2}\log n$, *there are therefore no perfect partitions with probability* $1 - O(e^{-\delta \log^2 n})$.

(ii) If $|\kappa - \kappa_c(b)| = O(n^{-1/2})$, *the term* $n^{1/2}S_n$ *is larger than* $n|\kappa - \kappa_c(b)|$ *with positive probability, implying that with positive probability,* $Z_n(\ell, s)$ *is smaller than 1, and hence zero. The above theorem therefore implies that for* $|\kappa - \kappa_c(b)| = O(n^{-1/2})$, *the probability that there are no perfect partitions stays bounded away from zero.*

(iii) As mentioned in Remark 2.2, we believe that $d_{opt} = 2^{[\kappa-\kappa_c+o_p(1)]n}$ *whenever* $\liminf(\kappa - \kappa_c) > 0$. *In other words, we believe that for every* $\varepsilon > 0$, *w.h.p.,* $d_{opt} \leq 2^{[\kappa-\kappa_c+\varepsilon]n}$. *If we assume such a bound, then w.h.p. the number of optimal partition* Z_{opt} *is bounded by the right hand side of* (6.2) *with* $\ell_n = \lfloor 2^{[\kappa-\kappa_c+\varepsilon]n} \rfloor$, *implying that w.h.p.* $Z_{opt} \leq 2^{2\varepsilon n}$. *Since* ε *was arbitrary, we get* $Z_{opt} = e^{o_p(n)}$ *whenever* $\liminf(\kappa-\kappa_c) > 0$.

Proof of Theorem 6.1 and Remark 6.1 (i). The bounds (6.3) and (6.4) follow from (6.2). Indeed, let ω_n be such that $\omega_n \to \infty$ and $[\kappa - \kappa_c(n)]n^{1/2} - \omega_n \to \infty$ as $n \to \infty$. Setting $\ell_n = \lfloor 2^{[\kappa-\kappa_c(b)]n-n^{1/2}\omega_n} \rfloor$, the bound (6.2) immediately implies $d_{opt} \geq \ell_n$, which gives (6.3). To prove (6.4), we set $\ell_n = \lfloor 2^{[\kappa-\kappa_c(b)-n^{-1/2}\log n]n} \rfloor$ and observe that for δ sufficiently small, S_n is bounded by $\frac{1}{2}\log n$ with probability $1 - O(e^{-\delta \log^2 n})$. As a

consequence, the r.h.s. of (6.2) goes to zero with probability $1 - O(e^{-\delta \log^2 n})$, implying again that $d_{opt} \geq \ell_n$.

It is thus enough to prove (6.1) and (6.2). Note that the bound (6.2) is not just a consequence of the bound (6.1) since the intersection of $2\ell_n - 1$ events happening with high probability does not necessarily happen with high probability if ℓ_n is not bounded.

Using (5.50), we rewrite $Z_n(\ell, s)$ as

$$Z_n(\ell, s) = 2^{n\kappa_c(b)} e^{n^{1/2} S_n + \zeta \ell/M + O(nM^{-1})} \mathcal{Z}_n(\ell, s), \tag{6.5}$$

where S_n is defined in (5.8) and

$$\mathcal{Z}_n(\ell, s) = \frac{1}{2\pi^2} \int\limits_{\substack{x \in (-\pi, \pi] \\ y \in (-\pi/2, \pi/2]}} e^{-i(\ell x + sy)} f(x, y; \mathbf{X}) \, dx dy, \tag{6.6}$$

with $f(x, y; \mathbf{X})$ as defined in (5.3). In contrast to (5.1), the relation (6.5) holds whether ℓ has the same parity as $\sum_j X_j$ or not, since x is now integrated over $[-\pi, \pi)$ instead of $[-\pi/2, \pi/2)$. Introducing finally

$$\mathcal{Z}_n(s) = \sum_{\ell: |\ell| < \ell_n} \mathcal{Z}_n(\ell, s), \tag{6.7}$$

we have

$$\sum_{\ell: |\ell| < \ell_n} Z_n(\ell, s) = 2^{n\kappa_c} e^{n^{1/2} S_n + O(\ell_n/M) + O(nM^{-1})} \mathcal{Z}_n(s). \tag{6.8}$$

Since $nM^{-1} = o(\log^2 n)$, the bounds (6.1) and (6.2) are equivalent to proving that, with probability $1 - O(e^{-\log^2 n})$, we have $\mathcal{Z}_n(\ell, s) \leq M^{-1} e^{\log^2 n}$ and $\mathcal{Z}_n(s) \leq \ell_n M^{-1} e^{\log^2 n}$.

We will prove these bounds by establishing a suitable bound on the expectation of $\mathcal{Z}_n(\ell, s)$. To this end, we first rewrite $\mathbb{E}(\mathcal{Z}_n(\ell, s))$ as

$$\mathbb{E}(\mathcal{Z}_n(\ell, s)) = \frac{1}{\pi^2} \iint\limits_{\substack{x \in (-\pi, \pi] \\ y \in (-\pi/2, \pi/2]}} e^{-i\ell x - isy} f^n(x, y) \, dx dy, \tag{6.9}$$

$$f(x, y) = \frac{1}{M} \sum_j p(j/M) e^{i(xj+y)} + \frac{1}{M} \sum_j q(j/M) e^{-i(xj+y)}. \tag{6.10}$$

As in the estimates of $\mathbb{E}(|I_{n2}(\mathbf{X})|^2)$ in the proofs of Theorem 5.1, we need the bounds of $|f(x, y)|$ for various ranges of x, y.

Pick $B > 0$. Let $|x| \geq B/M$. Using Lemma 5.1 and (6.10), we get

$$|f(x, y)| \leq c/B. \tag{6.11}$$

Let $|x| \leq B/M$. Setting $x = z/M$, we have $|z| \leq B$. For these x's, let us bound $|f(x,y)|$ more sharply. We have

$$\left| \frac{1}{M} \sum_{j=1}^{M} p(j/M) e^{i(zj/M)+iy} \right|^2$$

$$= \frac{1}{M^2} \sum_{j=1}^{M} p^2(j/M) + \frac{2}{M^2} \sum_{j_1 < j_2} p(j_1/M) p(j_2/M) \cos(z(j_1/M - j_2/M))$$

$$= \left(\frac{1}{M} \sum_{j=1}^{M} p(j/M) \right)^2 - \frac{2}{M^2} \sum_{j_1 < j_2} p(j_1/M) p(j_2/M) \big(1 - \cos(z(j_1/M - j_2/M))\big). \quad (6.12)$$

Here

$$\frac{1}{M} \sum_{j=1}^{M} p(j/M) = \int_0^1 p(u)\, du + O(M^{-1}). \quad (6.13)$$

Pick a small ε and consider $j_1 < j_2$ such that

$$B \frac{j_2 - j_1}{M} \leq 2\pi - \varepsilon \iff j_2 - j_1 \leq \beta M, \ \beta = \frac{2\pi - \varepsilon}{B}. \quad (6.14)$$

Clearly there are $\Theta(\beta M^2)$ such pairs (j_1, j_2). For those (j_1, j_2), and $|z| \leq B$, there is a positive constant $c = c(\varepsilon)$, such that

$$1 - \cos(z(j_1/M - j_2/M)) \geq c\big[z(j_1/M - j_2/M)\big]^2 \quad (6.15)$$

So the double sum in (6.12) is bounded below by

$$\frac{cz^2}{M^2} \sum_{|j_1/M - j_2/M| \leq \beta} p(j_1/M) p(j_2/M) (j_1/M - j_2/M)^2 = (c'B^{-1} + O(M^{-1}))z^2,$$

$$c' = \frac{c}{B} \iint_{\substack{u_1, u_2 \in [0,1] \\ |u_1 - u_2| \leq \beta}} p(u_1) p(u_2) (u_1 - u_2)^2 \, du_1 du_2. \quad (6.16)$$

We thus obtain

$$\left| \frac{1}{M} \sum_{j=1}^{M} p(j/M) e^{i(zj/M+y)} \right|^2 \leq \left(\int_0^1 p(u)\, du + O(1/M) \right)^2 - (c'B^{-1} + O(M^{-1}))z^2, \quad (6.17)$$

so that

$$\left| \frac{1}{M} \sum_{j=1}^{M} p(j/M) e^{i(zj/M+y)} \right| \leq \left(\int_0^1 p(u)\, du + O(M^{-1}) \right) e^{-\alpha_1 B^{-1} z^2}, \quad (6.18)$$

for some positive constant α_1. Analogously to (6.18),

$$\left| \frac{1}{M} \sum_{j=1}^{M} q(j/M) e^{-i(zj/M+y)} \right| \leq \left(\int_0^1 q(u)\, du + O(1/M) \right) e^{-\alpha_2 B^{-1} z^2}, \quad (\alpha_2 > 0), \quad (6.19)$$

hence, for $\alpha = \min\{\alpha_1, \alpha_2\}$,

$$|f(x,y)| \leq (1 + O(M^{-1}))e^{-\alpha B^{-1}z^2} \leq e^{-\alpha' B^{-1}z^2}, \quad \alpha' > 0, \tag{6.20}$$

for $B \geq |z| \geq \Theta(\sqrt{B/M})$. The bounds (6.11) and (6.20) indicate that $|f(x,y)|^n$ is small for large and moderate values of $z(= xM)$, *regardless* of y. The value of y begins to matter when z is small. To see how, we need yet a sharper bound for $|f(x,y)|$ for small $|z|$. By the definition (6.10) of $f(x,y)$, we have

$$
\begin{aligned}
|f(x,y)|^2 = & \frac{1}{M^2} \sum_{j_1,j_2} p(j_1/M)p(j_2/M)e^{iz(j_1/M - j_2/M)} \\
& + \frac{1}{M^2} \sum_{j_1,j_2} q(j_1/M)q(j_2/M)e^{iz(j_2/M - j_1/M)} \\
& + \frac{1}{M^2} \sum_{j_1,j_2} p(j_1/M)q(j_2/M)e^{i(z(j_1/M + j_2/M) + 2y)} \\
& + \frac{1}{M^2} \sum_{j_1,j_2} q(j_1/M)p(j_2/M)e^{-i(z(j_1 + j_2) + 2y)},
\end{aligned}
\tag{6.21}
$$

so that

$$
\begin{aligned}
|f(x,y)|^2 \leq & \left(\frac{1}{M}\sum_j p(j/M)\right)^2 + \left(\frac{1}{M}\sum_j q(j/M)\right)^2 \\
& + 2\left(\frac{1}{M}\sum_j p(j/M)\right)\left(\frac{1}{M}q(j/M)\right) \\
& - \frac{2}{M^2}\sum_{j_1,j_2} p(j_1/M)q(j_2/M)\big[1 - \cos(z(j_1/M + j_2/M) + 2y)\big].
\end{aligned}
\tag{6.22}
$$

Here the first three terms add up to

$$\left(\frac{1}{M}\sum_j (p(j/M) + q(j/M))\right)^2 = 1. \tag{6.23}$$

Furthermore, picking $z_0 > 0$ small enough so that

$$2z_0 + 2|y| \leq 2(z_0 + \pi/2) < 2\pi - \varepsilon, \tag{6.24}$$

we get: for $|z| \leq z_0$,

$$1 - \cos(z(j_1/M + j_2/M) + 2y) \geq c\big[z(j_1/M + j_2/M) + 2y\big]^2. \tag{6.25}$$

The first inequality in (6.24) holds because $|y| \leq \pi/2$, a consequence of $s \equiv n \pmod{2}$.

So, within the factor $2c$, the double sum in (6.22) exceeds

$$\frac{1}{M^2} \sum_{j_1, j_2} p(j_1/M) q(j_2/M) \left[z^2 (j_1/M + j_2/M)^2 + 4yz(j_1/M + j_2/M) + 4y^2 \right]$$

$$= z^2 \left(\iint_{u_1, u_2 \in [0,1]} p(u_1) q(u_2) (u_1 + u_2)^2 \, du_1 du_2 + O(M^{-1}) \right)$$

$$+ 4yz \left(\iint_{u_1, u_2 \in [0,1]} p(u_1) q(u_2) (u_1 + u_2) \, du_1 du_2 + O(M^{-1}) \right) \tag{6.26}$$

$$+ 4y^2 \left(\iint_{u_1, u_2 \in [0,1]} p(u_1) q(u_2) \, du_1 du_2 + O(M^{-1}) \right),$$

Since the functions 1 and $u_1 + u_2$ are linearly independent, there exists $c_0 > 0$ such that, for M large enough, the quadratic form is bounded below by $c_0(z^2 + y^2)$. So

$$|f(x,y)|^2 \leq 1 - c_0(z^2 + y^2) \implies |f(x,y)| \leq e^{-c_0(z^2 + y^2)/2}, \tag{6.27}$$

if $|z| \leq z_0$, $y \in (-\pi/2, \pi/2]$, $M \geq M(z_0)$. Putting (6.20) and (6.27) together enables us to conclude that (6.27), with a possibly smaller c_0, holds for all z, y with $|z| \leq B$ and $|y| \leq \pi/2$. Note however, that c_0 now depends on B and goes to zero like B^{-1} as $B \to \infty$. Making this dependence explicit, we have that

$$|f(x,y)| \leq e^{-c_0'(z^2 + y^2)/B} \tag{6.28}$$

whenever M is large enough, $|z| \leq B$ and $|y| \leq \pi/2$.

