RC 21738 (97926) (4 May 2000)
Mathematics/Computer Science

IBM Research Report

Indivisibility and Divisibility Polytopes

Don Coppersmith & Jon Lee

IBM Research Division
T.J. Watson Research Center
Yorktown Heights, New York

IBM Research Division
Almaden · Austin · Beijing · Delhi · Haifa · T.J. Watson · Tokyo · Zurich

INDIVISIBILITY AND DIVISIBILITY POLYTOPES

Don COPPERSMITH[1] & Jon LEE[2]

April 2000

Abstract

We study the the polytopes of binary n-strings that encode (positive) integers that are not divisible by a particular positive integer p — the *indivisibility polytopes*, as well as the more general "clipped cubes". Also, we discuss a potential application to factoring. Finally, we present some results concerning divisibility polytopes.

Keywords: integer program, polytope, clipped cube, totally dual integral, ideal matrix, generalized set covering, binary encoding, divisible, factoring.

[1]Dept. of Mathematical Sciences, T.J. Watson Research Center, IBM, Yorktown Heights, N.Y., U.S.A.

[2]Dept. of Mathematics, 715 POT, University of Kentucky, Lexington, KY 40506-0027, U.S.A.; CORE, 34 voie du Roman Pays, Université Catholique de Louvain, 1348 Louvain-la-Neuve, BELGIUM; Email: jlee@ms.uky.edu . WWW: http://www.ms.uky.edu/~jlee .

Introduction

We assume familiarity with the basics of polytopes (see [39]) and integer programming (see [30]). Let p and n be positive integers, and let $N := \{0, 1, 2, \ldots, n-1\}$. We define the *indivisibility polytopes*

$$\mathcal{I}_{pn} := \text{conv}\left\{ x \in \{0,1\}^N \ : \ \sum_{j \in N} 2^j x_j \not\equiv 0 \pmod{p} \right\}.$$

That is, $\mathcal{I}_{pn}$ is the polytope of binary n-strings that encode (positive) integers that *are not* divisible by p. As an example, which can be used to visualize many of the results, we depict $\mathcal{I}_{33}$ in Figure 1. Extreme points of the cube are labeled in base 10.

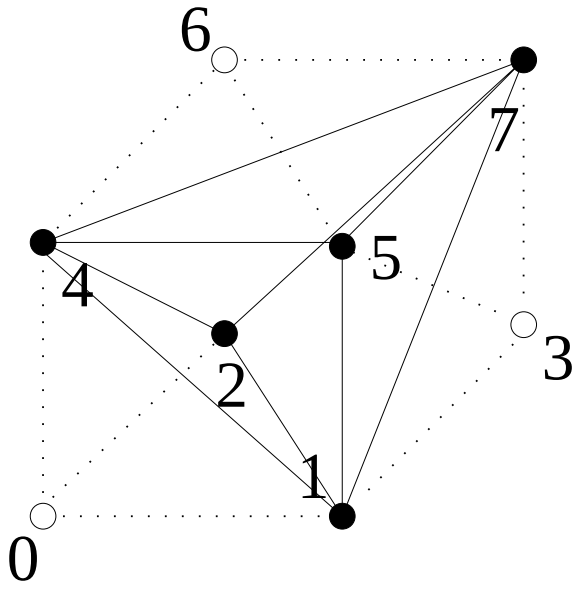

Figure 1: The indivisibility polytope $\mathcal{I}_{33}$

If we were only interested in methods for incorporating indivisibility by p as a constraint on a positive integer variable y in an optimization formulation, we could simply introduce further integer variables $\ell \geq 0$ and $1 \leq z \leq p-1$, and then set $y = \ell p + z$. Our interest in indivisibility polytopes stems from a desire to form products of such variables, which is effectively accomplished using their binary representation (see [14]). In Section 1, we introduce "clipped cubes". Most indivisibility polytopes — the "nondyadic" ones — are clipped

cubes, and this notion provides a clean view of certain aspects of these indivisibility polytopes. In particular, we (i) give a characterization as the solution set of a totally dual integral system of linear inequalities, (ii) characterize adjacency of extreme points, (iii) describe a simple construction for finding short edge paths, (iv) give an efficient separation algorithms for the facet describing inequalities, (v) give an efficient algorithm for optimizing a linear function, (vi) make connections with balanced and ideal $0, \pm 1$ matrices, and (vii) discuss alternative models.

In Section 2, we focus on indivisibility polytopes and make the connection with clipped cubes. To complete the study of indivisibility polytopes implicitly studied in Section 1, we give linear inequality descriptions and characterize extreme point adjacency for the relatively trivial "dyadic" indivisibility polytopes which are *not* clipped cubes. We describe very mild conditions which ensure that the simple bound inequalities describe facets of the nondyadic indivisibility polytopes. indivisibility polytopes. In Section 3, we discuss a potential application to factoring.

In Section 4, we define the divisibility polytopes. For divisibility polytopes, we investigate some properties of the facet describing inequalities.

Other notation: For $j \in S$, $S - j := S \setminus \{j\}$. For $j \notin S$, $S + j := S \cup \{j\}$. For sets $S_1, S_2 \in N$, $S_1 \triangle S_2$ denotes the *symmetric difference* $(S_1 \setminus S_2) \cup (S_2 \setminus S_1)$. Let 2^N denote the set of all subsets of N. For positive integer n, $\mathbb{R}^N$ denotes the vector space of real n-tuples with coordinates indexed from N. Similarly, $[0,1]^N := \{x \in \mathbb{R}^N \ : \ 0 \leq x_j \leq 1, \forall\ j \in N\}$, and $\{0,1\}^N := \{x \in \mathbb{R}^N \ : \ x_j \in \{0,1\}, \forall\ j \in N\}$. $x \in \mathbb{R}^N$ so that when integer, the low order bits $\langle c, x\rangle := \sum_{j \in N} c_j x_j$. For $j \in N$, e^j is the standard unit vector in $\mathbb{R}^N$. For $S \subset N$, $x(S) := \sum_{j \in N} e^j$. Also, we write e for any vector of all ones. For a polytope Q, $G(Q)$ is the 1-skeleton of P, $V(G(Q))$ is the set of vertices of $G(Q)$ (i.e., the set of extreme points of Q), and $E(G(Q))$ is the set of edges of $G(Q)$ (i.e., the set of 1-dimensional faces of Q). Finally, $\mathrm{vol}_n(Q)$ denotes the volume (i.e., n-dimensional Lebesgue measure) of the polytope $Q \subset \mathbb{R}^N$.

1 Clipped Cubes

In this section we introduce and study "clipped cubes". In Section 2, we make a precise connection between most indivisibility polytopes and clipped cubes.

For a subset $\mathcal{C}$ of 2^N, we define a polytope

$$\mathcal{Q}(\mathcal{C}) := \mathrm{conv}\left\{x(S) \ : \ S \in 2^N \setminus \mathcal{C}\right\} \subset \{0,1\}^N.$$

A *clippable subset* of 2^N is a $\mathcal{C} \subset 2^N$ satisfying:

(C1) $\{j\} \notin \mathcal{C},\ \forall\ j \in N$;

(C2) $S \notin \mathcal{C}$, for some $S \subset N$ having $|S| > 1$;

(C3) $|S_1 \triangle S_2| \neq 1, \forall\ S_1, S_2 \in \mathcal{C}$.

As will become evident, the important property is C3, while C1–C2 are included for technical reasons. We note that if $\mathcal{C}$ is clippable, then all subsets of $\mathcal{C}$ are clippable. That is, the *set of* clippable sets is an "independence system". On the other hand, clippable sets can be large; for example, the set of even cardinality subsets of N is clippable (when $n \geq 3$).

For a clippable subset $\mathcal{C}$ of 2^N, we refer to $\mathcal{Q}(\mathcal{C})$ as a *clipped cube*.

1.1 Inequality Description

Obviously, the simple bound inequalities

$$-x_j \leq 0\ , \tag{1}$$
$$x_j \leq 1\ , \tag{2}$$
$$\forall\ j \in N\ ,$$

are valid for $\mathcal{Q}(\mathcal{C})$. In addition, we have the *clipping inequalities*

$$\Theta(S): \qquad \sum_{j \in S} x_j - \sum_{j \in N \setminus S} x_j \leq |S| - 1\ , \tag{3}$$
$$\forall\ S \in \mathcal{C}\ .$$

Proposition 1 *A point $x \in \{0,1\}^N$ satisfies the clipping inequalities (3) for all $S \in \mathcal{C}$ if and only if $x \in \mathcal{Q}(\mathcal{C})$.*

Proof: Suppose that $x \in \{0,1\}^N$ is not in $\mathcal{Q}(\mathcal{C})$. Then $S := \{j \in N\ :\ x_j = 1\} \in \mathcal{C}$. For this choice of S, the left-hand side of (3) is $|S|$, which exceeds the right-hand side. So not all clipping inequalities (3) are satisfied by x. Conversely, considering all $x \in \{0,1\}^N$, the maximum of the left-hand side of (3) is $|S|$, and this is only achieved when $x_j = 1$ for all $j \in S$ and $x_j = 0$ for all $j \in N \setminus S$. But in this case, the hypothesis indicates that x is not in $\mathcal{Q}(\mathcal{C})$. □

Proposition 2 *The clipped cube $\mathcal{Q}(\mathcal{C})$ is full dimensional.*

Proof: Suppose that

$$\sum_{j \in N} a_j x_j = b \tag{4}$$

is a nontrivial equation satisfied by all points of $\mathcal{Q}(\mathcal{C})$. By C1, $x(\{j\}) \in \mathcal{Q}(\mathcal{C})$ for all $j \in N$, so we can plug these points into (4) to obtain $a_j = b$ for all $j \in N$. Since we have assumed that (4) is nontrivial, we can divide (4) by b to obtain

$$\sum_{j \in N} x_j = 1 \ . \tag{5}$$

Next, by C2, we choose an $S \subset N$ such that $S \notin \mathcal{C}$ and $|S| > 1$. Plugging $x(S)$ into (5), we obtain a contradiction. Therefore, there are no nontrivial equations satisfied by all points of $\mathcal{Q}(\mathcal{C})$. □

Proposition 3 *All clipping inequalities describe facets of the clipped cube* $\mathcal{Q}(\mathcal{C})$.

