Threshold results for the Inventory Cycle Offsetting Problem

Ernest Croot Department of Mathematics Georgia Institute of Technology Atlanta, GA, 30332 ecroot@math.gatech.edu

Kai Huang Department of Systems and Industrial Engineering University of Arizona Tucson, AZ, 85721 kaih@tucson.sie.arizona.edu

February 12, 2007

Abstract

In a multi-item inventory system, given the order cycle lengths and unit volumes of the items, the determination of the replenishment times (i.e. "cycle offsets") of items, so as to minimize the resources needed to store the items, is known as the inventory cycle offsetting problem. In this paper we show that so long as the cycle times and inventory unit volumes satisfy certain mild constraints, there is an assignment of replenishment times so as to keep the resource requirements near the minimum that is theoretically possible for the time interval $[0, C_1^K Q)$, where $C_1 > 1$ is a certain costant, K is the number of items, and Q is the maximum of the cycle lengths. We further prove that there is a certain constant $C_2 > C_1 > 1$ so that with high probability, the resource requirements for the time interval $[0, C_2^K Q]$ are near the worst that they could be, at least when the cycle lengths and inventory volumes are chosen randomly from certain intervals with uniform distributions. Determining the best constants C_1 and C_2 , given certain constraints, seems to be a very difficult problem, and is not something that we work out in this paper; nonetheless, at the end of the paper we present some computer experiments that suggest how C_1 depends on certain problem parameters (our experiments tell us nothing about C_2).

1 Introduction

Consider a multi item inventory system with resource capacity constraints. Assume that, for each item, the demand is constant and known, and the lead time is constant. The main constraint requires that the resource occupied at any time along a finite or infinite time horizon does not exceed a given capacity. In an inventory system, such a constraint can be imposed by the maximum number of dollars permitted to be tied up in the inventory, or by the maximum available warehouse space. The decisions to be made are the timing of the individual product replenishment times, and the quantity of each product to be delivered daily. In the literature, this problem has been addressed and under study for a long time (see, e.g., Hadley and Whitin [?], Johnson and Montgomery [?], Naddor [?], Tersine [?], Zipkin [?]).

In the unconstrained case, the problem is separable and can be solved for each item independently. However, when there exists a global resource capacity constraint, the problem becomes extremely hard. Different approaches have been proposed in the literature. The very first approach is called the Lagrangian multiplier approach (cf. Hadley and Whitin [?], Parsons 1966 [?], Johnson and Montgomery [?]). In this approach, only the order quantities are decision variables. Lagrangian multipliers are used to minimize the overall ordering cost and inventory holding cost, under the resource capacity constraint. This approach does not consider the cycle offsetting effect at all, i.e. the selection of replenishment times to minimize the maximum resource occupied along the time horizon. Therefore, in this approach, it is automatically assumed that there exist times along the horizon, such that all the items are replenished simultaneously. A second approach is called the fixed cycle approach (cf. Krone [?], Parsons 1965 [?], Homer [?], Page and Paul [?], Zoller [?], Goyal 1978 [?]), in which all the items share the same cycle. The decisions are to choose the fixed cycle length and the replenishment times for items. In Page and Paul [?], it was shown that the fixed cycle approach will always generate better space utilization (when the resource is warehouse space) than the Lagrangian multiplier approach. However, in terms of total cost, this approach is not necessarily better. In Rosenblatt and Rothblum [?], the fixed cycle approach was generalized to incorporate the case where the resource capacity is treated as a decision variable, with a general convex cost function of resource capacity utilization. By considering optimality conditions, the authors proposed an efficient algorithm to solve the problem within a fixed cycle framework.

In Rosenblatt [?], a comparison was made between the Lagrange multipliers and the fixed cycle approach, and it was shown that none of them is dominant. In Gallego et al. [?], it was shown the worst case performance of the Lagragian multiplier approach can be up to one hundred percent worse than the optimal solution. In Anily [?], it was shown the worst case performance of the fixed cycle approach can be arbitrarily bad. Thus, not surprisingly, a third approach has received a lot of attention, which is known as the basic cycle approach (cf. Goyal 1973 [?], Silver [?], Goyal and Belton [?], Kapsi and Rosenblatt [?]). In this approach, a basic cycle length is determined. The cycle of each item is a multiple of this basic cycle length. By this approach, the setup cost can be reduced due to the benefits of joint replenishment. The decision variables in this approach are the basic cycle length and the integer multiples of the basic cycle length. When the basic cycle length is given, the problem can be regarded as a partitioning problem and solved efficiently in most practical cases (cf. Chakravarty et al. 1983) [?], Chakravarty et al. 1985 [?]). In Gallego et al. [?], a variant of the basic cycle approach was proposed, where the cycle lengths of items are set to be power of two times of basic cycle length. In Hariga and Jackson [?], a similar approach was discussed.

In most of the basic cycle approach papers, there is very little discussion of the cycle offsetting problem; it is usually assumed that there exists times along the horizon, such that the overall resource occupied is just the sum of the maximum resource occupations of individual items. This may be due to the difficulty of solving the cycle offsetting problem as a subproblem. In Gallego et al. [?], it was shown that the cycle offsetting problem is NPcomplete. In Goyal 1978 [?], a heuristic was proposed to incorporate the cycle offsetting with a fixed cycle approach. Then in Hall [?], the author considered the separate replenishment policy for two items, where the cycle time of one item is defined as the basic cycle, and the other item's cycle length is an integer multiple of this basic cycle. The optimal offsetting solution for this special case was derived. Later in Murphy et al. [?], the general two item cycle offsetting problem was solved. By using modular arithmetic, a closed form of the optimal solution was obtained. Furthermore, the authors also showed that cycle offsetting can increase resource utilization by as much as fifty percent, which implies that it is very necessary to consider the cycle offsetting effect when resources are limited. To conclude, in previous research on the inventory cycle offsetting problem, the two item case was solved, while for the case of large number of items, only a few heuristics exist.