Finally, for $|z|, |y|$ both small

$$e^{\pm i(z(j/M) + y)} = 1 \pm i\left(z\frac{j}{M} + y\right) - \frac{1}{2}\left(z\frac{j}{M} + y\right)^2 + O(|z|^3 + |y|^3). \tag{6.29}$$

So

$$f(x,y) = 1 + i\left(z\frac{1}{M}\sum_j \frac{j}{M}\left(p(\frac{j}{M}) - q(\frac{j}{M})\right) + y\frac{1}{M}\sum_j \left(p(\frac{j}{M}) - q(\frac{j}{M})\right) \right)$$

$$- \frac{1}{2}\frac{1}{M}\sum_j (z^2(\frac{j}{M})^2 + 2zy\frac{j}{M} + y^2) + O(|z|^3 + |y|^3)$$

$$= 1 + ia_n z + i(b_n + s/n)y - \frac{1}{2}\frac{1}{M}\sum_j (z^2(\frac{j}{M})^2 + 2zy\frac{j}{M} + y^2) + O(|z|^3 + |y|^3), \tag{6.30}$$

where, by the definitions $p(u) = P(\zeta u + \eta)$ and $q(u) = 1 - P(\zeta u + \eta)$, and equations (3.8) and (4.2),

$$a_n = \frac{1}{M}\sum_j \frac{j}{M}\left(p(\frac{j}{M}) - q(\frac{j}{M})\right) = \int_0^1 u(p(u) - q(u)) \, du + O(M^{-1}) = O(M^{-1}) \tag{6.31}$$

$$b_n = \frac{1}{M} \sum_j \left(p(\frac{j}{M}) - q(\frac{j}{M}) \right) - \frac{s}{n} = \int_0^1 (p(u) - q(u)) \, du - b + O(M^{-1}) = O(M^{-1}).$$

(6.32)

Exponentiating the expansion for f, we arrive at

$$
\begin{aligned}
f(x,y) = &\exp \left(iza_n + iy \left(\frac{s}{n} + b_n \right) \right) \\
&\times \exp \left(-\frac{1}{2}(z,y)\mathcal{Q}(z,y)' + O(|z|^3 + |y|^3) \right),
\end{aligned}
$$

(6.33)

where

$$
\begin{aligned}
\mathcal{Q}_{11} &= \mathbb{E}[(X/M)^2] + O(M^{-2}) \to \mathbb{E}[(X/M)^2], \\
\mathcal{Q}_{12} &= \mathbb{E}(X/M) + O(bM^{-1}) \to \mathbb{E}(X/M), \\
\mathcal{Q}_{22} &= 1 - (b + O(M^{-1}))^2 \to 1 - b^2.
\end{aligned}
$$

(6.34)

Note that the matrix $\mathcal{Q}$ is positive definite in the limit since

$$\mathbb{E}[(X/M)^2]\,(1-b^2) - \mathbb{E}^2(X/M) \to \frac{1}{3}(1-b^2) - \frac{1}{4} = \frac{1-4b^2}{12} > 0,$$

(6.35)

since $b < 1/2$. By (6.33) and (6.34)

$$e^{-i\ell x - isy} f^n(x,y) = \exp \left(iz(\tilde{a}_n + iy b_n - \frac{n}{2}(z,y)\mathcal{Q}(z,y)' + O(n(|z|^3 + |y|^3)) \right),$$

(6.36)

where $\tilde{a}_n = na_n - \ell/M$ and $\tilde{b}_n = nb_n$.

Let us derive an asymptotic formula for $\mathbb{E}(\mathcal{Z}_n(\ell, s))$, using (6.11), (6.28), and (6.33)-(6.36). By (6.9) and (6.11), the contribution of the (x,y) with $|x| > B/M$ to $\mathbb{E}(\mathcal{Z}_n(\ell, s))$ is of order $O((c/B)^n)$. Let $|x| \le B/M$. Switch to $z = Mx, y = y$. By (6.28), the contribution of the (z,y)'s with $\|(z,y)\| \ge r_n := n^{-1/2} \log n$ is of order

$$M^{-1} \int_{r \ge r_n} r e^{-nc_0' r^2/B} \, dr = M^{-1} e^{-\Theta(B^{-1}\log^2 n)}.$$

(6.37)

By (6.33)-(6.36), the contribution of the (z,y)'s with $\|(z,y)\| \le r_n$ is asymptotic to

$$
\begin{aligned}
&\frac{1}{2M\pi^2} \iint_{\|(z,y)\| \le r_n} \exp \left(iz\tilde{a}_n + iy\tilde{b}_n - \frac{n}{2}(z,y)\mathcal{Q}(y,z)' \right) \left(1 + O(n|z|^3 + n|y|^3) \right) dzdy \\
&= \frac{1}{2M\pi^2} \iint_{\|(z,y)\| \le r_n} \exp \left(iz\tilde{a}_n + iy\tilde{b}_n - \frac{n}{2}(z,y)\mathcal{Q}(z,y)' \right) dzdy + O\left(\frac{1}{Mn} n^{-1/2} \right).
\end{aligned}
$$

(6.38)

The first term on the r.h.s. of (6.38) is equal to

$$\frac{1}{Mn\pi\sqrt{\det \mathcal{Q}}} \left[\exp \left(-\frac{1}{2n} \|(\tilde{a}_n, b_n)\mathcal{Q}^{-1/2}\|^2 \right) + O\left(\int_{t \ge \Theta(\log n)} t e^{-t^2/2} \, dt \right) \right],$$

(6.39)

where the exponential term is

$$1 + O(n^{-1}(\tilde{a}_n^2 + b_n^2)) = 1 + O(n/M^2) + O(n^{-1}(\ell/M)^2 = 1 + O(e^{-\Theta(n)}) + O(n^{-1}(\ell/M)^2), \tag{6.40}$$

while the integral is of order $e^{-\Theta(\log^2 n)}$. Combining the last formula with the estimates of contributions of other ranges of (x, y), we obtain

$$\mathbb{E}(\mathcal{Z}_n(\ell, s)) = (1 + O(n^{-1/2}) + O((\ell/M)^2 n^{-1})) \frac{1}{Mn} \frac{1}{\pi\sqrt{(1 - b^2)\mathbb{E}(U^2) - \mathbb{E}^2(U)}}$$

$$= (1 + o(1)) \frac{2\sqrt{3}}{\pi\sqrt{1 - b^2}} \frac{1}{Mn}, \tag{6.41}$$

whenever $|\ell| \le \ell_n = o(n^{1/2}M)$. Summing over $\ell \in \{-(\ell_n - 1), \dots, \ell_n - 1\}$, the bound (6.41) clearly implies a similar bound for $\mathcal{Z}_n(s)$, namely

$$\mathbb{E}(\mathcal{Z}_n(s)) = (1 + o(1)) \frac{2\sqrt{3}}{\pi\sqrt{1 - b^2}} \frac{2\ell_n - 1}{Mn}. \tag{6.42}$$

By the bounds (6.41) and (6.42) and Markov's inequality, we have that $Z_n(\ell, s) \le M^{-1}e^{\log^2 n}$ and $\mathcal{Z}_n(s) \le \ell_n M^{-1}e^{\log^2 n}$ with probability $1 - O(e^{-\log^2 n})$. Combined with (6.5) and (6.8) this implies (6.1) and (6.2). ∎

6.2 A Digression: The Expected Number of Perfect Partitions

The reader may have noticed how gingerly we have tiptoed around the first factor in (5.1), concentrating instead on the asymptotic behavior of the double integral. To see why, we will show that $\mathbb{E}(Z_n(\ell, s))$ remains exponentially large above the curve $\kappa = \kappa_c(b)$, in sharp contrast to the fact that, in this domain, w.h.p. there are no perfect partitions at all.

Theorem 6.2 *Let $|\ell| \le 1$. For $s > 0$, $s + n \equiv 0 \pmod 2$, and $b = s/n$ bounded away from 0 and 1,*

$$\mathbb{E}[Z_n(\ell, s)] \sim \frac{2}{M} \binom{n}{\frac{n+s}{2}} \frac{e^{\lambda s}\phi^n(\lambda)}{\sqrt{2\pi n \, Var(U_\lambda)}}, \quad \phi(\lambda) := \frac{\sinh \lambda}{\lambda}. \tag{6.43}$$

where $U_\lambda \in [-1, 1]$ has density

$$\frac{e^{\lambda x}/2}{\int_{y \in [-1,1]} e^{\lambda y}/2 \, dy}, \tag{6.44}$$

and $\lambda < 0$ is such that $\mathbb{E}(U_\lambda) = -b$, or explicitly:

$$\coth \lambda - \frac{1}{\lambda} = -b. \tag{6.45}$$

Consequently,

$$\lim_{n \to \infty} \frac{1}{n} \log \mathbb{E}[Z_n(\ell, s)] = R(\kappa, b), \tag{6.46}$$

where

$$R(\kappa, b) = \frac{1+b}{2} \log \frac{2}{1+b} + \frac{1-b}{2} \log \frac{2}{1-b} + \lambda b + \log \frac{\sinh \lambda}{\lambda} - \kappa \log 2. \tag{6.47}$$

Proof of Theorem 6.2. In order to calculate the expectation of $Z_n(\ell, s)$, we use the following analogue of (3.6), which is valid whether or not ℓ has the same parity as $\sum_j X_j$:

$$Z_n(\ell, s) = \frac{2^n}{2\pi^2} \iint_{\substack{x \in (-\pi, \pi] \\ y \in (-\pi/2, \pi/2]}} e^{-i(\ell x + sy)} \prod_{j=1}^{n} \cos(xX_j + y) \, dx dy. \tag{6.48}$$

This gives

$$\mathbb{E}(Z_n(\ell, s)) = \frac{2^n}{2\pi^2} \iint_{\substack{x \in (-\pi, \pi] \\ y \in (-\pi/2, \pi/2]}} e^{-i(\ell x + sy)} \mathbb{E}^n \big(\cos(xX + y) \big) \, dx dy, \tag{6.49}$$

where

$$\begin{aligned}
\mathbb{E}\big(\cos(xX + y)\big) &= \text{Re} \left[e^{iy} M^{-1} \sum_{j=1}^{M} e^{ixj} \right] = \text{Re} \left[M^{-1} e^{i(x+y)} \frac{e^{ixM} - 1}{e^{ix} - 1} \right] \\
&= \frac{\sin\left(\frac{Mx}{2}\right)}{M \sin\left(\frac{x}{2}\right)} \cos\left(\frac{(M+1)x}{2} + y\right).
\end{aligned} \tag{6.50}$$

Notice that the first factor is a function of x only, and the argument of the cosine is y shifted by $x(M+1)/2$. Integrating first with respect to y, we can choose $y \in (-\pi/2 + x(M+1)/2, \pi/2 + x(M+1)/2]$, thus reducing the y-integral to

$$e^{isx\frac{M+1}{2}} \frac{1}{\pi} \int_{y \in (-\pi/2, \pi/2]} e^{-isy} \cos^n y \, dy. \tag{6.51}$$

Here we can write $\cos y = \mathbb{E}(e^{iy\sigma})$, $\mathbb{P}(\sigma = \pm 1) = 1/2$. So, introducing the independent copies $\sigma_1, \ldots, \sigma_n$ of σ, we write the last integral as

$$\mathbb{P}\left(\sum_{j=1}^{n} \sigma_j = s \right) = \frac{1}{2^n} \binom{n}{\frac{n+s}{2}}. \tag{6.52}$$

Therefore we get the simpler expression

$$\mathbb{E}(Z_n(\ell, s)) = \binom{n}{\frac{n+s}{2}} \frac{1}{2\pi} \int_{x \in (-\pi, \pi]} e^{ixt} \left(\frac{\sin\frac{Mx}{2}}{M \sin\frac{x}{2}} \right)^n dx; \tag{6.53}$$

$$t := -\ell + s\frac{M+1}{2}. \tag{6.54}$$

To simplify the rest of the exposition, let us assume that $\sin x/2$ in denominator can be replaced asymptotically by $x/2$. (A refined version of the argument shows that this

replacement is asymptotically correct for $n = o(M)$. We leave it to the interested reader to check this.) Substituting $z = Mx/2$, we get then

$$\mathbb{E}(Z_n(\ell, s)) \sim \binom{n}{\frac{n+s}{2}} \frac{1}{\pi M} \int\limits_{z \in (-M\pi/2, M\pi/2]} e^{i\tau z} \left(\frac{\sin z}{z}\right)^n dz,$$

$$\tau := s(1 + M^{-1}) - 2\ell/M,$$

(6.55)

so that τ is very close to s, since $|\ell| \leq 1$. Next, we observe that $y^{-1} \sin y$ is the characteristic function of the random variable U, uniformly distributed on $[-1, 1]$. Hence $\left(\frac{\sin z}{z}\right)^n$ is the characteristic function of $S_n = \sum_{j=1}^n U_j$, where U_j are the independent copies of U. In particular, using the Fourier inversion formula for f_{S_n}, the density of S_n,

$$f_{S_n}(-\tau) = \frac{1}{2\pi} \int\limits_{z \in (-\infty, \infty)} e^{i\tau z} \left(\frac{\sin z}{z}\right)^n dz,$$

(6.56)

we get from (6.55):

$$\mathbb{E}(Z_n(\ell, s)) \sim \frac{2}{M} \binom{n}{\frac{n+s}{2}} f_{S_n}(\tau).$$

(6.57)

(The error caused by extending the integration interval in (6.55) to $(-\infty, \infty)$ is extremely small, of order $M^{-n} = 2^{-\kappa n^2}$.) We cannot use the local limit theorem for $f_{S_n}(-\tau)$ directly as $\mathbb{E}S_n = n\mathbb{E}U \neq -\tau$. So we introduce an auxiliary random variable U_λ with density proportional to $e^{\lambda x}$ on $[-1, 1]$, choosing λ such that $\mathbb{E}(U_\lambda) = -\tau/n$, that is setting λ equal the root of

$$\frac{\phi'(\lambda)}{\phi(\lambda)} = -\frac{\tau}{n}, \quad \phi(\lambda) := \frac{1}{2} \int\limits_{x \in [-1, 1]} e^{\lambda x} dx = \frac{\sinh \lambda}{\lambda}.$$

(6.58)

Then

$$f_{S_n}(-\tau) = e^{-\lambda(-\tau)} \phi^n(\lambda) f_{S_{n,\lambda}}(-\tau),$$

(6.59)

where $S_{n,\lambda} = \sum_{j=1}^n U_{j,\lambda}$. By the local limit theorem (see, e.g., [11], Sect. 5.10), the density $f_{S_{n,\lambda}}(-\tau)$ of $S_{n,\lambda}$ is asymptotic to

$$\frac{1}{\sqrt{2\pi n \mathrm{Var} U_\lambda}},$$

(6.60)

where $\mathrm{Var}(U_\lambda)$ can be explicitly calculated, giving

$$\mathrm{Var}(U_\lambda) = \frac{\phi''(\lambda)}{\phi(\lambda)} - (\tau/n)^2.$$

(6.61)

Thus

$$\mathbb{E}(Z_n(\ell, s)) \sim \frac{2}{M} \binom{n}{\frac{n+s}{2}} e^{\lambda\tau} \phi^n(\lambda) f_{S_{n,\lambda}}(-\tau) \sim \frac{2}{M} \binom{n}{\frac{n+s}{2}} \frac{e^{\lambda s} \phi^n(\lambda)}{\sqrt{2\pi n \mathrm{Var}(U_\lambda)}},$$

(6.62)

as claimed. ∎

6.3   Optimal Imperfect Partitions

In Theorem 6.1 we proved that, for $\kappa > \kappa_c(b)$ *and* $b < b_c$, w.h.p. the minimum discrepancy is at least $2^{n(\kappa - \kappa_c(b)) - O_p(n^{1/2})}$. The next theorem provides a complementary upper bound for the minimum discrepancy.