Proof: Let $\mathcal{F}_S(\mathcal{C})$ be the face of $\mathcal{Q}(\mathcal{C})$ that is described by (3) for an $S \in \mathcal{C}$. We will demonstrate that any other linear inequality that also describes $\mathcal{F}_S(\mathcal{C})$ is just a positive multiple of (3). Suppose that

$$\sum_{j \in N} a_j x_j \leq b \ , \tag{6}$$

describes the same face of $\mathcal{Q}(\mathcal{C})$ as (3) does. By C3, we observe that for each $k \in S$, $S - k \notin \mathcal{C}$. Therefore, for each $k \in S$, since obviously $x(S-k)$ satisfies (3) as an equation, we have $x(S-k) \in \mathcal{F}_S(\mathcal{C})$. Plugging this point into (6) as an equation, we conclude that

$$\sum_{j \in S-k} a_j = b \ , \quad \forall \ k \in S \ . \tag{7}$$

Furthermore, $x(S) \notin \mathcal{F}_S(\mathcal{C})$, therefore

$$\sum_{j \in S} a_j > b \ . \tag{8}$$

Subtracting (7) from (8), we conclude that $a_k > 0$ for all $k \in S$. Similarly, by C3, we observe that for each $l \in N \setminus S$, $S + l \notin \mathcal{C}$. Therefore, for each $l \in N \setminus S$,

since obviously $x(S+l)$ satisfies (3) as an equation, we have $x(S+l) \in \mathcal{F}_S(\mathcal{C})$. Plugging this point into (6) as an equation, we conclude that

$$a_l + \sum_{j \in S} a_j = b \ , \quad \forall \ l \in N \setminus S \ . \tag{9}$$

Subtracting (7) from (9), we conclude that

$$a_k + a_l = 0 \ , \quad \forall \ k \in S, \ l \in N \setminus S \ . \tag{10}$$

So we can divide (6) by $|a_j|$, which is the same for all $j \in N$, to obtain the inequality (3). Notice that the right-hand side of (3) is correctly obtained as a consequence of (7). $\square$ We also have a converse to this last result.

Proposition 4 *If $\mathcal{C} \subset 2^N$ satisfies C1 but not C3, then there are (at least two) clipping inequalities that do not describe facets of $\mathcal{Q}(\mathcal{C})$.*

Proof: Suppose that $\mathcal{C}$ satisfies C1 but not C3. Then there is a set $S \in \mathcal{C}$ and an element $k \in N \setminus S$ with $S+k \in \mathcal{C}$. Clearly $S \neq \emptyset$ or C1 would be violated; hence the existence of $S+k \in \mathcal{C}$ means that $\mathcal{C}$ satisfies C2. Therefore, $\mathcal{Q}(\mathcal{C})$ is full dimensional and its facet describing inequalities are unique up to positive scalar multiplication.

Now, we add the valid clipping inequalities $\Theta(S)$ and $\Theta(S+k)$, divide by two, and round the right-hand side down to obtain the valid inequality

$$\sum_{j \in S} x_j - \sum_{j \in N \setminus (S+k)} x_j \leq |S| - 1 \ . \tag{11}$$

Since $\Theta(S)$ (resp., $\Theta(S+k)$) is the sum of the valid inequalities (11) and $-x_k \leq 0$ (resp., $x_k \leq 1$), these two clipping inequalities do not describe facets of $\mathcal{Q}(\mathcal{C})$. $\square$

Next, we give a complete characterization of the clipped cube by linear inequalities.

Proposition 5 *Let $\mathcal{C}$ be a clippable subset of 2^N. Every facet of $\mathcal{Q}(\mathcal{C})$ is described by a simple bound inequality or a clipping inequality.*

Proof: Suppose that (6) describes a facet of $\mathcal{Q}(\mathcal{C})$ other than one described by a simple bound inequality. Let

$$\mathcal{S} := \{ j \in N \ : \ a_j > 0 \} \, ,$$

and let

$$\mathcal{S}' := \{j \in N \ : \ a_j < 0\}\,.$$

First, by contradiction, we demonstrate that $S \in \mathcal{C}$. Suppose otherwise. Then $x(\mathcal{S})$ maximizes the left-hand side of (6) over the extreme points of $\mathcal{Q}(\mathcal{C})$. Indeed, every maximizer of the left-hand side of (6) has $x_j = 1$ for all $j \in \mathcal{S}$ and $x_j = 0$ for all $j \in \mathcal{S}'$. But, since (6) is not described by a simple upper bound inequality, we must have $\mathcal{S} = \mathcal{S}' = \emptyset$. But then $a_j = 0$ for all $j \in N$, contradicting the hypothesis that (6) describes a facet. Next, we observe by C3 that $x(\mathcal{S}-j) \in \mathcal{Q}(\mathcal{C})$ for all $j \in \mathcal{S}$, and $x(\mathcal{S}+j) \in \mathcal{Q}(\mathcal{C})$ for all $j \in N \setminus \mathcal{S}$. So, these $|N|$ points are among the extreme points of $\mathcal{Q}(\mathcal{C})$ that may potentially maximize the left-hand side of (6). Let

$$\alpha := \min\{|a_k| \ : \ k \in N\}\,.$$

Indeed, the maximum of the left-hand side is $x(\mathcal{S}) - \alpha$. Certainly we have $\alpha > 0$ since (6) describes a facet of $\mathcal{Q}(\mathcal{C})$. Now, if $a_j > \alpha$ for some $j \in \mathcal{S}$, then $x_j = 1$ for every maximizer of the left-hand side of (6). Also, if $a_j < \alpha$ for some $j \in N \setminus \mathcal{S}$, then $x_j = 0$ for every maximizer of the left-hand side of (6). Either case would contradict our initial hypothesis. Therefore, $|a_j| = \alpha$ for all $j \in N$. Now, plugging in a maximizing point (either $x(\mathcal{S} - j)$ for some $j \in \mathcal{S}$ or $x(\mathcal{S} + j)$ for some $j \in N \setminus \mathcal{S}$), we obtain $b = \alpha(|\mathcal{S}| - 1)$. Finally, dividing (6) by α, we obtain the clipping inequality (3) with $S = \mathcal{S}$. □

1.2 Separation, Optimization and Total Dual Integrality

Let $\mathcal{C}$ be a clippable subset of 2^N that is described by a membership oracle. Let $\tilde{x}$ be a point in $\mathbb{Q}^N$. We consider the following decision problem.

CLIPMEMB: Is $\tilde{x}$ in the clipped cube $\mathcal{Q}(\mathcal{C})$?

Proposition 6 *CLIPMEMB is in NP ∩ Co-NP.*

Proof: Proposition 5 implies that whenever $\tilde{x}$ is not in $\mathcal{Q}(\mathcal{C})$, there is a short proof of this fact — namely, a violated clipping inequality. That is, CLIPMEMB is in Co-NP.

Next, by Carathéodory's Theorem (see Proposition 1.15, (ii), p. 46 of [39], for example), if $\tilde{x}$ is in $\mathcal{Q}(\mathcal{C})$, then there are $n+1$ sets $S_i \in 2^N \setminus \mathcal{C}$ such that the following system has a solution:

$$\sum_{i=0}^{n} \lambda_i \, x(S_i) = \tilde{x}\ ;$$

$$\sum_{i=0}^{n} \lambda_i = 1 \ ;$$
$$\lambda_i \geq 0 \ , \quad \text{for } i = 0, 1, \ldots, n \ .$$

In fact, exploiting standard results concerning rational inequality systems, this system has a rational extreme point solution which has a short binary encoding (see Proposition 2.12, (ii), p. 158 of [30], for example). Note that we can check that each S_i is not in $\mathcal{C}$ using the membership oracle. Therefore, CLIPMEMB is in NP. □

Proposition 6 is strong evidence for CLIPMEMB being in P. Indeed, we provide a simple algorithm for CLIPMEMB in the proof of the following result.

Proposition 7 *CLIPMEMB is in P.*

Proof: We describe an $\mathcal{O}(n)$ procedure. We may assume that $\tilde{x}$ satisfies the simple bound inequalities since there are only $2n$ of them to check. The point $\tilde{x}$ violates (3) if and only if

$$\sum_{j \in S} (1 - \tilde{x}_j) + \sum_{N \setminus S} \tilde{x}_j < 1 \ . \tag{12}$$

Define the set $S' := \{j \in N \ : \ \tilde{x}_j > \frac{1}{2}\}$. Clearly S' minimizes the left-hand side of (12) over all $S \subset N$. Now, this minimum in nonnegative, and any set $S \subset N$ will make the left-hand side of (12) at least $|S' \triangle S|/2$. Therefore, we only need consider, for possible violation of (12), those $n+1$ choices of S with $|S' \triangle S| \leq 1$. So if any of these sets S is in $\mathcal{C}$ and satisfies (12), we have the violated clipping inequality $\Theta(S)$. Otherwise, $\tilde{x}$ is in $\mathcal{Q}(\mathcal{C})$. □

Another use of the separation procedure is a converse to Proposition 5.

Proposition 8 *If $\mathcal{C} \subset 2^N$ satisfies C1 but not C3, then there are facets of $\mathcal{Q}(\mathcal{C})$ that are described by no simple bound inequality and no clipping inequality.*

Proof: Suppose that $\mathcal{C}$ satisfies C1 but not C3. Choose nonempty S and $k \in N \setminus S$ as in the proof of Proposition 4. Let l be any element of S. Consider the point $\tilde{x} := \frac{1}{2}x(S) + \frac{1}{2}x(S - l + k)$. Obviously $\tilde{x}$ satisfies all of the simple bound inequalities. It is easy to confirm that $\tilde{x}$ violates the valid inequality (11) (by $\frac{1}{2}$). Also, because $\tilde{x}$ has two coordinates equal to $\frac{1}{2}$, the separation procedure indicates that there is no violated clipping inequality.

Hence $\mathcal{Q}(\mathcal{C})$ must have a facet that is described by no simple bound inequality and no clipping inequality. □

Another natural problem for the clipped cube $\mathcal{Q}(\mathcal{C})$ is the following linear optimization problem. Let c be in $\mathbb{Q}^n$.

CLIPOPT: Find a point x of $\mathcal{Q}(\mathcal{C})$ that maximizes $\sum_{j\in N} c_j x_j$.

A consequence of Proposition 7 is the following result.

Proposition 9 *There is a polynomial-time algorithm for CLIPOPT.*

Proof: This follows from Proposition 7, using the polynomial-time equivalence of separation and linear-function optimization for polytopes implied by the ellipsoid method (see [19, 20, 21]). □

A more direct and constructive proof of Proposition 9 is provided by the simple recipe of the next result.

Proposition 10 *Let $\mathcal{C}$ be a clippable subset of 2^N, let $c \in \mathbb{R}^N$, and let $S^+ := \{j \in N \ : \ c_j \geq 0\}$.*

(i) If $S^+ \in 2^N \setminus \mathcal{C}$, then $x(S^+)$ maximizes $\langle c, x\rangle$ on $\mathcal{Q}(\mathcal{C})$;

(ii) if $S^+ \in \mathcal{C}$, then let $k := \operatorname{argmax}\{c_j \ : \ j \in N \setminus S^+\}$, and let $l := \operatorname{argmin}\{c_j \ : \ j \in S^+\}$ (so $c_k < 0$ or $= -\infty$, and $c_l \geq 0$ or $= +\infty$).

(a) If $-c_k \leq c_l$, then $x(S^+ + k)$ maximizes $\langle c, x\rangle$ on $\mathcal{Q}(\mathcal{C})$;

(b) if $c_l \leq -c_k$, then $x(S^+ - l)$ maximizes $\langle c, x\rangle$ on $\mathcal{Q}(\mathcal{C})$.