In this paper we will prove a certain "coarse threshold" result, which says the following

• if the time horizon is at most $C_1^K Q$ (for a certain $C_1 > 1$), where Q is the maximum of the cycle lengths q_1, \ldots, q_K , and if the volumes d_i and cycle lengths q_i satisfy some fairly mild and natural constraints, then there is always a way to schedule the deliveries so as to keep the resources constraints close to the minimum that is theoretically possible; and,

• for most instances of the inventory capacity problem of a certain type (where the cycle lengths q_i and volumes d_i are chosen randomly from uniform distributions over certain intervals), if the time horizon is larger than $C_2^K Q$ for a certain constant $C_2 > C_1 > 1$, then with high probability, no matter what cycle offsetting is used, the resource requirements will be near the worst that is possible.

Notice that in the first bullet there is no randomization or probability involved – randomization only appears when working with the upper bound $C_2^K Q$.

One would like to be able to prove that M_N has a "sharp threshold", which would mean that the resource requirements are near the smallest that is theoretically possible for $N \leq (C-o(1))^K Q$, while the resource requirements are near the largest they could be when $N \geq (C + o(1))^K Q$. We strongly believe, however, that this is not the case – that is, we believe M_N does not have a sharp threshold. This can perhaps be proved using the methods in our paper, though we have not bothered to do so.

Although we do not not give good estimates for these constants C_1 and C_2 , as this is a very technical and delicate mathematical problem, in section 7

we experimentally determine (heuristic) lower bounds for C_1 , assuming that the cycle times and inventory volumes are randomly selected according to uniform distributions over certain intervals.

2 The Inventory Cycle Offsetting Problem (ICP)

2.1 Problem Statement

The statement of the inventory cycle offsetting problem is simple: Consider multiple items in joint storage, whose inventory cycles are given. A resource is occupied or consumed when items are stored. The resource can be the amount of dollars invested in inventory, or the warehouse space, etc. The decision problem is to decide the replenishment times of items, to minimize the overall resource utilization along a given time horizon (finite or infinite). In this problem, we assume that for each time period, the demand for each item is constant and known. We also assume that the replenishment is immediate (this assumption can be simply extended to the case of constant lead time). To describe the mathematical model, we introduce the following notations:

- K : the number of items
- k : index for items
- d_k : volume of a unit of item k consumed or occupied in unit time
- q_k : inventory cycle of item k
- δ_k : replenishment time for item k (decision variable), $0 \leq \delta_k < q_k$

Within a basic cycle framework (cf. Murphy et al. [?]), we can assume q_k and δ_k are integers. The parameter d_k is an estimation of resource occupation for item k consumed in unit time. It can be regarded as the multiplication of demand rate and the consumption of resource for each unit of item k. For example, let the resource be warehouse space. The demand rate of item k is 2 units per day. And each unit has a volume of 4 cubic feet. Then the d_k value will be $2 \times 4 = 8$.

Define the following function for each item k:

$$f_k(t) = q_k - t \quad \forall 0 \le t < q_k. \tag{1}$$

Then, we periodize by defining for each integer t,

$$f_k(t) = f_k(t + hq_k),$$

where h is the unique integer such that $0 \le t + hq_k < q_k$. Thus, the inventory cycle offsetting problem can be expressed as follows:

Efficiently determine

$$M_N(q_1,...,q_K;d_1,...,d_K) := \mathop{\mathrm{Min}}_{\delta_1,\delta_2,...,\delta_K} \mathop{\mathrm{Max}}_{0 \le t \le N-1 \atop t \in \mathbb{Z}} \sum_{k=1}^K d_k f_k(t+\delta_k),$$

and determine a choice for $\delta_1,...,\delta_K$ where this Minimum-Maximum is attained.

3 Summary of Results

3.1 Basic Bounds

Our first observation is the following theoretical lower bound.

Theorem 1 For $L = \operatorname{lcm}(q_1, ..., q_K)$ we have that

$$M_L(q_1, ..., q_K; d_1, ..., d_K) \geq \frac{d_1(q_1+1) + \dots + d_K(q_K+1)}{2}.$$

Proof. Note that the average value of the periodic function $d_k f_k(t + \delta_k)$ in a full cycle is

$$\frac{d_k(1+\cdots+q_k)}{q_k} = \frac{d_k(q_k+1)}{2}.$$

Since q_k divides L, we can easily see that the average value of $S(t; \delta_1, ..., \delta_K)$ over $0 \le t \le L - 1$ is

$$\frac{d_1(q_1+1) + \dots + d_K(q_K+1)}{2}$$

Therefore, the resource capacity should be at least this big, no matter what phases $\delta_1, ..., \delta_K$ are chosen. This is just what the theorem is claiming. \Box

As the quantity appearing on the right-hand-side of this theorem comes up many times, we give it a name: Let

$$B = B(q_1, ..., q_K; d_1, ..., d_K) := \frac{d_1(q_1+1) + \dots + d_K(q_K+1)}{2}.$$
 (2)

By a slightly longer argument we can further prove that M_N approximately satisfies such a bound, where N is a small factor of the largest q_k ; specifically, we have:

Theorem 2 Suppose that

$$N \geq h \max_{1 \leq k \leq K} q_k$$
, with $h \geq 2$.

Then,

$$M_N(q_1, ..., q_K; d_1, ..., d_K) \geq \left(1 - \frac{2}{h}\right) B,$$

where B is as in (2).

Proof. For each k = 1, ..., K write

$$N = s_k q_k + r_k$$
, where $0 \le r_k \le q_k - 1$.

