1 Basics

Let us recall some definitions and results seen in the previous lectures. Proofs of all statements mentioned in here can be found in [2]. Unless otherwise stated, we always assume that \( P = \{ x : Ax \leq b \} \subseteq \mathbb{R}^n \) is a rational polyhedron. Hence, wlog, \( A, b \) have integer entries. \( ax \leq \lfloor \beta \rfloor \) is a Chvátal cut for \( P \) if \( a \in \mathbb{Z}^n \) and \( ax \leq \beta \) is a valid inequality for \( P \). Note that a Chvátal cut is satisfied by any point of \( P \cap \mathbb{Z}^n \). The convex set obtained by adding all Chvátal cuts is called the first Chvátal closure, and denoted by \( P^{(1)} \).

**Theorem 1** \( P^{(1)} = \{ x \in P : uAx \leq \lfloor ub \rfloor \ \forall u : 0 \leq u < 1, uA \in \mathbb{Z}^n \} \).

**Corollary 2** \( P^{(1)} \) is a rational polyhedron.

By adding to \( P^{(1)} \) all the Chvátal cuts valid for \( P^{(1)} \), we obtain the second Chvátal closure \( P^{(2)} \). The process can be iterated as to produce the 3rd, 4th,... the \( i \)-th Chvátal closure \( P^{(i)} \).

**Theorem 3** For each polyhedron \( P \subseteq \mathbb{R}^n \), there exists \( t \in \mathbb{N} \) such that \( P^{(t)} = P \).

**Lemma 4** Let \( F \) be a non-empty face of \( P \), \( t \in \mathbb{N} \). Then \( P^{(t)} \cap F = F^{(t)} \).

We will also use the following known fact in convexity.

**Theorem 5** (Carathéodory) Let \( x \in \text{conv}(X) \). There exists a set \( Y \subseteq X \) with \( |Y| \leq \dim(X) + 1 \) such that \( x \in \text{conv}(Y) \).

2 The optimization problem for the first Chvátal closure

A natural question is whether we can efficiently optimize over \( P^{(1)} \) in polynomial time. In this section we give a negative answer to this question.

**Definition 6** (Optimization problem for the Chvátal closure) Given: A system of linear inequalities defining a non-empty, rational polyhedron \( P \), \( c \in \mathbb{Z}^n \).

Conclude: \( P^{(1)} \) is empty, or find \( x^* \in P \) achieving \( \max_{x \in P^{(1)}} cx \), or that the latter problem is unbounded.

**Theorem 7** The Optimization problem for the Chvátal closure is NP-hard.

To prove Theorem 7, we will go through a series of reductions. We first need some definitions. Theorem 1 implies that

\[
P^{(1)} = \{ x \in P : (uA)x \leq \lfloor ub \rfloor, uA \in \mathbb{Z}^n, 0 \leq u < 1 \},
\]

where \( u \) represents a vector of non-negative multipliers of the rows of \( A \). We now introduce a different closure where we further restrict the multipliers. Let the \((\frac{1}{2}, \frac{1}{2})\)-closure of \( P \) be the following polyhedron:

\[
\hat{P} = \left\{ x \in P : \lambda Ax \leq \lfloor \lambda b \rfloor, \lambda A \in \mathbb{Z}^n, \lambda \in \left\{ 0, \frac{1}{2} \right\}^m \right\} .
\]

We can now define the decisions problems we will work with.

---

This is crucial. Many of the results stated here are not valid for irrational polyhedra.
Definition 8 (Membership problem for the Chvátal closure (MEC))

Given: A system of linear inequalities defining a rational polyhedron \( P \subseteq \mathbb{R}^n, x^* \in \mathbb{R}^n \);
Decide: if \( x^* \notin P \) (1).

Definition 9 (Membership problem for the \((0, \frac{1}{2})\)-closure (MOC))

Given: A system of linear inequalities defining a rational polyhedron \( P \subseteq \mathbb{R}^n, x^* \in \mathbb{R}^n \);
Decide: if \( x^* \notin \tilde{P} \).

Definition 10 (Weighted binary clutter problem (WBC))

Given: \( Q \in \{0,1\}^{r \times t}, d \in \{0,1\}^r, w \in \mathbb{Q}^t \geq 0 \);
Decide: if \( \exists z \in \{0,1\}^t : Qz \equiv d \mod 2, wz < 1 \).