Theorem 6.3 *Suppose that* $\limsup |s|/n < b$ *and that* $0 < \liminf \kappa \le \limsup \kappa < \infty$. *Let* $\varepsilon > 0$, *let* S_n *be the random variable defined in* (5.8), *and let* ℓ_n *be a sequence of positive integers with* $\ell_n = o(Mn^{1/2}/\log n)$ *and* $\ell_n \ge 2^{[\kappa - \kappa_-(b) + \varepsilon]n}$. *Then there is a constant* $\delta > 0$ *such that, with probability* $1 - O(e^{-\delta \log^2 n})$,

$$\sum_{\ell : |\ell| < \ell_n} Z_n(\ell, s) = \ell_{n,\mathbf{X}} 2^{[\kappa_c(b) - \kappa]n} e^{n^{1/2} S_n + o(n^{1/2})}, \tag{6.63}$$

where $\ell_{n,\mathbf{X}}$ *is the number of integers* ℓ *with* $|\ell| < \ell_n$ *with the same parity as* $\sum_j X_j$. *With probability* $1 - O(e^{-\delta \log^2 n})$, *we thus have*

$$d_{opt} \le \lceil 2^{(\kappa - \kappa_-(b) + \varepsilon)n} \rceil, \tag{6.64}$$

implying in particular that $M^{-1} d_{opt}$ *is exponentially small in* n.

Note that for $\limsup(\kappa - \kappa_-(b)) < 0$, we recover that $d_{opt} \le 1$. Not astonishingly, the proof of Theorem 6.3 follows closely the proof of Theorem 5.1, which established that, w.h.p., there are exponentially many perfect partitions for $\limsup(\kappa - \kappa_-(b)) < 0$.

Proof of Theorem 6.3. Let us first note that depending on the parity of $\sum_j X_j$, the number $\ell_{n,\mathbf{X}}$ is either ℓ_n or $\ell_n - 1$, implying in particular that $\ell_{n,\mathbf{X}} \ge \ell_n - 1$. Using this fact, it is not hard to see that the bound (6.64) follows from (6.63). Indeed, let $\ell_n = \lceil 2^{(\kappa - \kappa_- + \varepsilon)n} \rceil + 1$. Since $\ell_{n\mathbf{X}} \ge \ell_n - 1 \ge 2^{(\kappa - \kappa_- + \varepsilon)n}$, the right hand side of (6.63) goes to infinity, implying that $d_{opt} \ge \ell_n - 1$. It is therefore enough to prove (6.63). Also, since both sides of (6.63) are identically zero if $\ell_{n,\mathbf{X}} = 0$, it is enough to consider $\ell_{n,\mathbf{X}} > 0$.

Analogously to the proof of Theorem 6.1, we set

$$\mathcal{Z}_n(s) = \sum_{\ell : |\ell| < \ell_n} \mathcal{Z}_n(\ell, s), \tag{6.65}$$

where $\mathcal{Z}_n(\ell, s)$ is the random integral defined in (6.6). Let us note, however, that $\mathcal{Z}_n(\ell, s)$ is equal to the random integral defined in (5.2) if ℓ is of the same parity as $\sum_j X_j$, and equal to zero otherwise. The sum in (6.65) can therefore be replaced by the sum over all ℓ with the same parity as $\sum_j X_j$, and

$$\mathcal{Z}_n(s) = \frac{1}{\pi^2} \iint_{\substack{x \in (-\pi/2, \pi/2] \\ y \in (-\pi/2, \pi/2]}} \left[\sum_{\ell : |\ell| < \ell_n}{}' e^{-i\ell x} \right] e^{-isy} f(x, y; \mathbf{X}) \, dx \, dy, \tag{6.66}$$

where the sum $\sum'$ indicates the sum over all ℓ with the same parity as $\sum_j X_j$. Obviously, we have

$$\left| \sum_{\ell : |\ell| < \ell_n}{}' e^{-i\ell x} \right| \le \ell_{n,\mathbf{X}} \tag{6.67}$$

and

$$\sum_{\ell:|\ell|<\ell_n}{}' e^{-i\ell x} = \ell_{n,\mathbf{X}}\big(1 + O\big((\ell_n|x|)^2\big)\big) \quad \text{as} \quad \ell_n|x| \to 0. \tag{6.68}$$

Recalling that, depending on the parity of $\sum_j X_j$, the number $\ell_{n,\mathbf{X}}$ of terms in the sum $\sum'$ is either ℓ_n or $\ell_n - 1$, we also have

$$\left|\sum_{\ell:|\ell|<\ell_n}{}' e^{-i\ell x}\right| = \left|\sum_{k=0}^{\ell_{n,\mathbf{X}}-1} e^{-i2kx}\right| \le 1 + \left|\frac{\sin((\ell_n-1)x)}{\sin x}\right| \le \ell_n. \tag{6.69}$$

As in the proof of Theorem 5.1, we split the right hand side of (6.66) into two parts, $J_{n1}(\mathbf{X})$ and $J_{n2}(\mathbf{X})$, for $|x| \le B/M$ and $|x| > B/M$ respectively. We start with $J_{n1}(\mathbf{X})$. As in (5.20), we restrict ourselves to the event A_n defined in (5.18). With the help of (6.67), we then bound the contributions of all x with $\|(Mx,y)\| \ge r_n = n^{-1/2}\log n$ by

$$\frac{\ell_{n,\mathbf{X}}}{\pi^2} \iint\limits_{\substack{\|(Mx,y)\|\ge r_n \\ |Mx|\le B}} |f(x,y;\mathbf{X})|\, dxdy \le \frac{\ell_{n,\mathbf{X}}}{Mn} \iint\limits_{\|\mathbf{z}\|\ge \log n} e^{-c_4\|\mathbf{z}\|^2}\, dz_1 dz_2 = O\left(\frac{\ell_{n,\mathbf{X}}}{Mn} e^{-c_4(\log^2 n)}\right). \tag{6.70}$$

For $\|(Mx,y)\| \le r_n$, we may use (6.68) since $\ell_n|x| \le M^{-1}\ell_n r_n = o(r_n n^{1/2}\log^{-1} n) \to 0$. And, analogously to (5.32), we have that with probability at least $1 - O(e^{-\delta_3\log^2 n})$

$$\frac{1}{\pi^2} \iint\limits_{\|(Mx,y)\|\le r_n} \left[\sum_{\ell:|\ell|<\ell_n}{}' e^{-i\ell x}\right] e^{-isy} f(x,y;\mathbf{X})\, dxdy$$

$$= \frac{\ell_{n,\mathbf{X}}}{Mn}\left[\frac{1}{\pi\sqrt{\det R}}\exp\big(-\tfrac{1}{4}\boldsymbol{\tau}_n R^{-1}\boldsymbol{\tau}_n'\big) + o(1)\right]. \tag{6.71}$$

Comparing (6.70) and (6.71) (and using again the bound (5.28), this time to get a lower bound on the right hand side of (6.71)), we see that the last expression is a sharp asymptotic formula for $J_{n1}(\mathbf{X})$.

Next, we use (6.69) to bound

$$\mathbb{E}(|J_{n2}(\mathbf{X})|^2) \le \frac{1}{\pi^4} \iiiint\limits_{\substack{|x_1|,|x_2|\in[B/M,\pi/2] \\ y_1,y_2\in(-\pi/2,\pi/2]}} (1 + S(x_1))(1 + S(x_2))|F(\mathbf{x},\mathbf{y})|^n\, d\mathbf{x}d\mathbf{y}, \tag{6.72}$$

where $F(\mathbf{x},\mathbf{y})$ is defined in (5.39) and

$$S(x) = \frac{|\sin((\ell_n-1)x)|}{|\sin(x)|}. \tag{6.73}$$

Arguing as in the case of $I_{n2}(\mathbf{X})$, we thus obtain that $\mathbb{E}(|J_{n2}(\mathbf{X})|^2)$ is of order

$$
(c/B)^n \left(1 + \int\limits_{x \in (-\pi/2, \pi/2]} \frac{|\sin((\ell_n - 1)x)|}{|\sin(x)|} \, dx \right)^2
$$
$$
+ (\rho + c/B)^n \iint\limits_{\substack{x_1, x_2 \in (-\pi/2, \pi/2] \\ |x_1 + x_2| \le B/M}} \left(1 + \frac{|\sin((\ell_n - 1)x_1)|}{|\sin(x_1)|} \right) \left(1 + \frac{|\sin((\ell_n - 1)x_2)|}{|\sin(x_2)|} \right) dx_1 dx_2, \quad (6.74)
$$

with, as before, $\rho = 2^{-\kappa_-}$. Here the single integral is of order

$$
\int\limits_{x \in (-\pi/2, \pi/2]} \frac{|\sin((\ell_n - 1)x)|}{|x|} \, dx = \int\limits_{|t| \le \pi(\ell_n - 1)/2} \frac{|\sin t|}{|t|} \, dt = O(\log \ell_n) = O(n), \quad (6.75)
$$

and the double integral is of order

$$
\frac{B}{M} \int\limits_{x \in (-\pi/2, \pi/2]} \ell_n \left(1 + \frac{|\sin((\ell_n - 1)x)|}{|\sin(x)|} \right) dx = O(M^{-1} \ell_n \log \ell_n) = O(n \ell_n M^{-1}). \quad (6.76)
$$

Combining the contributions from (6.75) and (6.76), we get that for B sufficiently large

$$
\mathbb{E}(|J_{n2}(\mathbf{X})|^2) = O\left(n^2 (c/B)^n \right) + O\left(n \ell_n M^{-1} (\rho + c/B)^n \right)
$$
$$
= O\left(\frac{\ell_n}{Mn^2} \rho^n e^{(\varepsilon/2)n} \right) = O\left(\left(\frac{\ell_n}{Mn} \right)^2 e^{-(\varepsilon/2)n} \right). \quad (6.77)
$$

Here, in the second step we used that ρ is bounded away from 0 and 1, and that B is large enough, while in the third step, we used that ℓ_n/M is assumed to be at least $\rho^n e^{\varepsilon n}$. By Markov's inequality (and the fact that $\ell_n \le \ell_{n,\mathbf{X}} + 1 \le 2\ell_{n,\mathbf{X}}$ whenever $\ell_{n,\mathbf{X}} \ne 0$), we conclude that with probability $1 - O(e^{-(\varepsilon/4)n})$,

$$
|J_{n2}(\mathbf{X})| \le \frac{\ell_n}{Mn} e^{-(\varepsilon/8)n} \le \frac{2\ell_{n,\mathbf{X}}}{Mn} e^{-(\varepsilon/8)n}. \quad (6.78)
$$

By (6.70), (6.71) and (5.28), $J_{n1}(\mathbf{X})$ is of order at least $\frac{\ell_{n,\mathbf{X}}}{Mn} e^{-\log^2 n}$ with probability $e^{-\delta_4 \log^2 n}$ for some $\delta_4 > 0$, much larger than the above order of $|J_{n2}(\mathbf{X})|$. We thus have shown that there is a constant $\delta = \delta(\varepsilon) > 0$ such that with probability at least $1 - O(e^{-\delta \log^2 n})$,

$$
\mathcal{Z}_n(s) = (1 + o(1)) \frac{\ell_{n,\mathbf{X}}}{Mn} \frac{1}{\pi \sqrt{\det R}} \exp\left(-\boldsymbol{\tau}_n (4R)^{-1} \boldsymbol{\tau}'_n \right). \quad (6.79)
$$

Together with (6.8), this implies the bound (6.63). ∎

The following corollary follows immediately from Remark 6.1 (i) and Theorem 6.3.

Corollary 6.1 *Assume that* $\limsup |s|/n < b$, $\limsup \kappa < \infty$ *and* $\liminf[\kappa - \kappa_c(b)] > 0$, *and let* $\varepsilon > 0$. *Then there exists a constant* $\delta > 0$ *such that with probability* $1 - O(e^{-\delta \log^2 n})$,

$$
2^{[\kappa - \kappa_c(b) - n^{-1/2} \log n]n} \le d_{opt} \le 2^{[\kappa - \kappa_-(b) + \varepsilon]n}. \quad (6.80)
$$

As argued in Remark 6.1(iii), we expect that for $\liminf \kappa > \kappa_c$, the number of optimal partitions Z_{opt} grows subexponentially. But so far, we only can prove the following corollary to Theorem 6.3.