We observe that $s_k = [N/q_k] \ge h$, and therefore for any δ_k ,

$$\frac{1}{N}\sum_{n=0}^{N-1} d_k f_k(n+\delta_k) = \frac{1}{s_k q_k} \sum_{n=0}^{s_k q_k} d_k f_k(n+\delta_k) + E_k = \frac{d_k(q_k+1)}{2} + E_k.$$

where the error E_k satisfies

$$E_k = \left(\frac{1}{N} - \frac{1}{s_k q_k}\right) \sum_{n=0}^{s_k q_k - 1} d_k f_k(n + \delta_k) + \frac{1}{N} \sum_{n=s_k q_k}^{N-1} d_k f_k(n + \delta_k).$$

The first term in this error E_k is smaller than

$$\frac{r_k d_k s_k (1+2+\dots+q_k-1)}{N s_k q_k} < \frac{d_k (q_k+1)}{2 s_k} \le \frac{d_k (q_k+1)}{2 h}.$$

The second term in the error E_k is smaller than

$$\frac{d_k(1+2+\dots+q_k)}{q_k s_k} = \frac{d_k(q_k+1)}{2s_k} \le \frac{d_k(q_k+1)}{2h}$$

Putting these errors together we deduce that

$$|E_k| < \frac{d_k(q_k+1)}{h};$$

and so, it follows that for all $\delta_1, ..., \delta_K$,

$$\left| B - \frac{1}{N} \sum_{n=0}^{N} \sum_{k=1}^{K} d_k f_k(n+\delta_k) \right| < \frac{2B}{h}.$$

The theorem follows because from this we know that the maximum value of this double sum is at least its average value, which is at least

$$B - \frac{2B}{h} = \left(1 - \frac{2}{h}\right)B.$$

So, from these simple results we know that M_N must be at least half its largest possible value (which is $d_1q_1 + \cdots + d_Kq_K$), even when N is not too large; for example, we have that if $N > 40 \operatorname{Max}_k q_k$, then

$$0.45(d_1(q_1+1) + \dots + d_K(q_K+1)) < M_N \leq d_1q_1 + \dots + d_Kq_K.$$

As mentioned in the previous sections, this leads one to ask: For what values of $q_1, ..., q_K$ and $d_1, ..., d_K$ and N, can we guarantee that M_N is close to B? And, for which values of parameters is M_N near to $d_1q_1 + \cdots + d_Kq_K$, the worst it could be?

3.2 Statments of Main Results

In the next two sections we will prove the following two theorems which partially address these questions.

Theorem 3 For every $\delta \geq \epsilon > 0$, there exists a constant $C_1 = C_1(\epsilon, \delta) > 0$, such that the following holds for $K > K_0(\epsilon, \delta)$ and $Q > Q_0(\epsilon, \delta)$: Let

$$1 \leq q_1, \dots, q_K \leq Q := \max_i q_i$$

be any set of integer phases, and let

$$0 \leq d_1, d_2, ..., d_K \leq D$$

be any set of unit volumes satisfying

$$B(q_1, \dots, q_K; d_1, \dots, d_K) \geq \delta KQD. \tag{3}$$

(See the remark below as to why this bound on B is a natural assumption.) Then,

$$M_N(q_1, ..., q_K; d_1, ..., d_K) \leq (1 + \epsilon) B$$
, for all $N \leq C_1^K Q$. (4)

Although our proof does not give good lower bounds for the best constant C_1 here, it at least gives us that we may take it to be any positive real number smaller than

$$\exp(\epsilon^2 \delta^2/2).$$

Remark. Observe that we are asserting that the conclusion holds for any set of integer phases $q_1, ..., q_K$ – there is no randomization at all. The proof, however, makes use of a probabilistic argument.

Also observe that the requirement (3) is fairly mild, when viewed through the appropriate lens: Pretend that the q_i and d_i are independent random variables that are uniformly distributed over $\{1, 2, ..., Q\}$ and [0, D], respectively. Then, (3) holds with probability 1 - o(1) (here, the o(1) tends to 0 as $K \to \infty$); and, in fact, it holds with $\delta = 1/8$. Actually, we have something even better, namely that (3) will hold for some value of $\delta > 0$ with probability 1 - o(1) just so long as the values $\mathbb{E}(q_1)$ and $\mathbb{E}(d_1)$ are more than a constant multiple of Q and D, respectively, regardless of whether or not the distributions are uniform.

Theorem 4 The following holds for Q sufficiently large: If

$$K_0 < K \leq \frac{\log(Q/33)}{6\log(41)}$$
, for a certain $K_0 > 0$,

and if we

• select integers $1 \leq q_1, ..., q_K \leq Q$ independently at random from uniform distributions, and

• select $0 < d_1, ..., d_K \leq D$ at random (they need not be integers) from uniform distributions (independent of the values of the q_i and from the other d_i),

then, with probability at least 90%,

 $M_N(q_1, ..., q_K; d_1, ..., d_K) \geq 0.90(d_1q_1 + \dots + d_kq_k), \text{ for all } N \geq C_2^K Q.$ (5)

Although our proof does not give us precise upper bounds on the size of this constant C_2 , it at least shows that for K sufficiently large, we may take

 $C_2 < 5.22 \times 10^8$,

which is clearly much too large to be useful in practical problems.

Remark. We could give a more precise theorem here, where the two numbers 90% and 0.9 are replaced with numbers arbitrarily close to 1, and where the constant C_2 depends on these numbers; however, the theorem as it is presently stated is good enough to describe the rough behavior of $M_N(q_1, ..., q_K; d_1, ..., d_K)$.

Taken together, these two theorems, along with Theorem 2, tell us that M_N "typically" undergoes a phase transition: if

$$Q \ll N \leq C_1^K Q, \tag{6}$$

then M_N is near B, roughly the smallest it could be; and, if

$$C_2^K Q \leq N, \tag{7}$$

then M_N is near $d_1q_1 + \cdots + d_Kq_K$, which is the largest it could be.

Left unanswered is the question of just what the optimal constants C_1 and C_2 are. The methods that go into the proofs of Theorems 3 and 4 l are too weak to answer this question (especially Theorem 4, where we only know that $C_2 < 5.22 \times 10^8$); however, if one is interested in knowing this dependence for practical considerations (actually solving instances of ICP computationally), and if one does not care about being mathematically certain of exactly what this dependence is, then one can perform some large computations on random data sets to determine the dependence. In section 7 we present some computer experiments which give heuristic lower bounds for C_1 if the numbers $q_1, ..., q_K$ and $d_1, ..., d_K$ are randomly chosen over certain intervals with the uniform distribution. Our computations tell us nothing about C_2 .