Proof: Our proof relies on linear programming duality. Consider the primal linear program of maximizing $\langle c, x\rangle$, subject to (1–2) $\forall\ j \in N$, (3) $\forall\ S \in \mathcal{C}$. We have the dual linear program

$$\begin{aligned}
&\min \sum_{j\in N} y_j + \sum_{S\in\mathcal{C}} (|S| - 1)\, z_S \ , \\
&\text{subject to} \quad y_j + \sum_{\substack{S\in\mathcal{C}\ :\\ j\in S}} z_S - \sum_{\substack{S\in\mathcal{C}\ :\\ j\in N\setminus S}} z_S \geq c_j \ , \quad \forall\ j \in N \ ; \\
&y_j \geq 0, \quad \forall\ j \in N \ ; \\
&z_S \geq 0, \quad \forall\ S \in \mathcal{C} \ .
\end{aligned}$$

If the hypothesis of (i) holds, then $x(S^+)$ is a primal feasible solution with objective value $\sum_{j\in S^+} c_j$. It is easy to check that setting $y_j = c_j$ for $j \in S^+$

and setting all other dual variables to 0 gives a dual feasible solution with the same objective value as the primal solution. Hence, both primal and dual solutions are optimal.

If the hypothesis of (iia) holds, then, by C3, $x(S^+ + k)$ is a primal feasible solution, and it has objective value $c_k + \sum_{j \in S^+} c_j$. It is easy to check that setting $y_j = c_j + c_k$ for $j \in S^+$, setting $z_{S^+} = -c_k$, and setting all other dual variables to 0 gives a dual feasible solution with the same objective value as the primal solution. Hence, both primal and dual solutions are optimal.

On the other hand, if the hypothesis of (iib) holds, then, by C3, $x(S^+ - l)$ is a primal feasible solution, and it has objective value $-c_l + \sum_{j \in S^+} c_j$. It is easy to check that setting $y_j = c_j - c_l$ for $j \in S^+$, setting $z_{S^+} = c_l$, and setting all other dual variables to 0 gives a dual feasible solution with the same objective value as the primal solution. Hence, both primal and dual solutions are optimal. □

One consequence of the *proof* of Proposition 10, is another proof of Proposition 5. Also, when the c_j are integers, the constructive proof method provides integer optimal dual solutions. Therefore, we have the following result.

Proposition 11 *Let $\mathcal{C}$ be a clippable subset of 2^N. The system (1–2) $\forall\ j \in N$, (3) $\forall\ S \in \mathcal{C}$ is totally dual integral.*

1.3 Generalized Covering

A 0,1 matrix is *balanced* if it does not contain a square submatrix of odd order with two ones per row and per column (see [3]). Berge demonstrated (among other things) that if A is balanced, then the the *fractional covering polyhedron*

$$\{x \in \mathbb{R}^n \ : \ Ax \geq e,\ x \geq 0\}$$

has only integer extreme points (see [4]). For an $m \times n$ $0, \pm 1$ matrix A, let $\nu(A) \in \mathbb{R}^m$ be defined by letting $\nu_i(A)$ be the number of entries in row i of A that are equal to -1. Following others, a $0, \pm 1$ matrix is *ideal* if the *fractional generalized covering polyhedron*

$$\{x \in \mathbb{R}^n \ : \ Ax \geq e - \nu(A),\ 0 \leq x \leq e\}$$

has only integer extreme points. (see [9, 31, 15], for example). These polyhedra are the natural ones to study when formulating propositional logic problems in "conjunctive normal form" as linear 0,1 optimization problems (see [8, 38]). Let $\pi(A) \in \mathbb{R}^m$ be defined by letting $\pi_i(A)$ be the number of entries in row

i of A that are equal to $+1$. Rewriting the defining system of the fractional generalized covering polyhedron as

$$\{x \in \mathbb{R}^n \ : \ (-A)x \leq \pi(-A) - e, \ 0 \leq x \leq e\} \ ,$$

we see an immediate connection with our inequality description of the clipped cube $\mathcal{Q}(\mathcal{C})$ (i.e., the system (1–2) $\forall\, j \in N$, (3) $\forall\, S \in \mathcal{C}$). That is, our inequality description of $\mathcal{Q}(\mathcal{C})$ describes a fractional generalized covering polyhedron. Interpreted in the framework of propositional logic, for each $S \in \mathcal{C}$, we can interpret (3), for binary encodings $x \in \mathbb{R}^N$, as saying either some bit in S is "off" or some bit not in S is "on" (otherwise x would encode S). By Proposition 5, this particular fractional generalized covering polyhedron has only integer extreme points — that is, the constraint matrix associated with the clipping inequalities is ideal. Truemper introduced balanced $0, \pm 1$ matrices as a generalization of balanced $0, 1$ matrices. A $0, \pm 1$ matrix is called *balanced* if every square submatrix with two nonzero entries per row and per column has the sum of its entries divisible by 4 (see [37]). Conforti and Cornuéjols generalized Berge's polyhedral result by showing (among other things) that if the $0, \pm 1$ matrix A is balanced, then A is ideal and the generalized covering formulation is totally dual integral (see [10, 9]). In light of Propositions 5 and 11, it is natural to wonder whether the constraint matrix described by the clipping inequalities (3) $\forall\ S \in \mathcal{C}$ is balanced. Alas this is *not* the case: since our matrix has no entries of zero, the only square submatrices with two nonzeros entries per row and per column are of order 2; except in some trivial cases, the constraint matrix has submatrices of the form

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \ ,$$

with the sum of the entries being 2. Indeed this submatrix also demonstrates that the constraint matrix is not ordinarily totally unimodular.

Finally, we wonder whether there is some higher reason that explains why the generalized covering formulations for balanced $0, \pm 1$ matrices and for the clipped cubes are totally dual integral.

The inductive proof scheme in [15] for demonstrating the total dual integrality of generalized covering formulations having $0, \pm 1$ *balanced* constraint matrices, relies only on the idealness of the constraint matrix and all submatrices obtained by the deletion of rows. So that proof scheme can be adapted here as well. So perhaps the class of ideal matrices having all submatrices obtained by the deletion of rows being ideal bears further study.

1.4 Volume and Alternative Models

Studying the n-dimensional volume of polytopes arising in discrete optimization was introduced in [25] and then further studied in [23, 35]. Let $\mathcal{Q} \subset [0,1]^N$ be an arbitrary polytope with extreme points in $\{0,1\}^N$. One theme in [25] is that for certain such polytopes $\mathcal{Q}$, it is desirable and may be possible to find a polytope $\mathcal{Q}' \subset [0,1]^N$ such that

(i) the volume of $\mathcal{Q}'$ is nearly that of $\mathcal{Q}$;

(ii) $\mathcal{Q}' \cap \{0,1\}^N = \mathcal{Q} \cap \{0,1\}^N$;

(iii) the inequality description of $\mathcal{Q}'$ is simpler than that of $\mathcal{Q}$.

The point is that because of (iii), we may have a relatively easy time working with the relatively simple linear programming subproblems associated with $\mathcal{Q}'$ — indeed, this would certainly be the case if we had an inequality description of $\mathcal{Q}'$ but not of $\mathcal{Q}$. The aim of (i) is to suggest that the relaxation from $\mathcal{Q}$ to $\mathcal{Q}'$ is not so weak in some average sense. Property (ii) ensures that optimal solutions of integer programs over $\mathcal{Q}'$ are extreme points of $\mathcal{Q}$. In this section, we investigate clipped cubes from this viewpoint.

First, we observe that even though clippable subsets of 2^N can be large (e.g., the even cardinality subsets of N when $n \geq 3$), the volume of a clipped cube is always nearly 1.

Proposition 12 *Let $\mathcal{C}$ be a clippable subset of 2^N. Then* $\mathrm{vol}_n(\mathcal{Q}(\mathcal{C})) = 1 - |\mathcal{C}|/n!$. *In particular,* $\mathrm{vol}_n(\mathcal{Q}(\mathcal{C})) \geq 1 - 2^{n-1}/n!$.

Proof: First, we demonstrate that the clipping inequalities remove pieces of the cube $[0,1]^N$ that have pairwise disjoint interiors. Suppose that S_1 and S_2 are distinct sets in $\mathcal{C}$. Consider the strict inequalities

$$-\sum_{j \in S_i} x_j + \sum_{j \in N \setminus S_i} x_j < 1 - |S_i| \ ,$$

for $i = 1, 2$. Adding these together, we obtain

$$-2 \sum_{j \in S_1 \cap S_2} x_j + 2 \sum_{j \in N \setminus (S_1 \cup S_2)} x_j < 2 - |S_1| - |S_2| \ .$$

Adding in twice the simple lower bound inequalities (1) for all $j \in N \setminus (S_1 \cup S_2)$ and twice the simple upper bound inequalities (2) for all $j \in S_1 \cap S_2$, we obtain

$$0 < 2 - |S_1| - |S_2| + 2|S_1 \cap S_2| \ ,$$

or, equivalently,

$$|S_1 \triangle S_2| < 2 \ ,$$

which contradicts C3.

Next, by demonstrating that each clipping inequality removes a simplex of volume $1/n!$ from the cube $[0,1]^N$, the first part of the result follows. For an $S \in \mathcal{C}$, the extreme points of the closure of the points of $[0,1]^N$ violating the clipping inequality (3) are: $x(S)$, $x(S-l)$ for $l \in S$, and $x(S+k)$ for $k \in N \setminus S$. That these $n+1$ points are affinely independent and have as their convex hull a simplex of volume $1/n!$ follows from the following calculation. We arrange these points as columns of an order $n+1$ square matrix with a row of ones appended at the top:

$$\begin{array}{r} \\ S: \\ N \setminus S: \end{array} \begin{array}{c} \begin{array}{ccc} & x(S-l) & x(S+k) \end{array} \\ \left(\begin{array}{c|c|c} 1 & 1_{1\times s} & 1_{1\times n-s} \\ \hline 1_{s\times 1} & 1_{s\times s} - I_{s\times s} & 1_{s\times n-s} \\ \hline 0_{n-s\times 1} & 0_{n-s\times s} & I_{n-s\times n-s} \end{array}\right) \end{array} \ ,$$

where $s := |S|$. Expanding the determinant along the last $n-s$ rows, and then subtracting the first row from the remaining row, we see that this matrix has the same absolute determinant as

$$\left(\begin{array}{c|c} 1 & 1_{1\times s} \\ \hline 0_{s\times 1} & -I_{s\times s} \end{array}\right) \ ,$$

which obviously has absolute determinant 1.

The inequality follows by noting that any set $\mathcal{C}$ of subsets of N satisfying C3 is a vertex packing on $G := G([0,1]^N)$. The maximum number of vertices in such a packing is bounded above by the optimal value of the linear program

$$\max \left\{ \sum_{v \in V(G)} y_v \ : \ y_v + y_w \leq 1, \ \forall \ \{v,w\} \in E(G); \ y_v \geq 0, \ \forall \ v \in V(G) \right\} \ .$$

This, in turn, is bounded above by the objective value of any feasible solution to the dual linear program

$$\min \left\{ \sum_{e \in E(G)} x_e \ : \ \sum_{e \in \delta(v)} x_e \geq 1, \ \forall \ v \in V(G); \ x_e \geq 0, \ \forall \ e \in E(G) \right\} \ .$$

Since $|\delta(v)| = n$ for all $v \in V(G)$, and there are 2^n vertices of G, it easily follows that $x_e := 1/n$ for all $e \in E(G)$ is a feasible solution to this dual linear program having objective value 2^{n-1}. $\square$

We note that when $n \geq 4$ is even, the lower bound of Proposition 12 is sharp — it is attained by the set of even cardinality subsets of N.