Corollary 6.2 *Suppose that* $\limsup |s|/n < b$ *and that* $0 < \liminf \kappa \le \limsup \kappa < \infty$. *Then for every* $\varepsilon > 0$, *there exists a constant* $\delta > 0$ *such that*

$$Z_{opt} \le 2^{(\kappa_c + \varepsilon)n} \max\{2^{-\kappa n}, 2^{-\kappa_- n}\} \tag{6.81}$$

with probability $1 - O(e^{-\delta \log^2 n})$.

Proof. Let $\ell_n = \lceil 2^{[\kappa - \kappa_-(b) + \varepsilon/2]n} \rceil + 1$. By the bound (6.64) of Theorem 6.3, we have that there exists some $\delta > 0$ such that $d_{opt} \le \ell_n - 1$ with probability $1 - O(e^{-\delta \log^2 n})$. Using the bound (6.63), we therefore get

$$Z_{opt} \le \ell_n 2^{[\kappa_c(b) - \kappa]n} e^{n^{1/2} S_n + o(n^{1/2})} \le \ell_n 2^{[\kappa_c(b) - \kappa]n} e^{O(n^{1/2} \log n)}, \tag{6.82}$$

again with probability $1 - o(e^{-\delta \log^2 n})$. Bounding $\ell_n \le 3 \max\{1, 2^{[\kappa - \kappa_-(b) + \varepsilon/2]n}\}$, we obtain the bound (6.81). ∎

7 The Sorted Phase

It remains to study the minimum discrepancy for $b > b_c$.

7.1 Characteristics of the Sorted Phase

Theorem 7.1 *Suppose that* $M \gg n^2$ *and* $\liminf s/n > b_c$. *Then w.h.p. the optimal partition* $\boldsymbol{\sigma}^*$ *is the sorted partition obtained as follows. Order* X_j *in the increasing order, so that* $X_{\pi(1)} \le \cdots \le X_{\pi(n)}$ *for some permutation* π *of* $\{1, \ldots, n\}$. *W.h.p. there will be no ties, and the ordering* π *will be uniquely defined. Denoting* $j_n = (n + s)/2 = n(1 + b)/2$, $b = s/n$,

$$\sigma_j^* = \begin{cases} 1, & 1 \le j \le j_n, \\ -1, & j_n < j \le n, \end{cases} \tag{7.1}$$

and w.h.p. the minimum discrepancy is asymptotic to $\frac{Mn}{4}[(1 + b)^2 - 2]$, *i.e. of order* Mn.

Proof of Theorem 7.1. We begin with the following observation. If

$$\delta_s(\boldsymbol{X}) = \sum_{j=1}^{j_n} X_{\pi(j)} - \sum_{j=j_n+1}^{n} X_{\pi(j)} \ge 0, \tag{7.2}$$

then the sorted partition is optimal, and $d_{opt} = \delta_s(\mathbf{X})$. Indeed, let $\boldsymbol{\sigma}$ be any feasible partition $\boldsymbol{\sigma}$. Then $s(\boldsymbol{\sigma}) = |\{j : \sigma_j = 1\}| - |\{j : \sigma_j = -1\}| = 2|\{j : \sigma_j = 1\}| - n$ so that

$|\{j : \sigma_j = 1\}| = j_n$. Thus

$$\boldsymbol{\sigma} \cdot \mathbf{X} = \sum_{\{j:\sigma_j=1\}} X_j - \sum_{\{j:\sigma_j=-1\}} X_j \tag{7.3}$$

$$\geq \sum_{j=1}^{j_n} X_{\pi(j)} - \sum_{j=j_n+1}^{n} X_{\pi(j)} \geq 0, \tag{7.4}$$

which implies optimality of the partition $\boldsymbol{\sigma}^*$ and $d_{opt} = \delta_s(\mathbf{X})$.

In light of this property, all we need to do is to show that, for $b > b_c$ and bounded away from b_c, w.h.p.

$$\delta_s(\mathbf{X}) = \frac{Mn}{4}\Big[(1+b)^2 - 2\Big](1 + o(1)) \geq 0. \tag{7.5}$$

Let U be $[0,1]$-uniform, and $U_1, \dots, U_n$ be the independent copies of U. Then the sequence $\{X'_j\} := \{\lceil MU_j \rceil\}$ has the same distribution as our sequence $\{X_j : 1 \leq j \leq n\}$. So we will consider $\{X'_j\}$ instead. Since $M \gg n^2$, it follows easily that w.h.p. $X'_{\pi(1)} < \cdots < X'_{\pi(n)}$ if and only if $U_{\pi(1)} < \cdots < U_{\pi(n)}$. Furthermore

$$0 \leq \lceil MU_j \rceil - MU_j \leq 1, \tag{7.6}$$

so it suffices to show that w.h.p.

$$\sum_{j=1}^{j_n} U_{\pi(j)} - \sum_{j=j_n+1}^{n} U_{\pi(j)} = \frac{n}{4}\Big[(1+b)^2 - 2\Big](1 + o(1)). \tag{7.7}$$

A second simplification is based on a fact that the sequence $\{U_{\pi(j)}\}_{1 \leq j \leq n}$ has the same distribution as $\{\frac{S_j}{S_{n+1}}\}_{1 \leq j \leq n}$, where $S_j = \sum_{k=1}^{j} Z_k$, and $Z_1, \dots, Z_n$ are independent copies of Z, the Exponential (λ), $\lambda > 0$ being arbitrary. Choose $\lambda = 1$ for certainty. Since S_{n+1} is w.h.p. asymptotic to $(n+1)\mathbb{E}Z = n + 1$, it suffices to show that w.h.p.

$$\sum_{j=1}^{j_n} S_j - \sum_{j=j_n+1}^{n} S_j = \frac{n^2}{4}\Big[(1+b)^2 - 2\Big](1 + o(1)), \tag{7.8}$$

or, in terms of Z_t's, that w.h.p.

$$\Sigma_1 - \Sigma_2 = \frac{n^2}{4}\Big[(1+b)^2 - 2\Big](1 + o(1)), \tag{7.9}$$

where

$$\Sigma_1 = \sum_{k=1}^{j_n}(j_n - k + 1)Z_k,$$

$$\Sigma_2 = (n - j_n)\sum_{k=1}^{j-n} Z_k + \sum_{k=j_n+1}^{n}(n - k + 1)Z_k. \tag{7.10}$$

Finally, introduce $\{Z'_k\}$, the truncated version of $\{Z_k\}$, namely

$$Z'_k = \min(Z_k, 2\log n), \quad 1 \le k \le n. \tag{7.11}$$

Noticing that

$$\mathbb{P}(\exists\, k \le n:\, Z'_k \ne Z_k) \le n\mathbb{P}(Z'_1 \ne Z_1) \tag{7.12}$$

$$= n\mathbb{P}(Z_1 > 2\log n) = n^{-1} \to 0, \tag{7.13}$$

we can and will replace Z_k by Z'_k in (7.10), denoting the corresponding sums by Σ'_i. Observe that

$$\mathbb{E}(Z'_k) = \mathbb{E}(Z_k) - \int_{2\log n}^{\infty} (y - 2\log n)e^{-y}\,dy = 1 - n^{-2}, \tag{7.14}$$

so that

$$\mathbb{E}(\Sigma'_i) = \mathbb{E}(\Sigma_i) + O(1), \quad i = 1, 2. \tag{7.15}$$

By the Azuma-Hoeffding inequality (see, e.g., [11], Section 12.2) and $Z'_k \le 2\log n$, we have: for every $\alpha > 0$,

$$\mathbb{P}(|\Sigma'_i - \mathbb{E}(\Sigma'_i)| > \alpha) \le 2\exp\left(-\frac{\alpha^2}{2n(2n\log n)^2}\right) = 2\exp\left(-\frac{\alpha^2}{8n^3\log^2 n}\right). \tag{7.16}$$

Using this bound with $\alpha = n^{7/4}$, we obtain that w.h.p.

$$|\Sigma'_i - \mathbb{E}(\Sigma'_i)| \le n^{7/4} \ll n^2, \tag{7.17}$$

implying that w.h.p.

$$\Sigma_1 - \Sigma_2 = \Sigma'_1 - \Sigma'_2 = \mathbb{E}(\Sigma'_1) - \mathbb{E}(\Sigma'_2) + O(n^{7/4}). \tag{7.18}$$

It remains to observe that

$$
\begin{aligned}
\mathbb{E}(\Sigma'_1 - \Sigma'_2) &= \mathbb{E}(\Sigma_1) - \mathbb{E}(\Sigma_2) + O(1) \\
&= \frac{j_n(j_n - 1)}{2} - (n - j_n)j_n - \frac{(n - j_n)(n - j_n + 1)}{2} + O(1) \\
&= \frac{2j_n^2 - n^2}{2} + O(n) \\
&= \frac{n^2}{4}[(1 + b)^2 - 2] + O(n),
\end{aligned}
\tag{7.19}
$$

which completes the proof. ∎

Remark 7.1 *Consider a point (κ, b) such that $b < b_c$. From the above proof, it is easy to show that w.h.p. the sorted partition $\boldsymbol{\sigma}^*$ cannot be optimal. Indeed, by (7.19), we see that*

$$\mathbb{E}(\Sigma'_1 - \Sigma'_2) = \frac{n^2}{4}\left[(1 + b)^2 - 2\right] + O(n) \le -\Theta(n^2). \tag{7.20}$$

This means that w.h.p.

$$\boldsymbol{\sigma}^* \cdot \mathbf{X} \le -\Theta(Mn) \implies |\boldsymbol{\sigma}^* \cdot \mathbf{X}| \ge \Theta(Mn), \tag{7.21}$$

and we know that $d_{opt} = o(Mn)$ for every (κ, b), with $b < b_c$.

7.2 The Dual Role of b_c.

In Theorem 4.1, we proved that b_c is the threshold of the values of b for solvability of the saddle point equations (3.18). Then, in Theorem 7.1, we proved that the same b_c is also the threshold for optimality of the sorted partition. At this point, while the results are complete, the equality of these two thresholds seems to be nothing but a numerical coincidence. In this subsection, we give an explanation of this coincidence. It turns out that the coincidence reflects a *deterministic* property of the integer partitioning problem which holds for a broad set of $\mathbf{X}$, see Theorem 7.2 below.

We caution the reader that Theorem 7.2 does not directly imply the two Theorems 4.1 and 7.1. Theorem 7.2 holds only for a given instance $\mathbf{X}$, and states that for s/n greater than some $b_c(\mathbf{X})$, the sorted partition is optimal, while for $s/n < b_c(\mathbf{X})$, the saddle point equations (3.13) have an unique solution. In order to apply this theorem to the random integer partitioning problem, we would have to address two issues. First, we would have to show that if $b > b_c$, then w.h.p., $b > b_c(\mathbf{X})$. This follows in a relatively straightforward fashion using the techniques of the last subsection. The more difficult issue is to relate existence of solutions of the saddle point equations (3.13) to that of the averaged saddle point equations (3.18). This requires that we establish existence and commutation of the limits $n \to \infty$ and $s/n \to b$, and deal with the fact that nb_c is generally not an integer so that, as $b \to b_c$, the solution to the saddle point equations gives a $\boldsymbol{\sigma}$ with some σ_j in the interval $[-1, +1]$ rather than all $\sigma_j \in \{-1, +1\}$, see below. Since the coincidence is already proved in Theorems 4.1 and 7.1, and since the purpose of this section is simply to elucidate the coincidence, we do not deal with these, admittedly difficult, issues here. We just present the result for a given $\mathbf{X}$.

Consider n arbitrary numbers $X_1, \ldots, X_n \in \{1, \ldots, M\}$, subject to the constraints that no two of them are equal, and that their sum is even (the odd case is similar and is left to the reader). Without loss of generality, further assume that the X_i are ordered in increasing order, so that $X_1 < X_2 < \cdots < X_n$. Consider the equations (3.13) with $\ell = 0$, and define $s_c(\mathbf{X})$ as the supremum over all s for which the equations (3.13) have a solution.

Let $\boldsymbol{\sigma}$ be a fractional partition, i.e., let $\boldsymbol{\sigma} \in [-1, 1]^n$. We say that $\boldsymbol{\sigma}$ has bias s, if $\sum_{i=1}^{n} \sigma_i = s$, and we say that it is sorted, if $\sigma_i \leq \sigma_{i+1}$ for all i and $|\sigma_i| = 1$ for all but at most one i. Note that there is exactly one sorted partition with bias s for any real $s \in [-n, n]$. We finally introduce the *critical sorted partition* as the sorted (fractional) partition $\tilde{\boldsymbol{\sigma}}$ that obeys the condition

$$\sum_{j=1}^{n} \tilde{\sigma}_j X_j = 0. \tag{7.22}$$

There is at most one such partition for a fixed set of weights $X_1, \ldots, X_n$. With slight abuse of notation, we say that a probability distribution $\mathbb{P}(\boldsymbol{\sigma})$ on partitions is concentrated on a fractional sorted partition $\tilde{\boldsymbol{\sigma}}$ if $\mathbb{P}(\sigma_i = \tilde{\sigma}_i) = 1$ whenever $|\tilde{\sigma}_i| = 1$, and $\mathbb{P}(\sigma_i = 1) = p$ when $\tilde{\sigma}_i$ takes the fractional value $2p - 1$.

The following theorem shows that the critical bias for the existence of a solution to the random saddle point equations and the critical bias for the optimality of the fractional

sorted partition are identical. For brevity, we drop the term "fractional" throughout.