One final point worth making, before we close this section and proceed with the proofs of the above theorems, is that the requirement $K \ll \log Q$ in Theorem 4 can probably be substantially weakened; however, it cannot be weakened to something like $K \ll Q$, because if K is near cQ, then there will likely be lots of pairs of the q_i that are equal, and when that occurs it is possible to choose the phases $\delta_1, ..., \delta_K$ so as to keep M_N from ever being near its largest value $d_1q_1 + \cdots + d_Kq_K$.

4 Proof of Theorem 3

First, we will need the following theorem of Hoeffding (see [?] or [?, Theorem 5.7]):

Proposition 1 Suppose that $z_1, ..., z_r$ are independent real random variables with $|z_i| \leq 1$. Let $\mu = \mathbb{E}(z_1 + \cdots + z_r)$, and let $\Sigma = z_1 + \cdots + z_r$. Then,

$$\mathbb{P}(|\Sigma - \mu| > rt) \leq 2\exp(-rt^2/2).$$

The way we use this proposition is as follows: Given $q_1, ..., q_K$, and $d_1, ..., d_K$, select the phases $\delta_1, ..., \delta_K$ independently and uniformly at random with $0 \leq \delta_i \leq q_i - 1$. We wish to give a lower bound for the probability that

for all $t = 0, ..., N - 1, d_1 f_1(t + \delta_1) + \dots + d_K f_K(t + \delta_K) \leq (1 + \epsilon) B.$

We can regard this as a question about the N events $E_0, ..., E_{N-1}$, where E_i is the event that

$$d_1 f_1(i+\delta_1) + \dots + d_K f_K(i+\delta_K) \leq (1+\epsilon)B.$$

An especially important property of these events E_i is that they enjoy a "weak continuity" property, and this property is what leads to the factor of Q appearing in (4) for the range $C_1^K Q$. This weak continuity property is given by the following lemma: Lemma 1 Let

$$S(t;\delta_1,...,\delta_K) = \sum_{k=1}^K d_k f_k(t+\delta_k).$$

Then, we have that

$$S(t-u;\delta_1,...,\delta_K) \leq u \sum_{k=1}^K d_k + S(t;\delta_1,...,\delta_K).$$

Proof. The proof amounts to observing that

$$f_k(t-u;\delta_1,...,\delta_K) \leq f_k(t;\delta_1,...,\delta_K) + u,$$

and then plugging in such inequalities to the sum $S(t-u; \delta_1, ..., \delta_K)$.

From this lemma we can deduce that in order for $E_0, ..., E_{N-1}$ to hold, it suffices that a certain shorter list of events $F_1, ..., F_H$ all hold, where

$$H = 1 + [3N/\epsilon\delta Q]$$

and F_j is the event

$$|S([\epsilon \delta j Q/3]; \delta_1, ..., \delta_K) - B| < \epsilon B/2.$$

To see that this implies that $E_0, ..., E_{N-1}$ all hold, suppose that $0 \le t \le N-1$. Then,

$$[\epsilon \delta(j-1)Q/3] < t \leq [\epsilon \delta jQ/3], \text{ for some } 1 \leq j \leq H.$$

Now, from Lemma 1 we deduce that

$$S(t; \delta_1, ..., \delta_K) \leq S([\epsilon \delta j Q/3]; \delta_1, ..., \delta_K) + (1 + \epsilon \delta Q/3) \sum_{i=1}^K d_i$$

$$\leq B(1 + \epsilon/2) + (1 + \epsilon \delta Q/3) DK$$

$$\leq B(1 + \epsilon/2) + DK + \epsilon \delta QDK/3$$

$$\leq B(1 + \epsilon/2) + DK + \epsilon B/3$$

$$< B(1 + \epsilon),$$

for $Q > Q_0(\epsilon, \delta)$ and $K > K_0(\epsilon, \delta)$.

Now, since $F_i \subseteq E_i$, we have

$$\mathbb{P}(E_0 \cap \dots \cap E_{N-1}) \geq \mathbb{P}(F_1 \cap \dots \cap F_H) \geq 1 - \sum_{i=1}^H \mathbb{P}(\overline{F_i}).$$

In order to give a lower bound on this last quantity, we must bound $\mathbb{P}(F_i)$ from below. To do this, given that we already know $d_1, ..., d_K, q_1, ..., q_K$, but that we let $\delta_1, ..., \delta_K$ vary, we define the random variables $\Sigma_0, ..., \Sigma_{N-1}$ by the relation

$$\Sigma_i = (d_1/QD)f_1(i+\delta_1) + \dots + (d_K/QD)f_K(i+\delta_K).$$

Each of these Σ_i is a sum of independent random variables, say

$$\Sigma_i = X_1 + \dots + X_K$$
, were $X_k = (d_k/QD)f_k(i+\delta_k)$,

and by dividing through by QD we have forced them to be bounded from above by 1, so that Hoeffding applies; indeed, we have that

$$\mathbb{P}(F_i) = \mathbb{P}(|B/QD - \Sigma_i| \le \epsilon B/QD) > 1 - 2\exp(-\epsilon^2 B^2/2KQ^2D^2).$$

So,

$$\mathbb{P}(E_0 \cap \dots \cap E_{N-1}) > 1 - 2H \exp(-\epsilon^2 B^2 / 2KQ^2 D^2).$$

This probability is positive, provided

$$2H < \exp(\epsilon^2 B^2 / 2KQ^2 D^2).$$

Using (3) we see that this holds provided

$$2H < \exp(\epsilon^2 \delta^2 K/2).$$

Using the fact that $H = 1 + [3NK/\epsilon\delta Q]$, we have that our inequality holds provided

$$N < \frac{\epsilon \delta Q}{6} \exp(\epsilon^2 \delta^2 K/2) - \frac{\epsilon \delta Q}{3}.$$

This right-most-quantity is bounded from above by $C_1^K Q$ for large K and for some C_1 that depends only on ϵ and δ ; in fact, for large K we may take C_1 to be any constant exceeding

$$\lim_{K \to \infty} \left(\frac{\epsilon \delta}{6} \exp(\epsilon^2 \delta^2 K/2) - \frac{\epsilon \delta}{3} \right)^{1/K} = \exp(\epsilon^2 \delta^2/2).$$

Our theorem is proved.