Already, Proposition 12 implies that (i) would automatically be achieved if we could find a polytope $\mathcal{Q}'$ satisfying (ii–iii). Alas, the following result implies that if $\mathcal{Q}$ is a clipped cubed, then there is no polytope $\mathcal{Q}' \subset [0,1]^N$ satisfying (ii–iii).

Proposition 13 *Let $\mathcal{C}$ be a clippable subset of 2^N. Then any polytope $\mathcal{Q}'$ such that $\mathcal{Q}' \cap \{0,1\}^N = \mathcal{Q}(\mathcal{C}) \cap \{0,1\}^N$ has at least $|\mathcal{C}|$ facets that are not described by simple bound inequalities.*

Proof: In order for $\mathcal{Q}'$ to have fewer than $|\mathcal{C}|$ facets that are not described by simple bound inequalities, there must be a facet describing inequality (6) of $\mathcal{Q}'$ and sets $S_1, S_2 \in \mathcal{C}$, such that $x(S_1)$ and $x(S_2)$ violate (6). That is,

$$\sum_{j \in S_i} a_j > b \ ,$$

for $i = 1, 2$. Moreover, C3 implies that for $k \notin S_i$, we have

$$\sum_{j \in S_i + k} a_j \leq b \ ,$$

and, for $l \in S_i$, we have

$$\sum_{j \in S_i - l} a_j \leq b \ .$$

Therefore, we have $a_k < 0$ for $k \notin S_i$ and $a_l > 0$ for $l \in S_i$. But since S_1 and S_2 are distinct, this can not be the case. □

1.5 Extreme Point Adjacency

Next, we characterize when a pair of distinct vertices of the 1-skeleton of a clipped cube $\mathcal{Q}(\mathcal{C})$ are adjacent. Knowledge of these adjacencies enables us to trace out "simplex method paths" on $\mathcal{Q}(\mathcal{C})$ without resorting to the linear algebra of "pivoting". As is usual, if x^1 and x^2 are extreme points of $\mathcal{Q}(\mathcal{C})$ and x^1 and x^2 are adjacent in $G(\mathcal{Q}(\mathcal{C}))$, then we say that x^1 and x^2 are *adjacent* on $\mathcal{Q}(\mathcal{C})$.

Proposition 14 *Let $\mathcal{C}$ be a clippable subset of 2^N. Let $x^1 = x(S_1)$ and $x^2 = x(S_2)$ be distinct extreme points of $\mathcal{Q}(\mathcal{C})$. The point x^2 is adjacent to x^1 on $\mathcal{Q}(\mathcal{C})$ if and only if S_2 is derived from S_1 in one of the following ways:*

(i) $S_2 = S_1 + k$, *for some* $k \in N \setminus S_1$;

(ii) $S_2 = S_1 - k$, *for some* $k \in N$;

(iii) $S_2 = S_1 + k - l$ *for some* $k \in N \setminus S_1$, $l \in S_1$, *such that* $S_1 + k \in \mathcal{C}$ *or* $S_1 - l \in \mathcal{C}$;

(iv) $S_2 = S_1 + k + l$, *for some* $k, l \in N \setminus S_1$, *such that* $S_1 + k \in \mathcal{C}$;

(v) $S_2 = S_1 - k - l$, *for some* $k, l \in S_1$, *such that* $S_1 - k \notin \mathcal{C}$.

Proof: First we demonstrate, one by one, that if S_2 is derived from S_1 in one of the five ways specified in the statement of the result, then x^2 is adjacent to x^1. In each case, we demonstrate adjacency on $\mathcal{Q}(\mathcal{C})$ by displaying $n-1$ facet describing inequalities of $\mathcal{Q}(\mathcal{C})$ that are satisfied as equations by x^1 and x^2, and which, when written as equations, are linearly independent. We leave the details for the energetic reader to check.

(i) $S_2 = S_1 + k$:

- The $|S_1|$ simple upper bound inequalities (2) with $j \in S_1$;
- the $|N \setminus S_1| - 1$ simple lower bound inequalities (1) with $j \in (N \setminus S_1) - k$.

(ii) $S_2 = S_1 - k$: Since we can interchange the roles of x^1 and x^2, this follows from (i).

(iii) $S_2 = S_1 + k - l$: Since we can interchange the roles of x^1 and x^2, there is no loss of generality in assuming that $S_1 + k \in \mathcal{C}$.

- The $|S_1| - 1$ simple upper bound inequalities (2) with $j \in S_1 - l$;
- the $|N \setminus S_1| - 1$ simple lower bound inequalities (1) with $j \in (N \setminus S_1) - k$;
- the clipping inequality (3) with $S = S_1 + k$.

(iv) $S_2 = S_1 + k + l$:

- The $|S_1|$ simple upper bound inequalities (2) with $j \in S_1$;
- the $|N \setminus S_1| - 2$ simple lower bound inequalities (1) with $j \in (N \setminus S_1) - k - l$;
- the clipping inequality (3) with $S = S_1 + k$.

(v) $S_2 = S_1 - k - l$: Since we can interchange the roles of x^1 and x^2, this follows from (iv).

Next, for the converse, we must show that the distinct extreme points $x^1 = x(S_1)$ and $x^2 = x(S_2)$ are not adjacent on $\mathcal{Q}(\mathcal{C})$ if they are not covered by the five cases in the statement of the result. Because we have already verified cases (i–ii), we need only consider $|S_1 \triangle S_2| \geq 2$. A preliminary observation which is easily verified is the following:

Observation 1 *The only clipping inequalities (3) that are satisfied as equations by x^i have $S = S_i - k$ for some $k \in S$ or $S = S_i + k$ for some $k \in N \setminus S$.*

With this observation, it is easy to see that if $|S_1 \triangle S_2| \geq 3$, then no clipping inequality is satisfied as an equation by both x^1 and x^2. But no more than $n - 3$ simple bound inequalities (1–2) are satisfied by both x^1 and x^2, so we can not produce enough facets for x^1 and x^2 to be adjacent on $\mathcal{Q}(\mathcal{C})$. If $|S_1 \triangle S_2| = 2$, we note that we easily find $n - 2$ simple bound inequalities that are satisfied as equations by x^1 and x^2. So it suffices to show that there is no clipping inequality that is satisfied as an equation by x^1 and x^2. Without loss of generality, we can consider just two cases.

(A) $S_2 = S_1 + k + l$, for some $k, l \in N \setminus S_1$, such that $x(S_1 + k), x(S_1 + l) \in \mathcal{Q}(\mathcal{C})$: Here, we note that by the observation, the only sets S that produce clipping inequalities that need be considered have the form $S_1 \pm j_1 = S_2 \pm j_2$. We easily see that the only possibility is $S = S_1 + k$ and $S = S_1 + l$, but neither clipping inequality is valid by the hypothesis of case (A).

(B) $S_2 = S_1 + k - l$, for some $k \in N \setminus S_1$, $l \in S_1$, such that $x(S_1 + k), x(S_1 - l) \in \mathcal{Q}(\mathcal{C})$: Again, by the observation, we only consider sets S of the form $S_1 \pm j_1 = S_2 \pm j_2$. Here, the only possibility is $S = S_1 + k$ and $S = S_1 - l$, but neither clipping inequality is valid by the hypothesis of case (B).

□ The Hirsch Conjecture

is that the diameter of any polytope is bounded by the number of its facets minus the dimension. For the clipped cube $\mathcal{Q}(\mathcal{C})$, that would only give us a bound of $|\mathcal{C}| + n$. But Naddef verified the Hirsch conjecture for polytopes with vertices in $\{0,1\}^N$. Indeed, he demonstrated the stronger property that such polytopes always have diameter bounded by n ([29]). Of course this applies to the clipped cube $\mathcal{Q}(\mathcal{C})$, but for these we can *easily construct* short edge-paths between extreme points.

Proposition 15 *Let $\mathcal{C}$ be a clippable subset of 2^N. Let $x(S)$ and $x(T)$ be arbitrary extreme points of $\mathcal{Q}(\mathcal{C})$. Let $S_0, S_1, S_2, \ldots, S_p$ be any (easily constructed!) sequence of subsets of N satisfying*

(i) $S_0 = S$;

(ii) $S_p = T$;

(iii) $|S_i \triangle S_{i-1}| = 1$, *for* $i = 1, 2, \ldots p$;

(iv) $p = |S \triangle T| (\leq n)$.

Let $S'_0, S'_1, S'_2, \ldots, S'_{p'}$ be the subsequence obtained by deleting the S_i that are not in $\mathcal{C}$. Then

(i') $x(S'_0) = x(S)$;

(ii') $x(S'_{p'}) = x(T)$;

(iii') $x(S'_i)$ *is adjacent to* $x(S'_{i-1})$ *on* $\mathcal{Q}(\mathcal{C})$, *for* $i = 1, 2, \ldots p'$;

(iv') $p' \leq n$.

Proof: The idea is to derive paths on the clipped cube $\mathcal{Q}(\mathcal{C})$ from paths on the cube $[0,1]^N$. Figure 2 illustrates the idea. The result easily follows from Proposition 14. Figure 3 illustrates that the construction may fail if $\mathcal{C}$ is not clippable. □

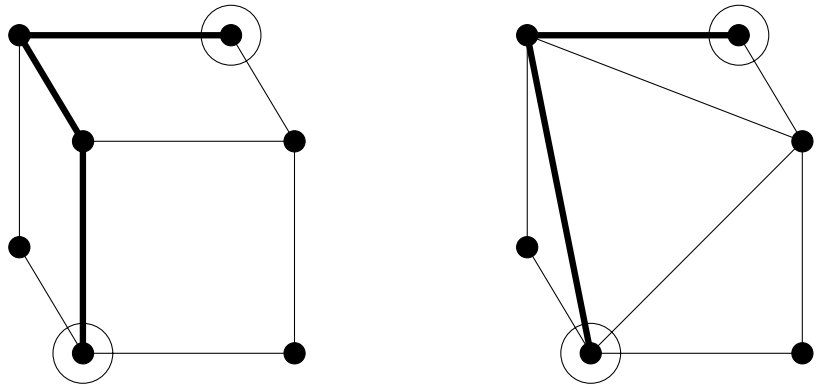

Figure 2: Transforming a path on a cube to one on a clipped cube

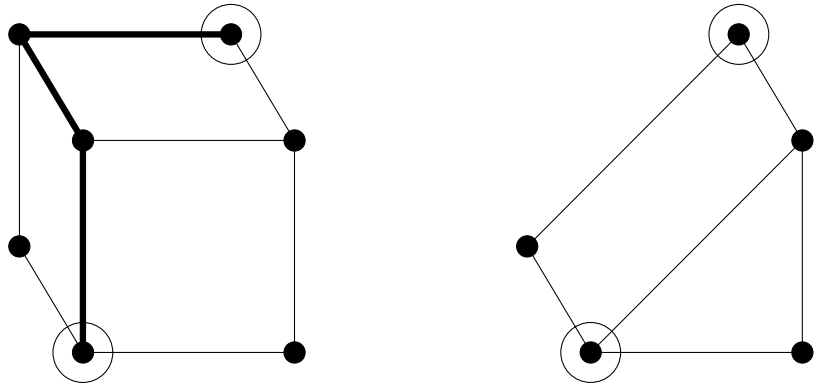

Figure 3: A lost path when $\mathcal{C}$ is not clippable

2 Indivisibility Polytopes

2.1 Dyadic Indivisibility Polytopes

For an integer $k \geq 0$, the *dyadic* indivisibility polytope $\mathcal{I}_{2^k n}$ is not so interesting. It is precisely the solution set of

$$\sum_{\substack{j \in N: \\ j < k}} x_j \geq 1 \ , \tag{13}$$

and the simple bound inequalities (1–2). In particular, we have the following result which is easily verified.