Theorem 7.2 *Let $X_1 < X_2 < \cdots < X_n \in \{1, \ldots, M\}$, and assume that the sum $\sum_{i=1}^{n} X_i$ is even.*

i) If $\ell = 0$ and $0 < s < s_c(\mathbf{X})$, then the saddle point equations (3.13) have a unique solution (ξ, η) with $-\infty < \eta < 0$, $0 < \xi < \infty$ and $|\eta|/\xi < M$.

ii) For $\ell = 0$, $s < s_c(\mathbf{X})$, and a solution (ξ, η) of the saddle point equations (3.13), let $\mathbb{P}_s(\cdot)$ be the probability distribution on partitions defined in (3.7). If $s \nearrow s_c(\mathbf{X})$, then $\xi \nearrow \infty$, $\eta \searrow -\infty$, and the distribution $\mathbb{P}_s(\cdot)$ gets concentrated on the critical sorted partition.

iii) If $\ell = 0$ and $s \geq s_c(\mathbf{X})$, then the saddle point equations (3.13) have no solution, and the sorted partition with bias s is optimal; if $s > s_c(\mathbf{X})$, this partition has non-zero discrepancy, implying that there are no perfect partitions with bias $s > s_c(\mathbf{X})$.

Remark 7.2 *Statement ii) clearly implies that the critical sorted partition has bias $s_c(\mathbf{X})$. As a consequence, a sorted partition with bias $s > s_c(\mathbf{X})$ has non-zero discrepancy. By an easy extension of the argument given for non-fractional partitions, this in turn implies that sorted partitions with bias $s \geq s_c(\mathbf{X})$ are optimal. Except for the statement that the saddle point equations (3.13) have no solution for $\ell = 0$ and $s = s_c(\mathbf{X})$, statement iii) is therefore an immediate consequence of statement ii).*

Proof of Theorem 7.2: i) Given $X_1 < X_2 < \cdots < X_n \in \{1, \ldots, M\}$, let

$$F(\xi, \eta) = \sum_{j=1}^{n} X_j \tanh(\xi X_j + \eta),$$

$$G(\xi, \eta) = \sum_{j=1}^{n} \tanh(\xi X_j + \eta). \tag{7.23}$$

Since the partial derivatives $\partial F(\xi, \eta)/\partial \xi$ and $\partial F(\xi, \eta)/\partial \eta$ are strictly positive for all $(\xi, \eta) \in \mathbb{R}^2$, the equation

$$F(\xi, \eta(\xi)) = 0 \tag{7.24}$$

has a well defined, unique solution $\eta(\xi)$ for all $\xi \in \mathbb{R}$, and $\eta(\xi)$ is strictly decreasing on $\mathbb{R}$. Let

$$g(\xi) = G(\xi, \eta(\xi)). \tag{7.25}$$

Each solution (ξ, η) of the saddle point equations (3.13) is then a solution of $g(\xi) = -s$ and $\eta = \eta(\xi)$, and vice versa. Using the fact that the derivatives of F and G are second order derivatives of the strictly convex function $L_n(\xi, \eta)$, one easily shows that $g(\cdot)$ is strictly decreasing. Combined with the fact that $\eta(0) = 0$ so that $g(0) = 0$, we easily complete that proof of i). Indeed, by the monotonicity of g, the equation $g(\xi) = -s$ has a unique solution $\xi \in (0, \infty)$ whenever

$$g(0) = 0 < s < s_c = - \lim_{\xi \nearrow \infty} g(\xi). \tag{7.26}$$

But $\xi > 0$ implies $\eta = \eta(\xi) < 0$, so we are just left with the proof of the inequality $|\eta| < \xi M$. To this end, we just observe that $F(\xi, \eta) = 0$, $\xi > 0$ and the fact that not all $X_j \in \{1, \ldots, M\}$ are equal imply that

$$0 = \sum_{j=1}^{n} X_j \tanh(\xi X_j + \eta) < \tanh(\xi M + \eta) \sum_{j=1}^{n} X_j, \tag{7.27}$$

which in turn gives $\xi M + \eta > 0$, as desired.

ii) By the strict monotonicity of g, $\xi \nearrow \infty$ as $s \nearrow s_c$ (otherwise, the equation $g(\xi) = -s_c$ would have a finite solution $\xi < \infty$, which contradicts the strict monotonicity of g on $(0, \infty)$). If $\eta = \eta(\xi)$ stayed bounded away from $-\infty$ as $\xi \nearrow \infty$, the function $F(\xi, \eta(\xi))$ would converge to the sum of the weights X_j, which is not compatible with $F(\xi, \eta(\xi)) = 0$. Thus $\eta \searrow -\infty$ as $s \nearrow s_c$. We now set $\sigma_j(\xi) = \tanh(\xi X_j + \eta(\xi))$, so that

$$F(\xi, \eta(\xi)) = \sum_{j=1}^{n} X_j \sigma_i(\xi). \tag{7.28}$$

In order to complete the proof of ii), we have to show that $\boldsymbol{\sigma}(\xi)$ converges to the critical sorted partition as $\xi \to \infty$.

To this end, we first note

$$|1 - |\sigma_j(\xi)|| \leq 2e^{-\xi}, \tag{7.29}$$

for all but at most one j. Indeed, let $X(\xi) = -\eta(\xi)/\xi$, so that $\sigma_j(\xi) = \tanh(\xi(X_j - X(\xi)))$. Let j_0 be such that $|X_{j_0} - X(\xi)|$ is minimal. Since two consecutive weights X_j, X_{j+1} differ by at least 1, we conclude that $|X_j - X(\xi)| \geq 1/2$ for all $j \neq j_0$. Together with the bound $||\tanh x| - 1| \leq 2e^{-2|x|}$ this proves (7.29) for $j \neq j_0$.

Consider now a sequence (ξ_r) with $\xi_r \to \infty$ as $r \to \infty$. By compactness, we can always find a subsequence such that $\boldsymbol{\sigma}(\xi_r)$ converges to some $\tilde{\boldsymbol{\sigma}}$. Due to (7.29), we must have that $|\tilde{\sigma}_j| = 1$ for all but at most one j. Since $F(\xi_r, \eta(\xi_r)) = \sum_j \sigma_j(\xi_r) X_j = 0$ and $\sigma_1(\xi) \leq \cdots \leq \sigma_n(\xi)$, the same holds for the limiting sequence $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_n$. As a consequence, $\tilde{\boldsymbol{\sigma}}$ is the critical sorted partition defined in (7.22) (recall that the critical sorted partition is unique). Thus any convergent subsequence of $\boldsymbol{\sigma}(\xi_r)$ converges to the critical sorted partition $\tilde{\boldsymbol{\sigma}}$, implying that $\boldsymbol{\sigma}(\xi_r)$ itself converges to $\tilde{\boldsymbol{\sigma}}$. This concludes the proof of ii).

iii) We already showed above that the equation $g(\xi) = -s_c$ has no finite solution $\xi < \infty$. As pointed out in the remark following the theorem, this is the only statement in iii) which does not follow directly from the statements in ii).

8 Relaxed Version of the Integer Partitioning Problem

It is a rather common idea to approximate an optimization problem defined with integer-valued variables by its relaxed version, where the variables are now allowed to assume any value within the real intervals whose endpoints are the admissible values of the original

integer variables. In our case, the relaxed version is a linear programming problem (LPP) which can be stated as follows. Find the minimum value d_{opt} of d, subject to linear constraints

$$-d \leq \sum_j \sigma_j X_j, \quad \sum_j \sigma_j X_j \leq d,$$

$$\sum_j \sigma_j = s, \tag{8.1}$$

$$-1 \leq \sigma_j \leq 1, \quad (1 \leq j \leq n).$$

As usual, the LPP has at least one basis solution, i.e. a solution $(\boldsymbol{\sigma}, d_{opt})$, which is an extreme (vertex) point of the polyhedron defined by the constraints (8.1). Let $N(\boldsymbol{\sigma}) := |\{j : \sigma_j \in (-1, 1)\}|$ be the number of components of $\boldsymbol{\sigma}$ which are non-integer. It is easy for the reader to verify that $N(\boldsymbol{\sigma}) \leq 2$ for all basis solutions $\boldsymbol{\sigma}$. In fact, $N(\boldsymbol{\sigma})$ cannot be 1 either, since in this case the exceptional $\sigma_{j_0} \neq \pm 1$ must be zero, which contradicts to $s \equiv n \pmod 2$. Thus, for a basis solution, $N(\boldsymbol{\sigma}) \in \{0, 2\}$. $N(\boldsymbol{\sigma}) = 0$ signals that $\boldsymbol{\sigma}$ is an optimal partition. Suppose $N(\boldsymbol{\sigma}) = 2$, and let $\{j_1, j_2\} = \{j : \sigma_j \in (-1, 1)\}$. Using the second line in (8.1), we see that

$$\sigma_{j_1} + \sigma_{j_2} \in \{-1, 0, 1\}. \tag{8.2}$$

Moreover, the second condition in (8.1), combined with $s \equiv n \pmod 2$, rules out the values ± 1. Therefore, $\{\sigma_j\}_{j \neq j_1, j_2}$ is a partition of $\{X_j\}_{j \neq j_1, j_2}$, of bias s.

Our last theorem shows that the horizontal line $b = b_c$ is a phase boundary for the LPP as well. For $b > b_c$ the solutions of the initial partition problem and of its LPP version coincide. For $b < b_c$ they are very far apart, in terms of the *ratio* of respective optimal discrepancies. To state this precisely, we introduce the fraction of basis solutions $\boldsymbol{\sigma}$ with a property that the deletion of the $N(\boldsymbol{\sigma})$ components of $\boldsymbol{\sigma}$ with values in $(-1, 1)$ produces an optimal integer partition for the remaining weights X_j. We denote this fraction by $F_n(\kappa, b)$.

Theorem 8.1 *Let* $\limsup \kappa < \infty$ *and* $0 < \liminf \kappa$.

(i) If $\liminf s/n > b_c$, *then w.h.p. the sorted partition* $\boldsymbol{\sigma}^*$ *is an unique solution of the LLP (8.1), so that in particular* $F_n(\kappa, b) = 1$ *and* $d_{opt} = \Theta(Mn)$.

   Let $\limsup s/n < b_c$.

(ii) W.h.p. $d_{opt} = 0$, *and there are* $2^{\kappa_c(b)n + O(n^{1/2} \log n)}$ *basis solutions* $(\boldsymbol{\sigma}, 0)$.

(iii) If $\liminf(\kappa - \kappa_c(b)) > 0$, *all basis solutions are fractional (i.e. have* $N(\boldsymbol{\sigma}) = 2$), *and if* $\limsup(\kappa - \kappa_-(b)) < 0$, *the number of basis solutions with* $N(\boldsymbol{\sigma}) = 0$ *is at most* $2^{(\kappa_c(b) - \kappa)n + O_p(n^{1/2})}$.

(iv) If $0 < \varepsilon < \kappa_-(b)$ *and* $\liminf(\kappa - \kappa_-(b)) > 0$, *then, w.h.p.,* $2^{-\kappa_c(b)n - \varepsilon n} \leq F_n(\kappa, b) \leq 2^{-\kappa_-(b)n + \varepsilon n}$. *If* $\limsup(\kappa - \kappa_-(b)) < 0$, *then, w.h.p.,* $F_n(\kappa, b) = 2^{-\kappa n + O(n^{1/2} \log n)}$.

Remark 8.1 *(i) As discussed in Remark 6.1 (iii), we believe that the number of optimal partitions above κ_c grows subexponentially in n. Let us assume such a bound, more precisely, assume that for $\varepsilon > 0$, for $b < b_c$, and for κ with $\liminf(\kappa - \kappa_c(b)) > 0$, we have that the number of optimal partitions is bounded by $2^{\varepsilon n}$, with probability at least $1 - o(n^{-2})$. Under this assumption, the proof of Theorem 8.1 can be easily generalized to show that, w.h.p., $2^{-\kappa_c(b)n - \varepsilon n} \le F_n(\kappa, b) \le 2^{-\kappa_c(b)n + \varepsilon n}$ whenever $b < b_c$ and $\liminf(\kappa - \kappa_c(b)) > 0$.*

(ii) If, on the other hand, one believes that the asymptotics of Theorem 5.1 hold up to κ_c, more precisely, if we assume that the bound (5.52) holds with probability at least $1 - o(n^{-2})$, whenever $b < b_c$ and $\limsup(\kappa - \kappa_c(b)) < 0$, then one can prove that, w.h.p., $F_n(\kappa, b) = 2^{-\kappa n + o(n)}$ for all (b, κ) with $b < b_c$ and $\limsup(\kappa - \kappa_c(b)) < 0$.

Proof of Theorem 8.1 and Remark 8.1. (i) Suppose $\liminf s/n > b_c$. Then w.h.p. $\sum_j \sigma_j^* X_{\pi(j)} = \Theta(Mn) > 0$, where $\boldsymbol{\sigma}^*$ is the sorted partition, so that $X_{\pi(1)} < \cdots < X_{\pi(n)}$, and

$$\sigma_j^* = \begin{cases} 1, & j \le j_n, \\ -1, & j > j_n. \end{cases} \tag{8.3}$$

Let $\boldsymbol{\sigma} \in [-1, 1]^n$ be an arbitrary relaxed partition with $\boldsymbol{\sigma} \cdot \mathbf{e} = \boldsymbol{\sigma}^* \cdot \mathbf{e}$. The proof of (1) then reduces to the proof of the statement that

$$\sum_j \sigma_j X_{\pi(j)} > \sum_j \sigma_j^* X_{\pi(j)} \quad \text{if} \quad \boldsymbol{\sigma} \ne \boldsymbol{\sigma}^*. \tag{8.4}$$

If $\boldsymbol{\sigma} \ne \boldsymbol{\sigma}^*$, then there exists a pair of indices $i < j$ such that $\sigma_i < 1$ and $\sigma_j > -1$. Assume that i is the first such index, and that j is the last such index. Since $X_{\pi(i)} < X_{\pi(j)}$, we can strictly lower the value of $\sum_j \sigma_j X_{\pi(j)}$ by raising σ_i and lowering σ_j, and preserving $\sigma_i + \sigma_j$, until at least one of them has absolute value 1, i.e. either $\sigma_i = \sigma_i^*$ or $\sigma_j = \sigma_j^*$. Repeating this procedure with the lowest i and the largest j such that $\sigma_i < 1$ and $\sigma_j > -1$ in the new configuration, we will eventually arrive at the configuration $\boldsymbol{\sigma}^*$. Since the value of $\sum_j \sigma_j X_{\pi(j)}$ was strictly lowered in each step, this proves (8.4), and thus statement (i).