5 Proof of Theorem 4

5.1 An Approximate Chinese Remainder Theorem

The time horizons N around where M_N is "large" turns out to be related to the parameter

$$s = s(q_1, ..., q_K; R) := \underset{\substack{(m_1, ..., m_K) \in \mathbb{Z}^K \\ |m_k| \le R \\ (m_1, ..., m_K) \neq (0, ..., 0)}}{\min} \left\| \left| \frac{m_1}{q_1} + \dots + \frac{m_K}{q_K} \right| \right|, \qquad (8)$$

where ||x|| denotes the distance from x to the nearest integer.

The connection between this parameter s and the number M_N is through an approximate version of the Chinese Remainder Theorem. Basically, we will use some elementary harmonic analysis to prove that given $\epsilon > 0$, for a certain R > 0, if s is "not too small" (in a way that depends on ϵ), then for N "not too large", for any choice of intervals (which amounts to a choice of $a_1, ..., a_K$)

$$I_1 := [a_1 - \epsilon q_1, a_1 + \epsilon q_1], \ I_2 := [a_2 - \epsilon q_2, a_2 + \epsilon q_2], \ \dots, \ I_K := [a_K - \epsilon q_K, a_K + \epsilon q_K],$$

there exists a number $0 \le n \le N-1$ such that for "most" j = 1, ..., K we will have n is congruent mod q_j to some number in the interval I_j . If this is the case, then no matter how we choose phases $\delta_1, ..., \delta_K$, it will turn out that $M_N(q_1, ..., q_K; \delta_1, ..., \delta_K)$ is "large".

If these intervals had $\epsilon = 0$, then they would just be the points $I_1 = \{a_1\}, ..., I_K = \{a_K\}$. If the $q_1, ..., q_K$ were coprime, then by the Chinese remainder theorem there would exist $n \leq \operatorname{lcm}(q_1, ..., q_K)$ satisfying $n \equiv a_i \pmod{q_i}$; therefore, n lies in the interval $I_i \mod q_i$. In our approximate version of the Chinese remainder theorem we do not need so strong a requirement as that the $q_1, ..., q_K$ are coprime, as it turns out that for "most" choices of $q_1, ..., q_K \leq Q$, the parameter s is "not too small", at least when

$$1 \leq K \ll \log Q.$$

Furthermore, the *n* that lies mod q_j in the interval I_j , for all j = 1, ..., K, will typically be much much smaller than $lcm(q_1, ..., q_K)$.

5.2 The connection between s and M_N

Rather than state the approximate Chinese Remainder Theorem as a seperate theorem, and then apply it, we will integrate it directly into the proof of the following theorem, which is all we really need for the proof of Theorem 4:

Theorem 5 Suppose $0 < \epsilon_1 < 1/2$, and suppose that $q_1, ..., q_K \ge 2$. Let $R \ge 1$ satisfy

$$\frac{R}{\log(4R) + \log 16} > \frac{27}{16\epsilon_1^3}.$$
(9)

If $s \neq 0$, then for

$$N \geq \frac{K \log(4R) + \log 16}{2s}$$

we have that

$$M_N(q_1, ..., q_K; d_1, ..., d_K) \geq (d_1 q_1 + \dots + d_K q_K) - K \max_k d_k (\epsilon_1 q_k + 1).$$
(10)

In order to relate this theorem to Theorem 4, we need a way to bound $s(q_1, ..., q_K; R)$ from below for almost all $q_1, ..., q_K \leq Q$, for a particular value of R. The following lemma is a step towards this:

Lemma 2 Suppose that $m_1, ..., m_n$ is a sequence of integers, not all 0, and suppose that $x_1, ..., x_n$ are chosen independently and uniformly at random from among the integers in [1, Q]. Then, the probability that

$$\left|\frac{m_1}{x_1} + \dots + \frac{m_n}{x_n}\right| < \epsilon_2 \tag{11}$$

is at most

$$\frac{1 + 2\epsilon_2 Q^2 / \operatorname{Max}_j |m_j|}{Q}.$$

Proof of the Lemma. Without loss of generality, assume that $|m_n|$ is maximal among the list $|m_1|, ..., |m_n|$.

Let E be the event (11). We first consider the probability

$$P = \mathbb{P}(y_1, ..., y_{n-1}) = \mathbb{P}(E \mid x_1 = y_1, x_2 = y_2, ..., x_{n-1} = y_{n-1})$$

This is the same as the probability that m_n/x_n lies in a certain interval of width 2ϵ ; specifically,

$$\frac{m_n}{x_n} \in -\left(\frac{m_1}{x_1} + \dots + \frac{m_{n-1}}{x_{n-1}}\right) + [-\epsilon_2, \epsilon_2].$$

This probability is maximal (the greatest number of x_n satisfy it) when

$$\frac{m_1}{x_1} + \dots + \frac{m_{n-1}}{x_{n-1}} = -\frac{m_n}{Q} - \epsilon_2,$$

in which case E holds whenever

$$\frac{1}{Q} \leq \frac{1}{x_n} < \frac{1}{Q} + \frac{2\epsilon_2}{|m_n|};$$

that is,

$$\frac{Q}{1+2\epsilon_2 Q/|m_n|} < x_n \leq Q$$

The width of this last interval is at most $2\epsilon_2 Q^2/|m_n|$. So,

$$P \leq \frac{1 + 2\epsilon_2 Q^2 / |m_n|}{Q}.$$

So,

$$\mathbb{P}(E) = \sum_{\substack{1 \le y_1, \dots, y_{n-1} \le Q \\ \leq \ \frac{1 + 2\epsilon_2 Q^2 / |m_n|}{Q}}, \mathbb{P}(x_1 = y_1, \dots, x_{n-1} = y_{n-1}) \mathbb{P}(E|x_1 = y_1, \dots, x_{n-1} = y_{n-1})$$

as claimed.