Proposition 16

(i) $\mathcal{I}_{2^0 n} = \emptyset$;

(ii) *A minimal equality/inequality description of* $\mathcal{I}_{2^1 n}$ *is given by the equation* $x_0 = 1$ *and the simple bound inequalities (1–2) for all* $j \in N - 0$;

(iii) *For integer* $\ell > 1$, *a minimal inequality description of the full dimensional* $\mathcal{I}_{2^\ell n}$ *is given by (13) and the simple bound inequalities (1–2) for all* $j \in N$.

Additionally, adjacency of extreme points is easily characterized for $\mathcal{I}_{2^k n}$. We have the following result which is easily verified.

Proposition 17

(i) *For* $S_1, S_2 \subset N - 0$, *let* $x^1 = x(0 + S_1)$ *and* $x^2 = x(0 + S_2)$ *be distinct extreme points of* $\mathcal{I}_{2^1 n}$. *Then* x^1 *and* x^2 *are adjacent precisely when* $|S_1 \triangle S_2| = 1$.

(ii) *For integer* $\ell > 1$, *let* $x^1 = x(S_1)$ *and* $x^2 = x(S_2)$ *be distinct extreme points of* $\mathcal{I}_{2^\ell n}$. *Then* x^1 *and* x^2 *are adjacent if and only if one of the following holds:*

  (a) $S_2 = S_1 + j$, *for some* $j \in N \setminus S_1$;

  (b) $S_2 = S_1 - j$, *for some* $j \in N$;

  (c) $S_2 = S_1 - j_1 + j_2$, $|\{j \in S_i \ : \ j < k\}| = 1$ *for* $i = 1, 2$, *and either* $\{j_1, j_2\} \subset \{j \in N \ : \ j < k\}$ *or* $\{j_1, j_2\} \subset \{j \in N \ : \ j \geq k\}$.

Therefore, in the sequel, we assume that **in the context of indivisibility polytopes,** p **is a positive integer that is not a power of 2.**

2.2 Nondyadic Indivisibility Polytopes

We have the following result which is easily verified.

Proposition 18 *Let* p *be a positive integer that is not a power of 2, and assume that* $n \geq 3$. *Let*

$$\mathcal{C}_{pn} := \left\{ S \in N \ : \sum_{j \in S} 2^j \cong 0 \pmod{p} \right\}.$$

Then $\mathcal{C}_{pn}$ *is clippable, so* $\mathcal{Q}(\mathcal{C}_{pn})$ *is a clipped cube.*

Proof: We verify C1–C3:

C1: 2^j is not divisible by p.

C2: If $p \neq 3$, then we observe that $\{0,1\} \in \mathcal{C}_{pn}$. On the other hand, if $p = 3$, then we observe that $\{0,2\} \in \mathcal{C}_{pn}$.

C3: If $\sum_{j \in S} 2^j \cong 0 \pmod{p}$, then $\sum_{j \in S \pm l} 2^j \ncong 0 \pmod{p}$.

□

In particular, all of the results of Section 1 apply to nondyadic indivisibility polytopes when $n \geq 3$.

2.2.1 Simple Bound Facets for Nondyadic Indivisibility Polytopes

Proposition 19 *The simple lower bound inequalities describe facets of $\mathcal{I}_{pn}$ when $n \geq 4$.*

Proof: Let $\mathcal{L}_{pn}(j)$ be the face of $\mathcal{I}_{pn}$ described by (1) for some $j \in N$. We will demonstrate that any other linear inequality that also describes $\mathcal{L}_{pn}(j)$ is just a positive multiple of (1). Suppose that

$$\sum_{k \in N} a_k x_k \leq b \tag{14}$$

describes $\mathcal{L}_{pn}(j)$. For all $k \in S - j$, $x(\{k\}) \in \mathcal{L}_{pn}(j)$, therefore, plugging into (14) as an equation, we obtain

$$a_k = b \ , \quad \forall \ k \in S - j \ . \tag{15}$$

Next, and this requires a bit of case checking, there is always a pair of distinct elements $l_1, l_2 \in N - j$ (indeed, in $\{0,1,2,3\} \setminus \{j\}$), so that p does not divide $2^{l_1} + 2^{l_2}$:

(i) for $j = 0$, we can take $l_1 = 1, l_2 = 3$ if $p = 3^\ell$ for some integer $\ell \geq 1$, and $l_1 = 1, l_2 = 2$ otherwise;

(ii) for $j = 1$, we can take $l_1 = 0, l_2 = 2$ if $p = 3^\ell$ for some integer $\ell \geq 1$, and $l_1 = 0, l_2 = 3$ otherwise;

(iii) for $j = 2$, we can take $l_1 = 1, l_2 = 3$ if $p = 3^\ell$ for some integer $\ell \geq 1$, and $l_1 = 0, l_2 = 1$ otherwise;

(iv) for $j \geq 3$, we can take $l_1 = 0, l_2 = 2$ if $p = 3^\ell$ for some integer $\ell \geq 1$, and $l_1 = 0, l_2 = 1$ otherwise.

For this choice of l_1, l_2, by plugging $x(\{l_1, l_2\})$ into (14) as an equation, we obtain

$$a_{l_1} + a_{l_2} = b \ . \tag{16}$$

Combining (15) and (16), we see that $b = 0$, and hence (14) has the form

$$a_j x_j \leq 0 \ . \tag{17}$$

Now $a_j \leq 0$ since otherwise (14) would exclude the point $x(\{j\}) \in \mathcal{I}_{pn}$, and $a_j \neq 0$ since $\mathcal{L}_{pn}(j)$ is nontrivial, therefore, (14) can be divided by $-a_j$ to obtain (1). □

Proposition 20 *The simple upper bound inequalities describe facets of $\mathcal{I}_{pn}$ when $n \geq 4$.*

Proof: Let $\mathcal{U}_{pn}(j)$ be the face of $\mathcal{I}_{pn}$ described by (2) for some $j \in N$. We will demonstrate that any other linear inequality that also describes $\mathcal{U}_{pn}(j)$ is just a positive multiple of (2). Suppose that (14) describes $\mathcal{U}_{pn}(j)$. First, we note that $x(\{j\}) \in \mathcal{U}_{pn}(j)$, so plugging this point into (14) as an equation, we obtain $a_j = b$. Next, for any $k \in N - j$, if p does not divide $2^j + 2^k$, we obtain $a_j + a_k = b$, which implies that $a_k = 0$. Next, suppose that $l \in N - j$ and p divides $2^j + 2^l$. Then we

$$\text{choose some } k \in N - j, \text{ such that } p \text{ does not divide } 2^j + 2^k \tag{18}$$

(*we need to check that we can do this!*). If p divides $2^j + 2^l$, then p can not divide $2^j + 2^k + 2^l$ (lest it divide the difference which is 2^k), therefore, plugging this into (14), we obtain $a_j + a_k + a_l = b$. But, we have already established that $a_0 = b$ and by the choice of k, we have $a_k = 0$, so we conclude that $a_l = 0$. To check (18) is always possible: If $n \geq 4$, there is some $k \in N - j$ (indeed, in $\{0, 1, 2, 3\} \setminus \{j\}$), so that p does not divide $2^j + 2^k$ (for $j \geq 2$, p cannot divide both $2^j + 2^0$ and $2^j + 2^1$, lest it divide the difference which is 1; for $j \leq 1$, p cannot divide both $2^j + 2^2$ and $2^j + 2^3$, lest it divide the difference which is 4). Therefore, we can conclude that $a_k = 0$ for all $k \in N - j$. Hence (14) has the form

$$a_j x_j \leq a_j \ . \tag{19}$$

Certainly $a_j \neq 0$ since $\mathcal{U}_{pn}(j)$ is nontrivial. Also, we can not have $a_j < 0$ since the inequality must be valid for $x(\{k\})$ for $k \in N - j$. Therefore, (14) is a positive multiple of (2). □

3 Factoring

In this section, we outline an approach to factoring a large (positive) integer y that can make use of our results. Other approaches to factoring are quite different (e.g., Pollard methods (see [33, 32]), the elliptic curve method (see [26, 28, 24]), the general number field sieve (see [7, 6, 16]), and the multiple polynomial quadratic sieve (see [34])). We wish to find a solution to

$$y = \sum_{i \in N} \sum_{j \in N} 2^{i+j} x_i^1 x_j^2 \tag{20}$$

in 0,1 variables x_i^1, x_j^2, where we choose n to be just less than the number of bits needed to encode y. In fact, we can make n even smaller, but always at least the number of bits needed to encode $\lceil \sqrt{y} \rceil$, if we check that y has no small factor (> 1). Working in a more general framework, Coppersmith, Lee and Leung demonstrated that *if y is treated as a variable*, then the convex hull of the solutions $(y, x^1, x^2) \in \mathbb{Z} \times \{0,1\}^N \times \{0,1\}^N$ to (20) is precisely the solution set of:

$$\begin{aligned}
& x_i^l \geq 0 \ , \quad \forall \ i \in N \ , \ l = 1, 2 \ ; \\
& x_i^l \leq 1 \ , \quad \forall \ i \in N \ , \ l = 1, 2 \ ; \\
& y \geq \sum_{(i,j) \in H} 2^{i+j} \left(x_i^1 + x_j^2 - 1 \right) \ , \quad \forall \ H \subset N \times N \ ; \\
& y \leq \sum_{i \in N} 2^i \sum_{j \in N} 2^j x_j^2 + \sum_{(i,j) \in H} 2^{i+j} \left(x_i^1 - x_j^2 \right) \ , \quad \forall \ H \subset N \times N \ .
\end{aligned}$$

So here is the idea. Treating y has fixed, we use linear programming methods to find an extreme-point minimum of

$$\sum_{i \in N} 2^i x_i^1 + \sum_{j \in N} 2^j x_j^2$$

subject to the above constraints. This can be done efficiently (see [14]).

We note that y and the constraint coefficients are quite large for problems of practical interest, so most (all?) readily available software for large-scale linear programming would not be appropriate. Some pivoting scheme using exact arithmetic could be used (e.g., Edmonds' "Q-pivoting" scheme seems particularly well suited (see [17, 18])).