(ii) Let $\limsup s/n < b_c$, and consider the partitioning problem for $\{X_j\}_{j \ge 3}$. Let $a > 0$, and set $\ell_n = \lceil Mn^{-a} \rceil$. By Theorem 6.3, we have that with probability $1 - O(e^{-\delta \log^2 n})$, there are at least $2^{n\kappa_c - O(n^{1/2} \log n)}$ tuples $\{\sigma_j\}_{j \ge 3}$ such that

$$\left| \sum_{j \ge 3} \sigma_j X_j \right| \le \ell_n. \tag{8.5}$$

We will denote the event expressed in (8.5) by $\mathcal{A}$. On the other hand, introducing the event $\mathcal{B} = \{|X_1 - X_2| > Mn^{-a_1}\}$, $a_1 \in (0, a)$, we have

$$\begin{aligned} \mathbb{P}(\mathcal{B}) &= 1 - \frac{1}{M^2} \sum_{\substack{1 \le i, j \le M \\ |i-j| \le Mn^{-a_1}}} 1 \\ &= 1 - O(n^{-a_1}). \end{aligned} \tag{8.6}$$

Introducing $\mathcal{C} = \mathcal{A} \cap \mathcal{B}$, we have then that $1 - \mathbb{P}(\mathcal{C}) \to 0$. On $\mathcal{C}$, we can define $\sigma_1 = -\sigma_2$ where

$$\sigma_1 = \frac{\sum_{j \ne 1, 2} \sigma_j X_j}{X_1 - X_2} = O(n^{-(a - a_1)}) \in [-1, 1]. \tag{8.7}$$

Clearly $\sum_{j=1}^{n} \sigma_j X_j = 0$, and denoting $\boldsymbol{\sigma} = \{\sigma_j\}_{1 \le j \le n}$, we have that $(\boldsymbol{\sigma}, 0)$ is a basis solution of the LPP. Thus w.h.p. the LPP has at least $2^{n\kappa_c - O(n^{1/2}\log n)}$ basis solutions.

Conversely, suppose $\boldsymbol{\sigma}$ is a basis solution, with $\sigma_1, \sigma_2 \in (-1, 1)$, and $\sigma_1 + \sigma_2 = 0$. Then

$$\left| \sum_{j \ge 3} \sigma_j X_j \right| \le |X_1 - X_2| \le M = o(Mn^{1/2}\log^{-1} n). \tag{8.8}$$

Again by Theorem 6.3, we know that with probability $1 - O(e^{-\delta \log^2 n})$, the total number of all such $(n-2)$-tuples with bias s is $2^{n\kappa_c + O(n^{1/2}\log n)}$, and for each such tuple, the feasible values of σ_1, σ_2 are determined uniquely. Since there are $\binom{n}{2}$ ways to select j_1, j_2 as indices of components $\sigma_j \in (-1, 1)$, and since the union of $\binom{n}{2}$ events happening with probability $1 - O(e^{-\delta \log^2 n})$ happens with probability $1 - O(n^2 e^{-\delta \log^2 n})$, we get that $2^{n\kappa_c + O(n^{1/2}\log n)}$ is also w.h.p. an upper bound on the number of basis solutions $\boldsymbol{\sigma}$ with $N(\boldsymbol{\sigma}) = 2$.

If $N(\boldsymbol{\sigma}) = 0$ then, since $b < b_c$, $\boldsymbol{\sigma}$ is a perfect partition, and thus of zero discrepancy. The number of such partitions can clearly be bounded by the number of partitions with discrepancy smaller than $\ell_n = M$. By Theorem 6.3, this is in turn bounded by $2^{n\kappa_c + O(n^{1/2}\log n)}$, completing the proof that the number of basis solutions with $N(\boldsymbol{\sigma}) = 0$ or $N(\boldsymbol{\sigma}) = 2$ is $2^{n\kappa_c + O(n^{1/2}\log n)}$.

(iii) If $\liminf(\kappa - \kappa_c(b)) > 0$ or $\limsup(\kappa - \kappa_-(b)) < 0$, we know a little bit more. In the first case, w.h.p. there are no perfect partitions, and thus no basis solutions with $N(\boldsymbol{\sigma}) = 0$. In the latter case, w.h.p. the number of perfect partitions of zero discrepancy (and thus the number of basis solutions with $N(\boldsymbol{\sigma}) = 0$) is at most $2^{(\kappa_c(b) - \kappa)n + O_p(n^{1/2})}$, which is negligible relative to $2^{\kappa_c(b)n + O(n^{1/2}\log n)}$.

(iv) If $\varepsilon > 0$ and $\liminf(\kappa - \kappa_-(b)) > 0$, then with probability $1 - O(n^2 e^{-\delta \log^2 n})$, for every subset of $(n-2)$ weights X_j, there are at most $2^{(\kappa_c - \kappa_- + \varepsilon)n}$ optimal integer partitions by Corollary 6.2. As in (ii), once the ± 1 values of the corresponding σ_j are known, the values of the two remaining σ_j are determined uniquely. So w.h.p. the LPP may have at most $\binom{n}{2} 2^{(\kappa_c - \kappa_- + \varepsilon)n}$ basis solutions with $N(\boldsymbol{\sigma}) = 2$ that have the optimal subpartition property. Similarly, the number of $\boldsymbol{\sigma}$ with $N(\boldsymbol{\sigma}) = 0$ is at most $2^{(\kappa_c - \kappa_- + \varepsilon)n}$. So for every ε, w.h.p.

$$F_n(\kappa, b) \le 2^{-\kappa_-(b)n + 2\varepsilon n}. \tag{8.9}$$

If we assume that for $\liminf(\kappa - \kappa_c(b)) > 0$, the number of optimal partitions obeys the bound $Z_{opt} \le 2^{\varepsilon n}$ with probability at least $1 - o(n^{-2})$, so that w.h.p. for every subset of $(n-2)$ weights X_j there are at most $2^{\varepsilon n}$ many optimal integer partitions, the above argument gives that for $\liminf(\kappa - \kappa_c(b)) > 0$, w.h.p.,

$$F_n(\kappa, b) \le 2^{-\kappa_c(b)n + 2\varepsilon n}. \tag{8.10}$$

Combined with the bound (8.13) below, this proves Remark 8.1.

Conversely, given j_1, j_2, with probability $1 - O(e^{-\delta \log^2 n})$ there exists at least one optimal partition $\{\sigma_j\}_{j \ne j_1, j_2}$ of the subset $\{X_j\}_{j \ne j_1, j_2}$, with discrepancy

$$\left| \sum_{j \ne j_1, j_2} \sigma_j X_j \right| \le M 2^{-\kappa_-(b)n + \epsilon n} \tag{8.11}$$

by the bound (6.64) of Theorem 6.3. Given such an optimal subpartition (and assuming that ε has been chosen smaller than $\kappa_-(b)$), with sufficiently high probability we can find an unique pair $\sigma_{j_1}, \sigma_{j_2} \in (-1, 1)$ such that $\{\sigma_j\}_{1 \leq j \leq n}$ is a basis solution of the full LPP, by solving

$$\sigma_{j_1} X_{j_1} + \sigma_{j_2} X_{j_2} = -\sum_{j \neq j_1, j_2} \sigma_j X_j,$$

$$\sigma_{j_1} + \sigma_{j_2} = 0.$$

Indeed, with probability $1 - O(e^{-\delta \log^2 n})$, the sum on the right is bounded by $M 2^{-\kappa_-(b)n + \varepsilon n}$, and with probability $1 - O(2^{-\kappa_-(b)n + \epsilon n})$,

$$|X_{j_1} - X_{j_2}| \geq M 2^{-\kappa_-(b)n + \epsilon n}. \tag{8.12}$$

Thus w.h.p. there exist at least $\binom{n}{2}$ basis solutions with the optimal subpartition property, so that

$$2^{-\kappa_c(b)n - \varepsilon n} \leq F_n(\kappa, b) \tag{8.13}$$

as long as $0 < \varepsilon < \kappa_-(b)$.

Consider finally $\limsup(\kappa - \kappa_-(b)) < 0$. Then, by Theorem 5.1, on the event "$\sum_j X_j$ is even," w.h.p. we have $2^{(\kappa_c(b) - \kappa)n + O(n^{1/2} \log n)}$ perfect partitions $\boldsymbol{\sigma}$ of discrepancy zero, each being a basis solution of the LPP with $N(\boldsymbol{\sigma}) = 0$. On the complementary event "$\sum_j X_j$ is odd", w.h.p. there are $2^{(\kappa_c(b) - \kappa)n + O(n^{1/2} \log n)}$ perfect partitions $\{\sigma_j\}_{j \neq 1, 2}$ of $\{X_j\}_{j \neq 1, 2}$, of discrepancy one, and we can find, uniquely, $\sigma_1, \sigma_2 \in (-1, 1)$ such that

$$\sigma_1 + \sigma_2 = 0, \quad \sigma_1 X_1 + \sigma_2 X_2 = -\sum_{j \neq 1, 2} \sigma_j X_j. \tag{8.14}$$

Indeed $|X_1 - X_2|$ is w.h.p. of order, say, $M n^{-a}$ at least $(a > 0)$, and the last sum is in $[-1, 1]$. Thus, regardless of the parity of $\sum_j X_j$, the LPP has w.h.p. at least $2^{(\kappa_c(b) - \kappa)n + O(n^{1/2} \log n)}$ basis solutions with the optimal subpartition property.

On the other hand, the total number of the optimal subpartition basis solutions $\boldsymbol{\sigma}$ is at most $2^{(\kappa_c(b) - \kappa)n + O(n^{1/2} \log n)}$ with probability $1 - O(n^2 e^{-\delta \log^2 n})$. Indeed, for $N(\boldsymbol{\sigma}) = 0$, $\boldsymbol{\sigma}$ is a perfect partition, and for $N(\boldsymbol{\sigma}) = 2$, the ± 1-valued σ_j form an optimal, hence perfect partition of the corresponding weights X_j. In either case, the number of corresponding perfect partitions is asymptotic to $2^{(\kappa_c(b) - \kappa)n + O(n^{1/2} \log n)}$, and $F_n(k, b) = 2^{-\kappa n + O(\sqrt{n} \log n)}$.

Finally, if we assume that the bound (5.52) holds with probability at least $1 - o(n^{-2})$, whenever $b < b_c$ and $\limsup(\kappa - \kappa_c(b)) < 0$, then the above arguments immediately give that, w.h.p., $F_n(k, b) = 2^{-\kappa n + o(n)}$. $\blacksquare$

9   Open Problems and Numerical Experiments

9.1   Open Problems

Many problems are left open in our analysis. Most important is the question of how we characterize the phase transition from the perfect phase to the hard phase. In the

unconstrained case [3], our theorems would have allowed us to give at least three equivalent definitions.

First, in the unconstrained problem, we defined the phase transition to be the point $\kappa = \kappa_c = 1$ at which the probability of a perfect partition decreases abruptly from 1 to 0. For the constrained case considered in this paper, we have proved only that such a transition occurs somewhere within the interval $(\kappa_-(b), \kappa_c(b))$. In particular, we have not proved that such a transition is sharp.

Second, in the constrained case, we could have characterized the phase transition as the point up to which the expected number of perfect partitions remains exponential, which again would have led to the value $\kappa = \kappa_c = 1$ [3]. In contrast, in the unconstrained case, here we have shown that the expected number of perfect partitions remains exponential until some $\kappa = \kappa_e(b) > \kappa_c(b)$, because up to $\kappa = \kappa_e(b)$, with vanishingly small probability, there are very many perfect partitions. Thus we cannot use the second definition in the constrained case. Alternatively, one could ask whether the *typical* (say median) number of perfect partitions changes from exponentially large to 0 at $\kappa = \kappa_c(b)$, a definition that would have given the same transition point $\kappa_c = 1$ in the unconstrained case, and that might also work here.

A third possible definition of the transition point is the point above which there is an unique optimal partition, a definition which would have again led to $\kappa_c = 1$ in the unconstrained case [3]. Here we cannot prove uniqueness until we are in the sorted phase $(b > b_c)$, far above $\kappa = \kappa_c(b)$.

A natural conjecture would be that at least the first and third definitions coincide and that both lead to a sharp transition along the line $\kappa = \kappa_c(b)$.

Assuming we could establish a sharp transition, we could then examine some other open problems. In the unconstrained problem, we were able to determine the finite-size scaling window around the transition point $\kappa = \kappa_c$, i.e. the region in which the probability of a perfect partition has nontrivial distribution. In [3], we showed that the window has width of order n^{-1}, and is centered at $\kappa_c + \Theta(n^{-1} \log n)$. In the constrained case, as discussed in Remark 2.4, the fluctuations in the number of perfect partitions should be large enough to lead to a nontrivial probability distribution within a window of width of order $n^{-1/2}$ about κ_c. Hence we expect the width of the window to be larger here than it was in the unconstrained case, at least of order $n^{-1/2}$. Our numerical experiments, reviewed in the next subsection, support this expectation.