Before we apply this lemma, we first consider the following question: Given $q_1, ..., q_K$ and $R \ge 1$, how small would we expect $s(q_1, ..., q_K; R)$ to be in absolute value? Well, there are, in total, $(2R + 1)^K - 1$ sequences $(m_1, ..., m_K) \ne (0, ..., 0)$ and each of the sums

$$\frac{m_1}{q_1} + \dots + \frac{m_K}{q_K}$$

must be smaller than KR/Q in absolute value; and, if these $(2R+1)^{K}-1$ sums were uniformly distributed in [-KR/Q, KR/Q], then we would expect that the smallest sum in absolute value has size about $(2KR/Q)(2R+1)^{-K}$. So, for example, we would expect that it is fairly unlikely that for any sequence of $(m_1, ..., m_K) \neq (0, ..., 0)$,

$$\left|\frac{m_1}{q_1} + \dots + \frac{m_K}{q_K}\right| < \frac{\delta}{Q(2R+1)^K},\tag{12}$$

once $\delta > 0$ is small enough. Our lemma above will allow us to say how unlikely: First, let $\epsilon_2 = \delta Q^{-1} (2R+1)^{-K}$. Then, from Lemma 2, each particular sequence $(m_1, ..., m_n) \neq (0, ..., 0)$ satisfies (12) with probability at most

$$\frac{1+2\delta Q(2R+1)^{-K}}{Q} = \frac{2\delta}{(2R+1)^{K}} + \frac{1}{Q}.$$

So, the probability that at least one of the $(2R+1)^{K}-1$ sequences $(m_1, ..., m_K) \neq (0, ..., 0)$ satisfies (12) is at most

$$2\delta + \frac{(2R+1)^K}{Q}.$$

So, just as we predicted, by choosing $\delta > 0$ very near to 0, we have that this will be unlikely, provided that $(2R + 1)^K$ is appreciably smaller than Q; in fact, assuming that

$$K < \frac{\log Q + \log \delta}{\log(2R+1)}$$

we will have that this probability is smaller than 3δ .

Given some $0 < \epsilon_1 < 1/2$, let $R \ge 500$ be the minimal integer that satisfies (9); this will mean that

$$\frac{27}{16\epsilon_1^3} < \frac{R}{\log(4R) + \log 16} < \frac{2}{\epsilon_1^3}.$$
(13)

With a little work one can check that

$$\log(2R+1) < 2\log\left(\frac{R}{2(\log(4R) + \log 16)}\right) < 2\log(1/\epsilon_1^3);$$

and so, we get that the probability of (12) holding for some $(m_1, ..., m_K) \neq (0, ..., 0)$, all $|m_i| \leq R$, is smaller than 3δ , provided that

$$K < \frac{\log Q + \log \delta}{2\log(1/\epsilon_1^3)} < \frac{\log Q + \log \delta}{\log(2R+1)}.$$

Combining this with Theorem 5, and choosing $\delta = 1/33$ and $\epsilon_1 = 1/41$, we have

Claim. If $1 \leq q_1, ..., q_K \leq Q$ are chosen at random, where

$$K_0 < K < \frac{\log(Q/33)}{6\log(41)},$$
 (14)

then with probability at least $1-3\delta \approx 91.1\%$ we will have that for R satisfying (13),

$$s(q_1, ..., q_K; R) \geq \frac{1}{33Q(2R+1)^K},$$

and therefore by Theorem 5, we deduce that for

$$N \geq (33/2)Q(2R+1)^{K}(K\log(4R) + \log 16) \geq \frac{K\log(4R) + \log 16}{2s},$$

we have that for Q sufficiently large

Note that these expectations that appear in these last two inequalities is a consequence of the fact that the d_i and q_i are chosen independenly and uniformly from sets [0, D] and $\{1, ..., Q\}$, respectively.

We can further refine this last inequality: We have by the Law of Large Numbers that for K sufficiently large, the sum

$$d_1q_1 + \cdots + d_Kq_K$$

lies near to $K\mathbb{E}(q_1)\mathbb{E}(d_1)$; in particular, we will have that we can replace the lower bound in (15) with

$$M_N \geq 0.9(d_1q_1 + \dots + d_Kq_K);$$

and, under the same assumptions that went into our claim above – in particular, (14) – we will have that this inequality on M_N holds with probability at least 90%.

For large values of K this range on N has the general form $C_2^K Q$, where C_2 is roughly 2R + 1. To be more precise, we have that since

$$\lim_{K \to \infty} \left(2(2R+1)^K (K \log(4R) + \log 16) \right)^{1/K} = 2R + 1,$$

then for any $\gamma > 0$ and K sufficiently large we will have that (15) holds for $N > (2R + 1 + \gamma)^K Q$. This clearly implies our theorem, and so we are done

once we prove Theorem 5. In order to translate this bound on C_2 into a numerical value, we observe from (13) that we must solve

$$\frac{R}{\log(4R) + \log 16} = \frac{2}{\epsilon_1^3} = 482447,$$

and using Maple we find that this satisfies

$$R < 2.61 \times 10^8$$
.

So, for K and Q sufficiently large we may take

$$C_2 < 5.22 \times 10^8.$$

6 Proof of Theorem 5

In this section we will prove Theorem 5 using the following technical proposition, and two of its corollaries.

Proposition 2 Suppose $R \ge 1$, and suppose that $q_1, ..., q_K \ge 2$. If s is as defined in (8), and $s \ne 0$, then given any set of integers $n_1, ..., n_K$, there exists an integer n satisfying

$$0 \le n < \frac{K \log(4R) + \log 16}{s\sqrt{8}},$$
 (16)

such that

$$\prod_{i=1}^{K} \left(1 - 4 \left\| \frac{n - n_i}{q_i} \right\|^2 \right) > \frac{2^{-1/R}}{(4R)^{K/4R}}.$$
(17)

Proof of the Proposition.