Of course we really only seek a feasible integer solution, but our choice of objective function is guided by our particular interest in factoring y when it

is the product of a pair of large primes of comparable size. Such factorization problems are particularly relevant to breaking public key cryptosystems like RSA (see [27, 36, 5], for example)

It is likely that the minimizer is fractional. We can use generic partitioning methods like branch-and-bound or Gomory cutting planes in an effort to find an integer solution. We may key a branch-and-bound search on fixing the high-order variables so that we can then exploit techniques that can take advantage of knowing high-order bits of factors (see [11, 12, 13, 22]). We can use local-search heuristics like "pivot-and-complement" to seek an integer solution (see [2, 1]).

We can also try to exploit problem-specific structure to impose additional linear inequalities that exclude this solution but preserve potential integer solutions. For example, we may use other methods to find a set of numbers $\mathcal{P}$ that do not divide y — e.g., trial division or sophisticated sieve methods. Then, using techniques described in the present paper, we may start imposing the mod p inequalities for $p \in \mathcal{P}$ on the variables x_i^1 and x_j^2 of this linear program.

As we have seen, for each odd p, the clipping inequalities alone remove very little volume from the cube $[0,1]^N$. However, we can derive stronger inequalities. For example, suppose that $\mathcal{C}$ is an arbitrary subset of 2^N (possibly the union of several clippable sets). Let (S,T,U) be a partition of N with $U \neq N$. Suppose that

$$S \cup K \in \mathcal{C} \ , \quad \forall\ K \subset U \ .$$

Then it is easy to see that the *clopping inequality*

$$\sum_{j \in S} x_j - \sum_{j \in T} x_j \leq |S| - 1 \tag{21}$$

is valid for $\mathcal{Q}(\mathcal{C})$. Of course when $U = \emptyset$, the clopping inequality is just a clipping inequality, but the clopping inequality can cut off much more volume than the clipping inequalities from which it derives. The clopping inequality excludes all $2^{|U|}$ extreme points of the cube of the form $x(S+K)$ having $K \subset U$. So, the volume that the associated clipping inequalities remove is at most $2^{|U|}/n!$. On the other hand, the subset of $[0,1]^N$ removed by the clopping inequality is the cross product of the unit cube $[0,1]^U$ and the simplex cut from the unit cube $[0,1]^{S \cup T}$ by the clopping inequality. Hence, the clopping inequality removes a volume of $1/(|S|+|T|)!$ from the unit cube $[0,1]^N$. For example, for $k \in N$, when $S = \{k\}$ and $T = \emptyset$ (resp., $T = \{k\}$ and $S = \emptyset$), the clopping inequality fixes x_k at 1 (resp., 0), thus removing the

entire (n-dimensional) volume of the cube. As far as separation goes, given a membership oracle for $\mathcal{C}$, it is easy to adapt the separation procedure for clipping inequalities to find violated clopping inequalities having $|U|$ bounded by a polynomial in $\log n$.

4 Divisibility Polytopes

In this section, we define and investigate "divisibility polytopes". We will see that the facial structure of these polytopes is much more complicated than that of the indivisibility polytopes. Again, let p be a positive integer. We define the *divisibility polytopes*

$$\mathcal{D}_{pn} := \operatorname{conv}\left\{ x \in \{0,1\}^N \ : \ \sum_{j \in N} 2^j x_j \cong 0 \pmod{p} \right\}.$$

That is, $\mathcal{D}_{pn}$ is the polytope of binary n-strings that encode (positive) integers that *are* divisible by p. We can write p uniquely as $p = 2^k q$, where k is a nonnegative integer and q is odd. Let $m := n - k$. For $y \in \mathbb{R}^M$ and $z \in \mathbb{R}^K$, we consider the point $x = (y, z)$ to be in $\mathbb{R}^N$, where $x_j = z_j$ for $j \in K$ and $x_{j+k} = y_j$ for $j \in M$. Now, we observe that $x \in \mathcal{D}_{pn}$ if and only if $y \in \mathcal{D}_{qd}$ and $z = 0$. So we can easily obtain an equality/inequality description of $\mathcal{D}_{pn}$ from one for $\mathcal{D}_{qd}$. Therefore, in the sequel, we assume that **in the context of divisibility polytopes, p is an odd positive integer.**

Let r be any nonzero integer. Let let $a \in \mathbb{Z}^N$ be any point satisfying

$$a_j \cong r2^j \pmod{p} ,$$

for all $j \in N$. Let b be any real number satisfying

$$b \geq \max\left\{ \sum_{j \in N} a_j x_j \ : \ x \in \mathcal{D}_{pn} \right\}.$$

By the definition of b, the inequality

$$\sum_{j \in N} a_j x_j \leq b \tag{22}$$

describes a (possibly empty) face of $\mathcal{D}_{pn}$.

We note that we can calculate the least number b for which the inequality (22) is valid for $\mathcal{D}_{pn}$ in time polynomial in p, n and the $\log |a_j|$. When p is

very large, we can do this by enumerating the few multiples of p. When p is small, we can do this by solving a "group knapsack" shortest path problem on an acyclic digraph with pn nodes. Using standard methods, we can solve this shortest dipath problem in $\mathcal{O}(np)$ time. We would prefer to see $\mathcal{O}(n \log p)$, since it could well be that p is exponential in n and there are still an exponential number of multiples of p that are less than n; for example, if $p = \mathcal{O}(a^n)$, with $1 < a < 2$, then the number of multiples of p that are less than n is $\Omega((2/a)^n)$.

Proposition 21 *The least number b for which the inequality (22) is valid for $\mathcal{D}_{pn}$ is an integer multiple of p.*

Proof: The extreme points of $\mathcal{D}_{pn}$ satisfy

$$\sum_{j \in N} 2^j x_j \cong 0 \,(\text{mod } p) \ .$$
$$\sum_{j \in N} r 2^j x_j \cong 0 \,(\text{mod } p) \ .$$
$$\sum_{j \in N} a_j x_j \cong 0 \,(\text{mod } p) \ .$$

The result follows. □

We refer to any inequality obtained in this manner, having b an integer multiple of p, as an (r, p, n) *inequality*. If b is as small as possible so that (22) is valid for $\mathcal{D}_{pn}$, then (22) describes a nonempty face and we refer to (22) as a *proper* (r, p, n) *inequality*. An *elementary* (r, p, n) *inequality* is derived by taking an integer r that is relatively prime to p with $1 \leq r \leq p-1$, and a set S in

$$\bar{C}_{pn} := \left\{ S \in N \ : \sum_{j \in S} 2^j \not\cong 0 \pmod{p} \right\}.$$

Let $\bar{r} := p - r$. An elementary (r, p, n) inequality has the form

$$\sum_{j \in S} [r 2^j \,(\text{mod } p)] x_j - \sum_{j \in N \setminus S} [\bar{r} 2^j \,(\text{mod } p)] x_j \leq p \left\lfloor \frac{\sum_{j \in S} [r 2^j \,(\text{mod } p)]}{p} \right\rfloor \ . \quad (23)$$

We do have the following.

Proposition 22 *Every elementary (r, p, n) inequality is an (r, p, n) inequality (and hence valid for $\mathcal{D}_{pn}$).*

Proof: Clearly the variable coefficients a_j have the correct form. And the right-hand side is obviously an integer multiple of p.

So the only thing to check is that the inequality is valid. Now the left-hand side of (23) can not exceed $\sum_{j\in S}\left[r2^j \pmod p\right]$ on $\{0,1\}^N$. But since the left-hand side is a multiple of p for all extreme points of $\mathcal{D}_{pn}$, the left-side can not be greater than the greatest multiple of p that does not exceed $\sum_{j\in S}\left[r2^j \pmod p\right]$. □

Not every elementary (r,p,n) inequality is proper. For example, the reader can check that $S := \{1,5,7\} \in \bar{\mathcal{C}}_{37,9}$ (i.e., $x(S)$ is the binary encoding of 162, which is not divisible by 37), and the associated elementary $(r = 27, p = 37, n = 9)$ inequality has right-hand side 37, while a right-hand side of 0 is valid.

In addition, there are facets of $\mathcal{D}_{pn}$ that are described by (r,p,n) inequalities that are not elementary. For example, the reader can check that $\mathcal{D}_{109,11}$ has a facet that is described by the $(r = 50, p = 109, n = 11)$ inequality

$$-139x_{10}-15x_9+47x_8-31x_7-70x_6-35x_5+37x_4+73x_3-18x_2-9x_1+50x_0 \le 0\,,$$

which is not elementary since the coefficient of x_{10} is out of range.

Nonetheless, the following result indicates a central role played by the elementary (r,p,n) inequalities.

Proposition 23 *Let p be an integer greater than one, and let $x \in \{0,1\}^N$. If there is an r (that is relatively prime to p and satisfies $1 \le r \le p-1$) such that x satisfies all elementary (r,p,n) inequalities (23), then $x \in \mathcal{D}_{pn}$.*

Proof: Suppose that $x \in \{0,1\}^N$ is *not* in $\mathcal{D}_{pn}$. That is, p does not divide $\sum_{j\in N} 2^j x_j$. Or, $S := \{j \in N \ : \ x_j = 1\} \in \bar{\mathcal{C}}_{pn}$. Choose *any* integer r that is relatively prime to p and satisfies $1 \le r \le p-1$ (e.g., $r = 1$). So p does not divide $r\sum_{j\in S} 2^j$. Hence p does not divide $\sum_{j\in S}\left[r2^j \pmod p\right]$. So

$$\sum_{j\in N}\left[r2^j \pmod p\right] x_j = \sum_{j\in S}\left[r2^j \pmod p\right] > p\left\lfloor \frac{\sum_{j\in S}\left[r2^j \pmod p\right]}{p}\right\rfloor\,.$$

Therefore, x violates (23). □

A far simpler way to attempt to exclude the points $x(S)$ for $S \in \bar{\mathcal{C}}_{pn}$ is by using the clipping inequalities (3) for all $S \in \bar{\mathcal{C}}_{pn}$. Unfortunately, the set $\bar{\mathcal{C}}_{pn}$ is not clippable. So even though the set of 0,1 valued points satisfying the clipping inequalities (3) for all $S \in \bar{\mathcal{C}}_{pn}$ is precisely the set of extreme points of $\mathcal{D}_{pn}$, we should not expect that these clipping inequalities will describe facets

of $\mathcal{D}_{pn}$. Indeed, we show how even the elementary (r, p, n) inequalities imply these clipping inequalities.

Proposition 24 *Let p be an integer greater than one, and let $S \in \bar{\mathcal{C}}_{pn}$. Then the corresponding clipping inequality (3) is obtained by choosing any r that is relatively prime to p and satisfies $1 \leq r \leq p-1$ (e.g., $r = 1$), summing the associated elementary (r, p, n) and $(\bar{r}, p, n)$ inequalities, and then dividing by p.*

Proof: First, we demonstrate that the elementary $(\bar{r}, p)$ inequality in the statement of the proposition is valid for $\mathcal{D}_{pn}$. Any common factor of p and $\bar{r}$ is also a factor of their difference r. Therefore, p and $\bar{r}$ are relatively prime.