Next, detailed estimates in the unconstrained case proved that the k smallest discrepancies (i.e., for a given set of n random integers, the k smallest absolute values of the difference in the sums of the integers in the two subsets) have a Poisson joint distribution [3]. This is the behavior that would be observed if the discrepancies of 2^{n-1} partitions (with σ_1 fixed) were independent random variables. This result confirmed the validity of the so-called Random Energy Model or REM approximation for the continuous case, proposed earlier by Mertens [18]. We have no analogous estimates for the constrained problem.

Finally, for both the constrained and unconstrained problems, it would be very useful to have theorems which establish the relevance of our phase transition results (and associated results like the Poisson joint distribution) to the complexity of the number

partitioning problem, and to the performance of widely used algorithms for the problem. In particular, is the perfect phase easy, i.e., in this phase, is it possible to find some perfect partition in polynomial time? Is the so-called hard phase actually computationally difficult (under the usual assumptions, e.g., P $\neq$ NP)? What are the changes in the behavior of commonly used algorithms at $\kappa = \kappa_c(b)$? Is $\kappa_-(b)$ an artifact of our proofs or does it reflect some change in the complexity of the problem? For example, is there a change in the (admittedly non-rigorous, but often very instructive) replica solution at $\kappa = \kappa_-(b)$? Do commonly used algorithms experience any slowdown across this curve? And finally, can our LPP results be extended to establish genuine average-case complexity results for a class of partitioning algorithms?

9.2 Numerics

In this subsection, we present some simulations which address the question of sharpness of the transition and finite-size scaling. We begin with a brief discussion of methods, then go on to finite-size effects, since this is important for the interpretation of the results. Most of our simulations concern the number of perfect partitions in the crescent-shaped region from $\kappa = \kappa_-(b)$ to $\kappa = \kappa_c(b)$.

9.2.1 Methods and Accessible System Sizes

The general experimental setup is this: generate a random instance, i.e. n random integers X_j, uniformly drawn from the interval $[1, M]$ and calculate the optimum discrepancy and the number of optimal solutions of the corresponding constrained partitioning problem. Loop over many such instances to get the *empirical* mean and the empirical standard deviation of quantities like the logarithm of the number of optimal partitions.

The numbers X_j are constructed from the output of *pseudorandom number generators*; we use LCG64, a 64 bit linear congruential random number generator from the TRNG collection [2]. It is known that the least significant bits of linear congruential recurrences are correlated, so it is dangerous to use the elements of such sequences directly as a random instance. Instead, we use a random number for *each bit* in X_j. The bits are set to 1 or 0 with probability $\frac{1}{2}$, depending on the most significant bits of the corresponding random number, thereby minimizing the influence of hidden correlations in the pseudorandom sequence. On the other hand, this restricts us to values of M that are integer powers of 2.

We can afford these extra calls to the random number generator, since the generation of the random instances is not the part of the simulation that limits the accessible system sizes. The hard part of the simulations is the solution of the particular instance. (After all, we are dealing with an NP-hard problem.) Even in the perfect phase, where a smart heuristic algorithm might find one of the exponentially many perfect partitions quickly, we want to find them all, so there is no obvious way to avoid an *exhaustive enumeration* of all partitions. The corresponding $O(2^n)$ time complexity is the limiting factor for our accessible system sizes.

Horowitz and Sahni [13] presented an algorithm that solves the unconstrained integer

partitioning problem in time $O(n \cdot 2^{\frac{n}{2}})$, and this algorithm can easily be modified to count all perfect partitions for the constrained problem within the same time complexity. The Horowitz-Sahni algorithm achieves its prodigious speed-up by dividing the set of numbers X_j in two halves and tabulating all $2^{\frac{n}{2}}$ possible discrepancies of the two half-sized sets. Each discrepancy of the original problem can then be represented by the sum or the difference of two elements, one from each table. The tables are sorted (this is the origin of the complexity $O(n \cdot 2^{\frac{n}{2}})$), and due to the monotonicity of the sorted tables, the perfect partitions of the original problem can be found with only one single scan through both lists.

The drawback of the Horowitz-Sahni algorithm is that it trades time against space. For $\kappa = 1$, the X_j's are n-bit numbers, hence the tables require $2n2^{\frac{n}{2}}$ bits of computer memory. Equipped with 512 MByte of main memory, this means $n \leq 50$. For a single instance of size $n = 50$, the optimum discrepancies for all (discrete) values of b can be found in about 4 minutes on a Pentium III CPU with 800 Mhz clock rate. Averages over 10^3 random instances can be calculated in less than half an hour using 156 CPUs of a Beowulf cluster [1]. Counting all perfect partitions in the perfect phase can take considerably longer if there are many such partitions, i.e. for small values of κ.

9.2.2   Concentration and Finite-Size Effects

For our first numerical experiment, we study the finite-size effects of the central quantity in the perfect phase, namely the number Z of perfect partitions for given b and κ.

Optimistically extending the formula (5.1) – (5.6) (Theorem 5.1), we expect that for large n

$$\mathbb{E}\Big(\frac{1}{n}\log Z\Big) \approx L(\zeta, \eta) - \kappa \log 2 - \frac{1}{n}\log\Big(\pi n \sqrt{\det R}\Big) - \frac{1}{4n}\mathrm{Tr}R^{-1}K \qquad (9.1)$$

is a valid approximation for all $\kappa < \kappa_c(b)$. It is illuminating to check accuracy of this approximation numerically, even in absence of an error term bound, better than $o(n^{-1})$, which is implicit in (9.1).

Figure 4 shows the results of the simulation. For each data point we generated 10^3 instances of n random κn-bit integers and counted the number Z of perfect partitions using the Horowitz-Sahni algorithm. Each symbol in Figure 4 denotes the empirical average over the 10^3 values of $n^{-1}\log Z$, and the error bars indicate ± 1 empirical standard deviation.

For $n \leq 50$, finite-size effects are clearly visible. On the other hand, the error bars decrease with increasing n, indicating a concentration of $n^{-1}\log Z$ around its expected value. Note that the size of the error bars does not decrease if the number of random samples increases. This indicates that the error bars are a measure of the inherent fluctuations in $n^{-1}\log Z$. Note also that for $b > 0$, the statistical fluctuations are much larger than in the $b = 0$ case, consistent with our rigorous results in Theorem B and Remark 2.4.

The most surprising observation is that Eq. 9.1 is a very good approximation for finite $n > 30$. Note that the "finite-size corrections" in Eq. 9.1, i.e. the $O(n^{-1}\log n)$-term and $O(n^{-1})$-term, are essential for a good approximation: even for $n = 50$, the measured values of $n^{-1}\mathbb{E}(\log Z)$ are about 20% below the predicted *asymptotic* values.

9.2.3 Sharpness and Location of the Perfect to Hard Transition

The major open problem with the phase diagram is the behavior of the system inside the crescent-shaped region between $\kappa = \kappa_-(b)$ and $\kappa = \kappa_c(b)$. From Theorems 5.1 and 6.1, we know that w.h.p. there are exponentially many perfect partitions for $\kappa < \kappa_-$ and no perfect partitions for $\kappa > \kappa_c$. What happens to the number of perfect partitions between $\kappa = \kappa_-$ and $\kappa = \kappa_c$? Is there a sharp transition from "no" to "exponentially many" perfect partitions, like in the unconstrained case or the case $b = 0$? If so, where does it occur?

For all numerical experiments shown in this section, we have chosen $b = 0.25$ because here the gap between $\kappa_- = 0.674\ldots$ and $\kappa_c = 0.799\ldots$ is relatively large. Setting $b = 0.25$ means that n must be a multiple of 8.

In the first experiment, we determine $\mathbb{P}_{\text{perfect}}$, the fraction of randomly generated instances that have a perfect partition. According to Theorems 5.1 and 6.2, as $n \to \infty$, this fraction should tend to 1 for $\kappa < \kappa_-$ and to 0 for $\kappa > \kappa_c$. Figure 5 shows the results for $n = 32, 40, 48$. For these finite n, the decay of $\mathbb{P}_{\text{perfect}}$ from 1 to 0 extends over an interval larger than the crescent-shaped region, but the values outside this region seem to converge to their limits 1 and 0 as n gets larger.

To see more clearly what is happening with $\mathbb{P}_{\text{perfect}}$, we define[5] $\overline{\kappa}$ by $\mathbb{P}_{\text{perfect}}(\overline{\kappa}) = \frac{1}{2}$ and plot $\mathbb{P}_{\text{perfect}}$ versus the rescaled control parameter $\Delta\kappa = (\kappa - \overline{\kappa})n^{1/2}$ for various values of n. By definition, all these curves intersect at $\Delta\kappa = 0$, but the simulation shows that the curves coincide for all values of $\Delta\kappa$ (Figure 6). This *data collapse* indicates that $\mathbb{P}_{\text{perfect}}$ is not a function of the two parameters κ and n, but of one single parameter $\Delta\kappa = (\kappa - \overline{\kappa})n^{1/2}$,

$$\mathbb{P}_{\text{perfect}}(\kappa, n) = f\big((\kappa - \overline{\kappa})n^{1/2}\big). \tag{9.2}$$

Validity of this *scaling hypothesis* in particular would imply that the transition $\mathbb{P}_{\text{perfect}} = 1$ to $\mathbb{P}_{\text{perfect}} = 0$ becomes sharp as $n \to \infty$ and that the width of the transition region scales like $O(n^{-1/2})$. The transition point $\overline{\kappa}$ itself depends on n but seems to converge to κ_c as $n \to \infty$ (see Figure 8). Our simulation results support the conclusion that the probability of a perfect partition shows a sharp transition at κ_c:

$$\lim_{n \to \infty} \mathbb{P}_{\text{perfect}} = \begin{cases} 1 & \kappa < \kappa_c \\ 0 & \kappa > \kappa_c \end{cases} \tag{9.3}$$

So far, the crescent-shaped region is not visible in the simulations, but this may change if we look at other quantities like the number of perfect partitions for $\kappa < \kappa_c$.

Figure 7 shows the result of a simulation with $n = 40$. The mean value of $n^{-1} \log Z$ is very well approximated by a piecewise linear function

$$n^{-1} \cdot \mathbb{E}\big(\log Z(\kappa)\big) = \begin{cases} (\tilde{\kappa} - \kappa)\log 2 & \kappa < \tilde{\kappa} \\ 0 & \kappa > \tilde{\kappa} \end{cases} \tag{9.4}$$

where $\tilde{\kappa}$ is a fit parameter that depends on n. Eq. 9.4 is a very accurate description of the numerical data even for rather small values of n. The value of n influences only the size

---

[5]Of course, for finite n, there is in general no solution $\overline{\kappa}$ to the equation $\mathbb{P}_{\text{perfect}}(\overline{\kappa}) = \frac{1}{2}$. Instead, we take $\overline{\kappa}_n$ to be the closest linear interpolation of solutions with parameters n and $M = 2^{\overline{\kappa}_n n}$.

of the fluctuations of $n^{-1} \cdot \log Z(\kappa)$ around its expected value and the value of $\tilde{\kappa}$. As n becomes larger, the fluctuations decrease and $\tilde{\kappa}$ increases, moving beyond κ_- and towards κ_c (see Figure 8). Note that Theorem 5.1 implies that $\lim_{n\to\infty} n^{-1} \log Z$ is linear function of κ for $\kappa < \kappa_-$.

Of course, the numerical data on $\tilde{\kappa}$ and $\overline{\kappa}$ do not allow us to conclude that both values will converge to κ_c as $n \to \infty$, but it is obvious that both values increase with increasing n and are larger than κ_-. Again we can use Theorem 5.1 to estimate the finite-size corrections to κ_c,

$$\kappa_c(n) = \frac{L(\zeta, \eta)}{\log 2} - \frac{\log\left(n\pi\sqrt{\det R}\right)}{n \log 2} - \frac{\text{Tr} R^{-1} K}{4n \log 2}. \tag{9.5}$$

Figure 8 shows that both $\overline{\kappa}$ and $\tilde{\kappa}$ are close to the finite-size estimate of κ_c.

In all our simulations, we did not find any trace of a critical line κ_-. The properties of the system do change for values below κ_c, but above κ_-, but there is some evidence that this is a finite-size effect and that for really large systems, it is only κ_c that matters.

References

[1] See http://tina.nat.uni-magdeburg.de for a description of the 156 cpu selfmade parallel computer TINA.

[2] Heiko Bauke. TRNG - a portable random number generator for parallel computing. http://tina.nat.uni-magdeburg.de/TRNG.

[3] C. Borgs, J.T. Chayes, and B. Pittel. Phase transition and finite-size scaling for the integer partitioning problem. *Rand. Struc. Alg.*, 19:247–288, 2001.

[4] C. Borgs, J.T. Chayes, and B. Pittel. Sharp threshold and scaling window for the integer partitioning problem. *Proc. 33rd ACM Symp. on Theor. of Comp.*, pages 330–336, 2001.

[5] B.Yakir. The differencing algoritm LDM for partitioning; a proof of a conjecture of Karmakar and Karp. *Math. of Operations Res.*, 21:85–99, 1996.

[6] B. Derrida. Random-energy model: An exactly solvable model of disordered systems. *Phys. Rev. B (3)*, 24:2613–2626, 1981.

[7] F.F. Ferreira and J.F. Fontanari. Probabilistic analysis of the number partitioning problem. *J. Phys. A: Math. Gen.*, 31:3417–3428, 1998.

[8] F.F. Ferreira and J.F. Fontanari. Statistical mechanics analysis of the continuous number partitioning problem. *Physica A*, 269:54–60, 1999.

[9] Y. Fu. The use and abuse of statistical mechanics in computational complexity. In *Lectures in the Science of Complexity; Proceedings of the 1988 Complex Systems*

Summer School, Santa Fe, New Mexico, 1988, edited by D.L. Stein. Addison-Wesley, Reading, MA, 1989.

[10] I.P. Gent and T. Walsh. In *Proc. of the 12th European Conference on Artificial Intelligence, Budapest, Hungary, 1996, edited by W. Wahlster*, pages 170–174. John Wiley & Sons, New York, NY, 1996.