Define

$$f(n) = \prod_{i=1}^{K} \left| e^{2\pi i n/q_i} + e^{2\pi i n_i/q_i} \right|^{2R},$$

and let

$$H(m_1, ..., m_K) = \frac{m_1}{q_1} + \dots + \frac{m_K}{q_K}$$

The fact we will exploit is that if f(n) is very large, say nearly its maximum value of 2^{2KR} , then we must have that $||(n - n_i)/q_i||$ is close to 0 for many values of i.

On expanding out f(n), we find that

$$\begin{split} f(n) &= \prod_{i=1}^{K} \left| \sum_{j=0}^{R} \binom{R}{j} e^{2\pi i (nj+n_i(R-j))/q_i} \right|^2 \\ &= \prod_{i=1}^{K} \sum_{0 \le j, j' \le R} \binom{R}{j} \binom{R}{j'} e^{2\pi i (n(j-j')+n_i(j'-j))/q_i} \\ &= \sum_{\substack{0 \le j_1, \dots, j_K \le R \\ 0 \le j_1, \dots, j_K' \le R}} \binom{K}{i=1} \binom{R}{j_i} \binom{R}{j'_i} \\ &\times e^{2\pi i n H(j_1-j'_1, \dots, j_K-j'_K)} e^{2\pi i H(n_1(j'_1-j_1), \dots, n_k(j'_K-j_K))} \end{split}$$

From the hypotheses of our proposition we have that if $m_1, ..., m_K$ are integers, not all 0, and $|m_i| \leq R$, then

$$\left|\sum_{n=-M}^{M} \binom{2M}{n+M} e^{2\pi i n H(m_1,\dots,m_K)}\right| = |1 + e^{2\pi i H(m_1,\dots,m_K)}|^{2M}$$

$$\leq |1 + e^{2\pi i s}|^{2M}$$

$$= 2^{2M} \cos^{2M}(\pi s)$$

$$\leq 2^{2M} \left(1 - 4s^2\right)^{2M}$$

$$\leq 2^{2M} \exp\left(-8s^2M\right). \quad (18)$$

And, trivially,

$$\sum_{n=-M}^{M} \binom{2M}{n+M} e^{2\pi i n H(0,\dots,0)} = 2^{2M}.$$

So,

$$\sum_{n=-M}^{M} \binom{2M}{n+M} f(n) = 2^{2M} \sum_{\substack{0 \le j_1, \dots, j_K \le R \\ (\text{and } j'_i = j_i)}} \prod_{i=1}^{K} \binom{R}{j_i}^2 + E$$

$$= 2^{2M} {\binom{2R}{R}}^{K} + E$$

> $\frac{2^{2M+2KR}}{(4R)^{K/2}} + E,$ (19)

where E is to be thought of as an error, and equals

$$\sum_{\substack{0 \le j_1, \dots, j_K \le R \\ 0 \le j'_1, \dots, j'_K \le R \\ (j_1, \dots, j_K) \ne (j'_1, \dots, j'_K)}} \left(\prod_{i=1}^K \binom{R}{j_i} \binom{R}{j'_i} \right) e^{2\pi i H(n_1(j'_1 - j_1), \dots, n_K(j'_K - j_K))} \\ \sum_{n=-M}^M \binom{2M}{n+M} e^{2\pi i n H(j_1 - j'_1, \dots, j_K - j'_K)}.$$

Using (18) we deduce that

$$|E| < 2^{2M} \exp(-8s^2 M) \left(\sum_{j=0}^{R} \binom{R}{j}\right)^{2K} = 2^{2M+2KR} \exp(-8s^2 M).$$

Combining this bound on |E| with (19), we deduce that

$$\sum_{n=-M}^{M} {\binom{2M}{n+M}} f(n) > \frac{2^{2M+2KR-1}}{(4R)^{K/2}}$$
(20)

whenever

$$\exp(8s^2M) > 2(4R)^{K/2},$$

which is to say

$$M > \frac{K \log(4R) + \log 4}{16s^2}.$$
 (21)

We now require a basic lemma:

Lemma 3 For all integers $M \ge 1$ we have that for $x \ge 0$,

$$\sum_{|n| \ge \sqrt{2Mx}} \binom{2M}{n+M} \le 2^{2M+1} e^{-2x}.$$

Proof. We could prove this using Stirling's formula; however, Hoeffding's inequality, which is stated as Proposition 1 in the proof of Theorem 3 above, quickly gives a decent upper bound. In our case, we set Y to be a binomial random variable with parameters n = 2M and p = 1/2, and then we let X = 2(Y - M), which can be written as $X_1 + \cdots + X_{2M}$, where X_i takes the values ± 1 each with probability 1/2. So, Hoeffding gives the bound

$$\frac{1}{2^{2M}} \sum_{|j| \ge \sqrt{2Mx}} \binom{2M}{j+M} = \mathbb{P}(|X| \ge 2\sqrt{2Mx}) \le 2e^{-2x}.$$

Applying the lemma with

$$x = \frac{K \log(4R)}{4} + \frac{\log 8}{2}$$
(22)

we find that

$$\sum_{|n| \ge \sqrt{2Mx}} \binom{2M}{n+M} \le \frac{2^{2M-2}}{(4R)^{K/2}};$$

and so, since $f(n) \leq 2^{2KR}$ we deduce

$$\sum_{|n| \ge \sqrt{2Mx}} \binom{2M}{n+M} f(n) \le \frac{2^{2M+2KR-2}}{(4R)^{K/2}},$$

Combining this with (20) we deduce

$$\sum_{|n|<\sqrt{2Mx}} \binom{2M}{n+M} f(n) > \frac{2^{2M+2KR-2}}{(4R)^{K/2}}.$$

Now, as the sum of these binomial coefficients is at most 2^{2M} , we deduce that there exists an integer n satisfying $|n| < \sqrt{2Mx}$ and

$$f(n) > \frac{2^{2KR-2}}{(4R)^{K/2}}.$$
 (23)

Using now the fact that for $\theta \in [-1/2, 1/2]$,

$$\left|1+e^{2\pi i\theta}\right| = \left|e^{-\pi i\theta}+e^{\pi i\theta}\right| = 2\cos(\pi\theta) \leq 2\left(1-4\theta^2\right),$$

we deduce that (23) implies that for some integer $|n| \leq \sqrt{2Mx}$,

$$\prod_{i=1}^{K} \left(1 - 4 \left\| \frac{n - n_i}{q_i} \right\|^2 \right) > \frac{2^{-1/R}}{(4R)^{K/4R}}.$$
(24)

Now, since this bound does not depend on the choice of phases $n_1, ..., n_K$, by shifting n_i by an amount $\lfloor \sqrt{2Mx} \rfloor + 1$, we deduce that (24) in fact holds for $0 \le n < 2\sqrt{2Mx}$.