Next, we let

$$\sum_{j \in S} a_j x_j - \sum_{j \in N \setminus S} a_j x_j \leq \left(\left\lfloor \frac{\sum_{j \in S} \left[r 2^j \pmod{p} \right]}{p} \right\rfloor + \left\lfloor \frac{\sum_{j \in S} \left[\bar{r} 2^j \pmod{p} \right]}{p} \right\rfloor \right) p \quad (24)$$

be the sum mentioned in the statement of the proposition. In particular, for all $j \in N$, we have that

$$a_j = \left[r 2^j \pmod{p} \right] + \left[\bar{r} 2^j \pmod{p} \right] .$$

We easily observe that $a_j \cong 0 \pmod{p}$ and that $2 \leq a_j \leq 2(p-1)$, so therefore $a_j = p$.

It only remains to determine the value of the right-hand side of the inequality. We observe that

$$\frac{\sum_{j \in S} \left[r 2^j \pmod{p} \right]}{p} - 1 < \left\lfloor \frac{\sum_{j \in S} \left[r 2^j \pmod{p} \right]}{p} \right\rfloor < \frac{\sum_{j \in S} \left[r 2^j \pmod{p} \right]}{p}$$

and that

$$\frac{\sum_{j \in S} \left[\bar{r} 2^j \pmod{p} \right]}{p} - 1 < \left\lfloor \frac{\sum_{j \in S} \left[\bar{r} 2^j \pmod{p} \right]}{p} \right\rfloor < \frac{\sum_{j \in S} \left[\bar{r} 2^j \pmod{p} \right]}{p} .$$

Adding these inequalities together, and using that each $a_j = p$, we obtain

$$|S| - 2 < \left\lfloor \frac{\sum_{j \in S} \left[r 2^j \pmod{p} \right]}{p} \right\rfloor + \left\lfloor \frac{\sum_{j \in S} \left[\bar{r} 2^j \pmod{p} \right]}{p} \right\rfloor < |S| .$$

Therefore, the right-hand side of (24) is $(|S| - 1)p$. The result follows. □

Proposition 25 *For odd $p > 1$, let d ($\leq p-1$) be the order of 2 modulo p (i.e., d is the smallest positive integer k so that $2^k = 1$). If $n \geq pd+1$, then the polytope $\mathcal{D}_{pn}$ is full dimensional.*

Proof: Suppose that (4) is an equation satisfied by all points of $\mathcal{D}_{pn}$. Plugging in $x(\emptyset) = 0$, which is in $\mathcal{D}_{pn}$, we establish that $b = 0$.

Next, let $S := \{0, d, 2d, \ldots, pd\}$. We observe that $2^j \cong 1 \pmod{p}$, for all $j \in S$. Therefore, since $|S| = p+1$, we have $x(S-k) \in \mathcal{D}_{pn}$ for all $k \in S$. Plugging into (4), we obtain $\sum_{j \in S-k} a_j = 0$ for all $k \in S$. This system of $p+1$ linear equations in $p+1$ variables has the *unique* solution $a_j = 0$ for all $j \in S$.

Next, consider any $j \in N \setminus S$. Let T be any subset of $p - [2^j \pmod{p}]$ elements from S. Then $2^j + \sum_{k \in T} 2^k \cong 0 \pmod{p}$, so we have $x(T+j) \in \mathcal{D}_{pn}$. Hence, plugging into (4), we have $a_j + \sum_{k \in T} a_k = 0$, and we can conclude that $a_j = 0$.

Therefore, the only linear equations satisfied by all points of $\mathcal{D}_{pn}$ are trivial, and the result follows. □

Proposition 26 *For odd $p > 1$, let d be the order of 2 modulo p. If $n \geq (p+1)d+1$, then every simple lower bound (1) inequality describes a facet of $\mathcal{D}_{pn}$.*

Proof: Let $\mathcal{L}_{pn}(j)$ be the face of $\mathcal{D}_{pn}$ described by (1) for some $j \in N$. Suppose that (14) also describes $\mathcal{L}_{pn}(j)$. First, we note that $x(\emptyset) = 0$ is in $\mathcal{L}_{pn}(j)$, so $b = 0$. Let S be any subset of $p+1$ elements from $\{0, d, 2d, \ldots, pd, (p+1)d\} \setminus \{j\}$. We observe that $x(S-k) \in \mathcal{L}_{pn}(j)$ for all $k \in S$, and so, as in the proof of Proposition 25, we conclude that $a_k = 0$ for all $k \in S$. Next, for every $k \in N \setminus S$, let T_k be any subset of $p - [2^k \pmod{p}]$ elements from S. Also, like before, we observe that $x(T_k + k) \in \mathcal{L}_{pn}(j)$, and we can conclude that $a_k = 0$ for all $k \in N \setminus S$. Therefore, (14) has the form (17). Finally, since $x(T_j + j) \in \mathcal{D}_{pn} \setminus \mathcal{L}_{pn}(j)$, we observe that $a_j < 0$. Therefore, (14) is just a positive multiple of (1), and the result follows. □

Proposition 27 *For odd $p > 1$, let d be the order of 2 modulo p. If $n \geq 2pd+1$, then every simple upper bound (2) inequality describes a facet of $\mathcal{D}_{pn}$.*

Proof: Let $\mathcal{U}_{pn}(j)$ be the face of $\mathcal{D}_{pn}$ described by (2) for some $j \in N$. Suppose that (14) also describes $\mathcal{U}_{pn}(j)$. Let $S := \{0, d, 2d, \ldots, (2p-1)d, 2pd\} \setminus \{j\}$. Let $t := p - [2^j \pmod{p}]$. Then we have $x(T+j) \in \mathcal{U}_{pn}(j)$ for all $T \subset S$ such that $|T| = t$. Therefore, $a_j + \sum_{k \in T} a_k = b$ for all $T \subset S$ such that $|T| = t$. This system has the family of solutions $a_k = (b - a_j)/t$ for all $k \in S$, and it is unique since $|S| > t$. Similarly, if we instead require $|T| = t + p$, then we get

the family of solutions $a_k = (b - a_j)/(t + p)$ for all $k \in S$, and it is unique since $|S| > t + p$. Equating these solutions, we conclude that $b = a_j$ and $a_k = 0$ for all $k \in S$.

Next, consider any $i \in (N \setminus S) - j$. Choose any subset T of S having $|T| = p - [2^j + 2^i \pmod p]$. Since $x(T + j + i) \in \mathcal{U}_{pn}(j)$, we have $a_j + a_i + \sum_{k \in T} a_k = b$, which, by earlier observations reduces to $a_i = 0$. Therefore, (14) has the form (19). Finally, since $x(\emptyset) = 0 \in \mathcal{D}_{pn} \setminus \mathcal{U}_{pn}(j)$, we observe that $a_j > 0$. Therefore, (14) is just a positive multiple of (2). The result follows. □ Determining which elementary (r, p, n) inequalities describe facets has been elusive. We do have the following necessary condition.

Proposition 28 *Suppose that the divisibility polytope $\mathcal{D}_{pn}$ is full dimensional (see Proposition 25 for a sufficient condition), r is relatively prime to p and satisfies $1 \le r \le p - 1$, and set $S \in \bar{\mathcal{C}}_{pn}$. Let δ be the least positive number by which $\sum_{j \in S} r2^j$ exceeds an integer multiple of p. If the elementary (r, p, n) inequality (23) describes a facet of $\mathcal{D}_{pn}$, then*

$$r2^j \pmod p \le \delta \ , \qquad \forall\ j \in S \ ;$$
$$\bar{r}2^j \pmod p \le \delta \ , \qquad \forall\ j \in N \setminus S \ .$$

Proof: Suppose that $r2^j \pmod p$ (resp., $\bar{r}2^j \pmod p$) $> \delta$ for some $j \in S$ (resp., $j \in N \setminus S$). Then it is easy to see $x_j = 1$ (resp., $x_j = 0$) for any extreme point of $\mathcal{D}_{pn}$ that satisfies (23) as an equation. Since we assume that $\mathcal{D}_{pn}$ is full dimensional, we conclude that (23) does not describe a facet of $\mathcal{D}_{pn}$. □

Toward characterizing the facets of $\mathcal{D}_{pn}$, we describe the "basic hyperplanes" determined by the extreme points of $\mathcal{D}_{pn}$.

Proposition 29 *Let (4) be a nontrivial equation satisfied by n affinely independent extreme points of $\mathcal{D}_{pn}$. Then there is a nonzero scalar λ so that in the equivalent equation*

$$\sum_{j \in N} (\lambda a_j) x_j = \lambda b \ ,$$

λb and λa_j, $j \in N$, are all integers, λb is a multiple of p, and $2^l(\lambda a_j) \cong 2^j(\lambda a_l) \pmod p$ for all $j, l \in N$.

Proof: Let $x^0, x^1, \ldots, x^{n-1}$ be n affinely independent points of $\mathcal{D}_{pn}$ that satisfy (4). We arrange these points as rows of a matrix B, and we denote the columns of B by B^j, $j \in N$. The hypothesis of affine independence

implies that any nontrivial equation satisfied by the points $x^0, x^1, \ldots, x^{n-1}$ is a nonzero multiple of (4). We note that

$$\begin{aligned} & B \text{ nonsingular} \\ \Leftrightarrow\ & B\vec{\alpha} = \vec{0} \text{ has a nontrivial solution} \\ \Leftrightarrow\ & \text{there is a nontrivial equation } \sum_{j \in N} \alpha_j x_j = 0 \\ & \text{satisfied by the points } x^0, x^1, \ldots, x^{n-1} \\ \Leftrightarrow\ & b = 0 \ . \end{aligned}$$

So we consider two cases.
Case 1: Suppose that B is nonsingular. Then we let $\lambda := \det(B)/b$. Let $\vec{2} := (2^0, 2^1, \ldots, 2^{n-1})^T$, and let $\vec{k} \in \mathbb{Z}^N$ satisfy

$$B\vec{2} = p\vec{k} \ .$$

By Cramer's rule, we have

$$2^j = \frac{p \cdot \det(B^0|\cdots|B^{j-1}|\vec{k}|B^{j+1}|\cdots|B^{n-1})}{\det(B)} \ .$$

Since p is odd, and the two determinants are integers, we have that p divides $\det(B)$. So we conclude that λb is a multiple of p.