[11] G.R. Grimmett and D.R. Stirzaker. *Probability and Random Processes.* Oxford University Press, 1992.

[12] B. Hayes. The easiest hard problem. *American Scientist*, 90:113–117, 2002.

[13] E. Horowitz and S. Sahni. Computing partitions with applications to the Knapsack problem. *Journal of the ACM*, 21(2):277–292, 1974.

[14] N. Karmarkar and R.M. Karp. The differencing method of set partitioning. Technical Report UCB/CSD 82/113, Computer Science Division (EECS), University of California, Berkeley, 1982.

[15] N. Karmarkar, R.M. Karp, G.S. Lueker, and A.M. Odlyzko. Probabilistic analysis of optimum partitioning. *J. Appl. Prob.*, 23:626–645, 1986.

[16] G.S. Lueker. Exponentially small bounds on the expected optimum of the partition and subset sum problem. *Rand. Struc. Alg.*, 12:51–62, 1998.

[17] S. Mertens. Phase transition in the number partitioning problem. *Phys. Rev. Lett.*, 81:4281–4284, 1998.

[18] S. Mertens. Random costs in combinatorial optimization. *Phys. Rev. Lett.*, 84:1347–1350, 2000.
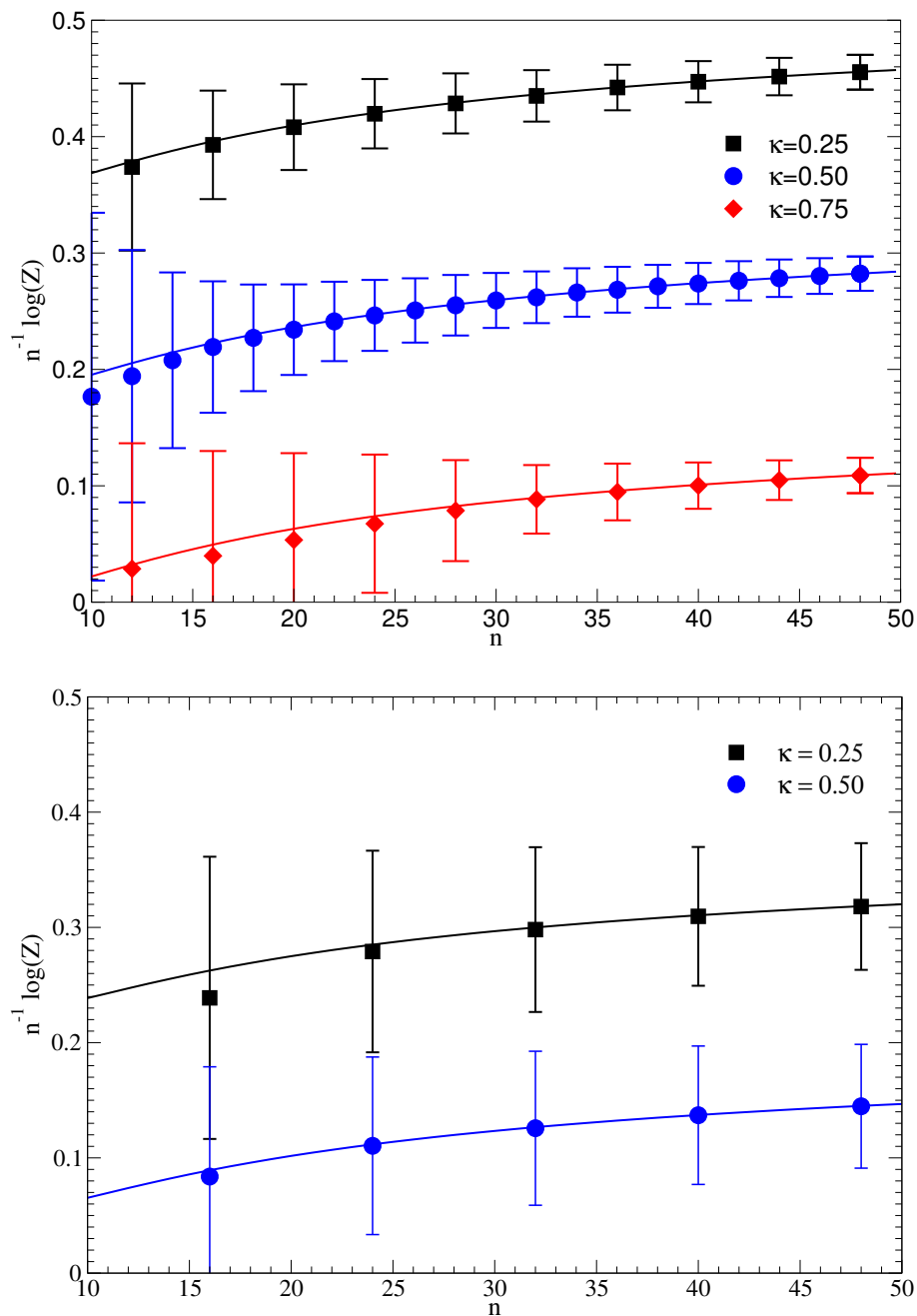
Figure 4: Comparison of eq. 9.1 (lines) for $b = 0$ (top) and $b = 0.25$ (bottom) with simulations. Symbols denote averages over 10^3 random samples of uniform numbers X, errorbars indicate ± 1 standard deviation.
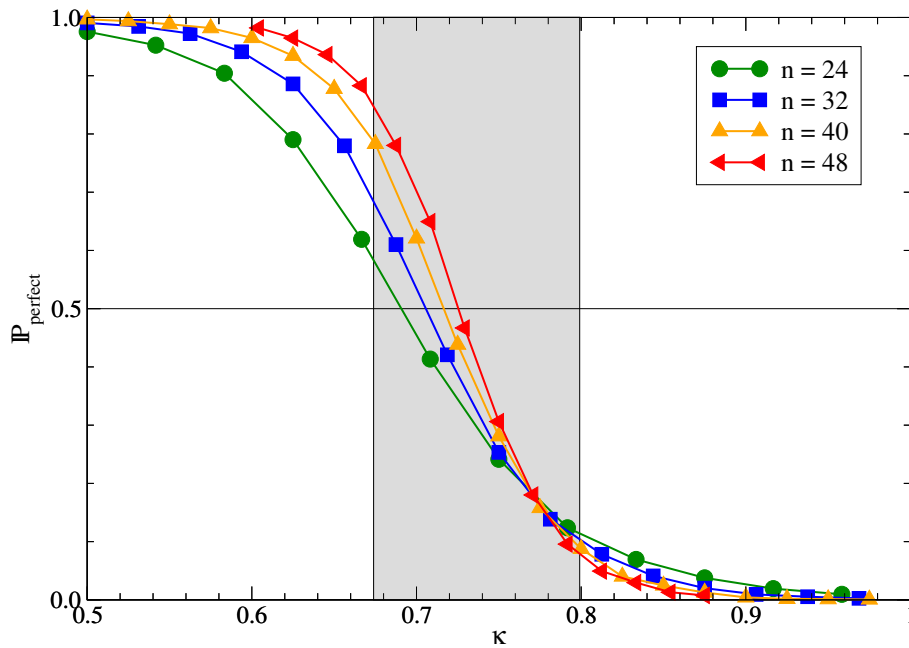
Figure 5: Probability of having a perfect partition in a random instance of the constrained partitioning problem with $b = 0.25$. Symbols are empirical probabilities found in 10^3 random samples. The shaded area is the crescent-shaped region from κ_- to κ_c.
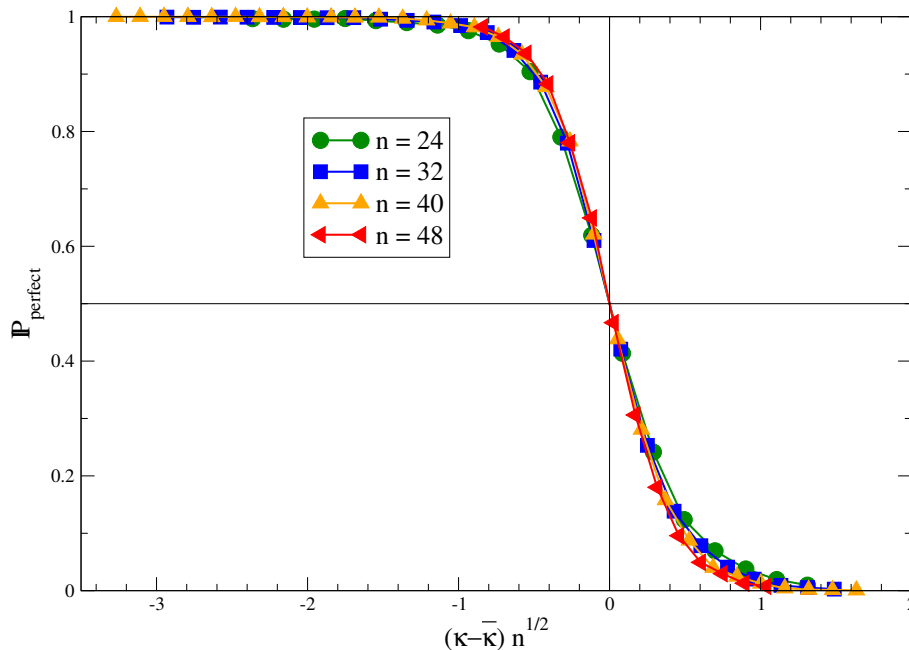

Figure 6: Same data as in Fig. 5, but this time plotted versus the scaled control parameter $\Delta\kappa = (\kappa - \overline{\kappa})n^{1/2}$. The data collapse indicates a sharp transition as $n \to \infty$ and a width $O(n^{-1/2})$ of the scaling window.
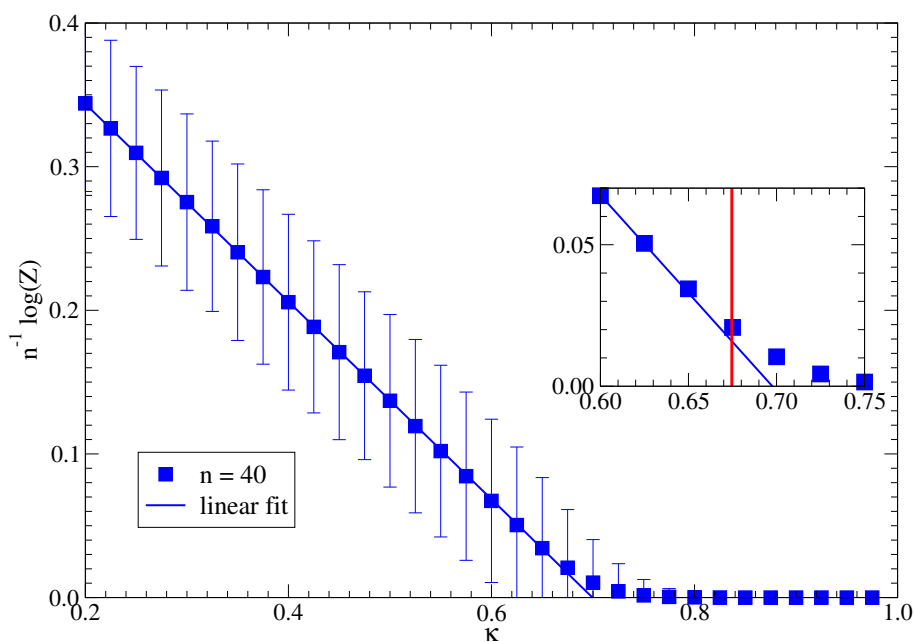
Figure 7: Logarithm of the number of perfect partitions in random instances of the constrained partitioning problem with $b = 0.25$. Symbols are averages over 10^3 random samples, errorbars indicate ± 1 standard deviation. Inset: Magnification of the "critical" region, the vertical line is κ_-.
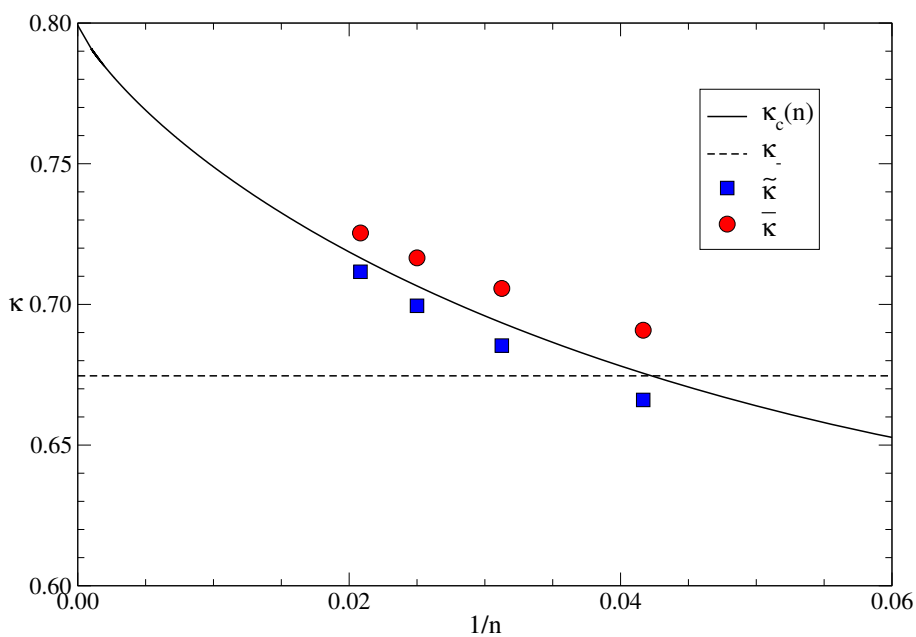

Figure 8: Values of κ that indicate a transition from the perfect to the hard phase.