Since this holds for any M satisfying (21), and for x satisfying (22), we have that (24) holds for $0 \le n < N$, for any N satisfying

$$N^2 > 8\left(\frac{K\log(4R) + \log 4}{16s^2}\right)\left(\frac{K\log(4R)}{4} + \frac{\log 8}{2}\right),$$

which certainly holds if

$$N \geq \frac{K \log(4R) + \log 16}{s\sqrt{8}}$$

Proposition 2 now easily follows.

Corollary 1 Let $0 < \epsilon < 1$ and $0 < \delta < 1/2$ be given, and suppose that

$$\frac{R}{\log(4R) + \log 16} > \frac{1}{16\epsilon\delta^2}.$$
 (25)

Then, if $q_1, ..., q_K \ge 2$ satisfy $s(q_1, ..., q_k; R) \ne 0$, then there exists an integer n in the range (16) such that

$$\left| \left| \frac{n - n_i}{q_i} \right| \right| < \delta, \text{ for all but } \epsilon K \text{ integers } i = 1, 2, ..., K.$$

Proof.

Suppose that R satisfies (25), and that for every integers n there are at least ϵK integers i = 1, ..., K satisfying

$$\left|\left|\frac{n-n_i}{q_i}\right|\right| \ge \delta.$$

Then, we will have that for every integer n,

$$\prod_{i=1}^{K} \left(1 - 4 \left\| \frac{n - n_i}{q_i} \right\|^2 \right) \leq \left(1 - 4\delta^2 \right)^{\epsilon K} \leq \exp\left(-4\epsilon K\delta^2 \right).$$

Using (25) we have that this right most quantity satisfies

$$\exp\left(-4\epsilon K\delta^2\right) < \frac{2^{-1/R}}{(4R)^{K/4R}}.$$

This then would give us a contradiction, because it would imply that (17) fails to hold for every n. The corollary now follows.

Corollary 2 Suppose $0 < \alpha, \beta < 1/2$; suppose that $q_1, \ldots, q_K \ge 2$ are integers; suppose that $R \ge 1$ satisfies

$$\frac{R}{\log(4R) + \log 16} > \frac{1}{4\alpha\beta^2};$$

and, suppose that $s(q_1, ..., q_K; R) \neq 0$.

Then, for any set of integer phases $\delta_1, ..., \delta_K$, there exists an integer n in the range (16), such that for at least $(1 - \alpha)K$ indices i = 1, 2, ..., K we have

$$f_i(n+\delta_i) \geq (1-\beta)q_i - 1.$$

Proof.

For i = 1, 2, ..., K, let

$$n_i = \lfloor \beta q_i / 2 \rfloor - \delta_i + 1,$$

and let $\epsilon = \alpha$ and $\delta = \beta/2$. It follows that

$$\frac{R}{\log(4R) + \log 16} > \frac{1}{16\epsilon\delta^2}.$$

Thus, since we have assumed $s(q_1, ..., q_K; R) \neq 0$, it follows from Corollary 1 that there exists an integer n such that for at least $(1 - \epsilon)K = (1 - \alpha)K$ indices i = 1, 2, ..., K,

$$\left\|\frac{n-n_i}{q_i}\right\| < \delta = \beta/2.$$

For such indices i and integer n we get that

$$f_i(n+\delta_i) = f_i(n-n_i+\lfloor\beta q_i/2\rfloor+1) > f_i(\beta q_i/2+\lfloor\beta q_i/2\rfloor+1)$$

$$\geq q_i(1-\beta)-1.$$

The proof of Theorem 5 is now but a simple application of Corollary 2: The hypotheses of this theorem match the hypotheses of Corollary 2 for $\alpha = \epsilon_1/3$ and $\beta = 2\epsilon_1/3$; and so, given any set of phases $\delta_1, ..., \delta_K$, there exists an integer n in the range (16) such that for at least $(1 - \alpha)K$ indices i we have that

$$f_i(n+\delta_i) \geq (1-\beta)q_i - 1.$$

Thus, if we let S_0 denote the set of all indices *i* where this inequality holds, and let $S_1 = \{1, ..., K\} \setminus S_0$, then we have

$$\sum_{i=1}^{K} d_i f_i(n+\delta_i)$$

$$\geq \sum_{i\in S_0} d_i((1-\beta)q_i-1) + \sum_{i\in S_1} d_i$$

$$= (d_1q_1 + \dots + d_Kq_K) - \sum_{i\in S_0} d_i(\beta q_i+1) - \sum_{i\in S_1} d_i(q_i-1)$$

$$\geq (d_1q_1 + \dots + d_Kq_K) - |S_0| \max_i d_i(\beta q_i+1) - |S_1| \max_i d_i(q_i-1)$$

$$\geq (d_1q_1 + \dots + d_Kq_K) - K \max_i d_i(\beta q_i+1) - \alpha K \max_i d_i(q_i-1)$$

Setting $\alpha = \epsilon_1/3$ and $\beta = 2\epsilon_1/3$ we get that this last line is at most

$$(d_1q_1 + \dots + q_Kq_K) - K \operatorname{Max}_i d_i(\epsilon_1q_i + 1),$$

and the theorem is proved.

7 Computer Experiments