Letting $\vec{a} := (a_0, a_1, \ldots, a_{n-1})^T$, we can express (4), for the n points $x^0, x^1, \ldots, x^{n-1}$, as

$$B\vec{a} = be \ .$$

Applying Cramer's rule, we have

$$a_j = \frac{b \cdot \det(B^0|\cdots|B^{j-1}|e|B^{j+1}|\cdots|B^{n-1})}{\det(B)} \ ,$$

or

$$\lambda a_j = \det(B^0|\cdots|B^{j-1}|e|B^{j+1}|\cdots|B^{n-1}) \ .$$

So, for distinct $j, l \in N$, we have

$$\begin{aligned} \lambda a_j &= \det(B^0|\cdots|B^{j-1}|e|B^{j+1}|\cdots|B^{l-1}|B^l|B^{l+1}|\cdots|B^{n-1}) \\ &= \det(B^0|\cdots|B^{j-1}| - B^l|B^{j+1}|\cdots|B^{l-1}|e|B^{l+1}|\cdots|B^{n-1}) \qquad (25) \end{aligned}$$

and

$$\lambda a_l = \det(B^0|\cdots|B^{j-1}|B^j|B^{j+1}|\cdots|B^{l-1}|e|B^{l+1}|\cdots|B^{n-1}). \qquad (26)$$

From (25–26), we see that

$$\begin{aligned}
&2^j(\lambda a_l) - 2^l(\lambda a_j) \\
&\quad = \det(B^0|\cdots|B^{j-1}|2^lB^l + 2^jB^j|B^{j+1}|\cdots|B^{l-1}|e|B^{l+1}|\cdots|B^{n-1}) \\
&\quad = \det(B^0|\cdots|B^{j-1}|p\vec{k}|B^{j+1}|\cdots|B^{l-1}|e|B^{l+1}|\cdots|B^{n-1}),
\end{aligned}$$

the last equation being realized by adding the linear combination $\sum_{i\in N\setminus\{j,l\}} 2^iB^i$ of the columns $B^0,\ldots B^{j-1},B^{j+1},\ldots,B^{l-1},B^{l+1},\ldots,B^{n-1}$ to the column $2^lB^l+2^jB^j$. So we conclude that $2^j(\lambda a_l) - 2^l(\lambda a_j)$ is an integer multiple of p.
Case 2: Suppose that B is singular. Then the hypothesis of linear independence implies that for some $l \in N$, the matrix

$$\widetilde{B} = (B^0|\cdots|B^{l-1}|e|B^{l+1}|\cdots|B^{n-1})$$

is nonsingular. Furthermore, $a_l \neq 0$ in the nontrivial equation (4), otherwise the columns $B^0,\ldots,B^{l-1},B^{l+1},\ldots,B^{n-1}$ would be linearly dependent. So we let $\lambda := \det(\widetilde{B})/a_l$, and we easily obtain $\lambda a_l \in \mathbb{Z}$. Then

$$\begin{aligned}
&B\vec{a} = \vec{0} \\
&\sum_{j\in N-l} a_jB^j = -a_lB^l \\
&\sum_{j\in N-l} a_jB^j + a_le = -a_l(e-B^l) \\
&\widetilde{B}\begin{pmatrix} a_0 \\ \vdots \\ a_{l-1} \\ 1 \\ a_{l+1} \\ \vdots \\ a_{n-1} \end{pmatrix} = a_l(e-B^l)\ .
\end{aligned}$$

So, by Cramer's rule, we have, for $j \in N-l$,

$$a_j = \frac{\det(B^0|\cdots|B^{j-1}|a^l(e-B^l)|B^{j+1}|\cdots|B^{l-1}|e|B^{l+1}|\cdots|B^{n-1})}{\det(\widetilde{B})}\ ,$$

hence

$$\begin{aligned}
\lambda a_j &= \frac{\det(B^0|\cdots|B^{j-1}|a^l(e-B^l)|B^{j+1}|\cdots|B^{l-1}|e|B^{l+1}|\cdots|B^{n-1})}{a_l} \\
&= \det(B^0|\cdots|B^{j-1}|-B^l|B^{j+1}|\cdots|B^{l-1}|e|B^{l+1}|\cdots|B^{n-1}),
\end{aligned}$$

exactly as in (25). Also, by the definition of λ, we have (26) in this case as well. So the present case can be completed as in Case 1.

The result follows. □

Proposition 30 *Suppose that $\mathcal{D}_{pn}$ is full dimensional. Then every facet describing inequality of $\mathcal{D}_{pn}$ is an (r, p, n) inequality.*

Proof: Let (14) describe a facet $\mathcal{F}$ of $\mathcal{D}_{pn}$. Then there are n affinely independent points of $\mathcal{D}_{pn}$ that satisfy (14) as an equation. By Proposition 29, there is a $\lambda \neq 0$ so that λb and λa_j, $j \in N$, are all integers, λb is a multiple of p, and $2^l(\lambda a_j) \cong 2^j(\lambda a_l) \pmod{p}$ for all $j, l \in N$. We can arrange for λ to be positive, by interchanging a pair of rows in B or $\widetilde{B}$ in the construction defining λ from the proof of Proposition 29. Therefore, the facet $\mathcal{F}$ is also described by

$$\sum_{j \in N} (\lambda a_j) x_j \leq \lambda b \ . \tag{27}$$

Now, let r be the integer $\lambda a_l / 2^l$ for some $l \in N$ for which $a_l \neq 0$. So we have $2^l(\lambda a_j) \cong 2^l r 2^j \pmod{p}$. Since p does not divide 2^j, we can conclude that $\lambda a_j \cong r 2^j \pmod{p}$. So (27) is an (r, p, n) inequality. □

Acknowledgments

The research of Jon Lee was partially supported by a CORE Fellowship and by Sabbatical and Scholarly Leaves from the University of Kentucky. The authors are grateful to Komei Fukuda for making his program `cddr+` available. Evidence collected with the use of `cddr+` led to conjectures which led us to some of the results.

References

[1] Ronny Aboudi, Åsa Hallefjord, Reidun Helming, and Kurt Jörnsten. A note on the pivot and complement heuristic for 0-1 programming problems. *Operations Research Letters*, 8(1):21–23, 1989.

[2] Egon Balas and Clarence H. Martin. Pivot and complement — a heuristic for 0-1 programming. *Management Science*, 26(1):86–96, 1980.

[3] Claude Berge. Sur certains hypergraphes généralisant les graphes bipartites. In *Combinatorial theory and its applications, I (Proc. Colloq., Balatonfured 1969)*, pages 119–133. North-Holland, Amsterdam, 1970.

[4] Claude Berge. Balanced matrices. *Mathematical Programming*, 2:19–31, 1972.

[5] David M. Bressoud. *Factorization and primality testing*. Springer-Verlag, New York, 1989.

[6] Johannes Buchmann, Jürgen Loho, and Jörg Zayer. An implementation of the general number field sieve (extended abstract). In *Advances in cryptology — CRYPTO '93 (Santa Barbara, CA, 1993)*, pages 159–165. Springer, Berlin, 1994.

[7] Joe P. Buhler, Hendrick W. Lenstra, Jr., and Carl Pomerance. Factoring integers with the number field sieve. In *The development of the number field sieve*, pages 50–94. Springer, Berlin, 1993.

[8] Vijay Chandru and John Hooker. *Optimization methods for logical inference*. Wiley, New York, 1999.

[9] Michele Conforti and Gérard Cornuéjols. Balanced $0, \pm 1$-matrices, bicoloring and total dual integrality. *Mathematical Programming, Series A*, 71:249–258, 1995.

[10] Michele Conforti and Gérard Cornuéjols. A class of logic problems solvable by linear programming. *Journal of the Association of Computing Machinery*, 42(5):1107–1113, 1995.

[11] Don Coppersmith. Quadratic integer programming and factoring with a clue. *IBM Research Report RC20089*, 1995.

[12] Don Coppersmith. Finding a small root of a bivariate integer equation; factoring with high bits known. In Ueli Maurer, editor, *Eurocrypt '96 Proceedings. Berlin: Springer-Verlag Lecture Notes in Computer Science*, volume 1070, pages 178–189, 1996.

[13] Don Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*, 10(4):233–260, 1997.

[14] Don Coppersmith, Jon Lee, and Janny Leung. A polytope for a product of real linear functions in 0/1 variables. *IBM Research Report RC21568 (temporarily available at* `http://www.ms.uky.edu/~jlee/recent.html`*)*, 1999.

[15] Gérard Cornuéjols. *Combinatorial Optimization: Packing and Covering.* (manuscript), 1999.

[16] Bruce Dodson and Arjen K. Lenstra. NFS with four large primes: an explosive experiment. In *Advances in cryptology — CRYPTO '95 (Santa Barbara, CA, 1995)*, pages 372–385. Springer, Berlin, 1995.

[17] Jack Edmonds. Exact pivoting without the Euclidean algorithm. *(Unpublished notes) presented at ECCO VII*, 1994.

[18] Jack Edmonds and Jean-Francois Maurras. Note sur les Q-matrices d'Edmonds. (A note on Edmonds' Q-matrices). *RAIRO, Recherche opérationelle*, 31(2):203–209, 1997.

[19] Martin Grötschel, László Lovász, and Alexander Schrijver. The ellipsoid method and its consequences in combinatorial optimization. *Combinatorica*, 1(2):169–197, 1981.

[20] Martin Grötschel, László Lovász, and Alexander Schrijver. Corrigendum to our paper: "The ellipsoid method and its consequences in combinatorial optimization". *Combinatorica*, 4(4):291–295, 1984.

[21] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric algorithms and combinatorial optimization.* Springer-Verlag, Berlin, second edition, 1993.

[22] Nicholas Howgrave-Graham. Finding small roots of univariate modular equations revisited. In Darnell, Michael, editor, *Cryptography and coding. 6th IMA international conference, Cirencester, GB, December 17–19, 1997, Proceedings. Berlin: Springer. Lecture Notes in Computer Science*, volume 1355, pages 131–142, 1997.

[23] Chun-Wa Ko, Jon Lee, and Einar Steingrímsson. The volume of relaxed Boolean-quadric and cut polytopes. *Discrete Mathematics*, 163(1-3):293–298, 1997.

[24] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.

[25] Jon Lee and Walter D. Morris, Jr. Geometric comparison of combinatorial polytopes. *Discrete Applied Mathematics*, 55(2):163–182, 1994.

[26] Hendrick W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics. Second Series*, 126(3):649–673, 1987.

[27] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC Press, Boca Raton, FL, 1997. With a foreword by R. L. Rivest.

[28] Victor S. Miller. Use of elliptic curves in cryptography. In *Advances in cryptology — CRYPTO '85 (Santa Barbara, Calif., 1985)*, pages 417–426. Springer, Berlin, 1986.

[29] Denis Naddef. The Hirsch conjecture is true for (0,1)–polytopes. *Mathematical Programming, Series B*, 45(1):109–110, 1989.

[30] George L. Nemhauser and Laurence A. Wolsey. *Integer and combinatorial optimization*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons Inc., New York, 1988. A Wiley-Interscience Publication.

[31] Paolo Nobili and Antonio Sassano. $(0, \pm 1)$ ideal matrices. *Mathematical Programming, Series A*, 80(3):265–281, 1998.

[32] John M. Pollard. Theorems on factorization and primality testing. *Proceedings of the Cambridge Philosophical Society*, 76:521–528, 1974.

[33] John M. Pollard. A Monte Carlo method for factorization. *Nordisk Tidskrift for Informationsbehandling (BIT)*, 15(3):331–334, 1975.

[34] Robert D. Silverman. The multiple polynomial quadratic sieve. *Mathematics of Computation*, 48(177):329–339, 1987.

[35] Einar Steingrímsson. A decomposition of 2-weak vertex-packing polytopes. *Discrete and Computational Geometry*, 12:465–479, 1994.

[36] Douglas R. Stinson. *Cryptography*. CRC Press, Boca Raton, FL, 1995. Theory and practice.

[37] Klaus Truemper. Alpha-balanced graphs and matrices and GF(3)-representability of matroids. *Journal of Combinatorial Theory, Series B*, 32:112–139, 1982.

[38] Klaus Truemper. *Effective logic computation*. Wiley, New York, 1998.

[39] Günter M. Ziegler. *Lectures on polytopes*, volume 152 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.