WBC is known to be \( NP \)-complete, see [4]. We will reduce WBC to MOC, and then MOC to MEC. We will then use the equivalence of optimization and separation to deduce Theorem 7. In particular, we will show that MEC is \( NP \)-complete already for \((0, \frac{1}{2})\)-polytopes.

Remark: Notice that we have stated MEC and MOC such that YES-instances correspond to \( x^* \notin P \) (resp. \( \tilde{P} \)). Thanks to this, our problems are in \( NP \). To see this for MEC, just notice that a YES-certificate for the instance \((P, x^*)\) is simply a separating Chvátal cut, i.e. a vector \( u \in [0, 1)^m \) such that \( uAx^* > \lfloor ub \rfloor \) and \( uA \) is integral. Hence, \( ||uA||_\infty \leq ||A||_\infty \) and the encoding length of this certificate is therefore polynomially bounded in the encoding length of \( A \). The argument for MOC is analogous.

Before we proceed to the reductions, we need a preliminary lemma.

Lemma 11 Let \( \bar{x} \in P \). Then \( \bar{x} \notin \tilde{P} \) if and only if there exist \( \mu \in \{0,1\}^m \) such that \( \mu A \equiv 0 \mod 2, \mu b \equiv 1 \mod 2, \mu(b - A\bar{x}) < 1 \).

Proof We have that \( \bar{x} \notin \tilde{P} \) if and only if one of the inequalities defining \( \tilde{P} \) is violated, i.e.:

\[
\exists \lambda \in \left\{0, \frac{1}{2}\right\}^m : \lambda A \in \mathbb{Z}^n, \lambda A \bar{x} > \lfloor \lambda b \rfloor. \tag{1}
\]

Now, since \( \bar{x} \in P \), and for such \( \lambda \) the inequality \( \lambda A \bar{x} \leq \lambda b \) is valid for \( P \), we have that \( \lambda A \bar{x} \leq \lambda b \), hence \( \lambda b \) must be fractional. Moreover 2\( \lambda \) is an integer (since 2\( \lambda \) and \( b \) are integers), hence \( \lambda b \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z} \), i.e., \( \lambda b = \lfloor \lambda b \rfloor + \frac{1}{2} \). Therefore \( \lambda A \bar{x} > \lfloor \lambda b \rfloor \) can be rewritten as \( \lambda(b - A\bar{x}) < \frac{1}{2} \), so we showed that condition (1) is equivalent to:

\[
\exists \lambda \in \left\{0, \frac{1}{2}\right\}^m : \lambda A \in \mathbb{Z}^n, \lambda b \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}, \lambda(b - A\bar{x}) < \frac{1}{2}.
\]

Now setting \( \mu = 2\lambda \) completes the proof. □

Theorem 12 MOC is \( NP \)-complete.

Proof We already argued that MOC is in \( NP \). Now, given a instance \((Q, d, w)\) of WBC, consider the following instance of MOC.

\[
A = \left( \begin{array}{c|c} Q^T & 2I_{t+1} \\ \hline d & \end{array} \right), \quad b = \left( \begin{array}{c} 2, \ldots, 2, 1 \end{array} \right), \quad \bar{x} = \left( \begin{array}{c} 0, \ldots, 0, 1 - \frac{1}{2}w_1, \ldots, 1 - \frac{1}{2}w_t, \frac{1}{2} \end{array} \right),
\]

2
where \( Q \in \{0,1\}^{r \times t} \) and \( I_{t+1} \) is the identity matrix of size \( t+1 \times t+1 \). We will show that \( (P = \{x : Ax \leq b\}, \bar{x}) \) is a YES-instance of MOC if and only if \((Q,d,w)\) is a YES-instance of WBC. One easily checks that \( A\bar{x} \leq b \), i.e., \( x \in P \). Thanks to Lemma 11 we have:

\[
\bar{x} \notin \bar{P} \iff \exists \mu \in \{0,1\}^{t+1} : \mu A \equiv 0 \mod 2, \mu b \equiv 1 \mod 2, \mu(b - A\bar{x}) < 1.
\]

Since \( \mu b = 2\mu_1 + \ldots + 2\mu_t + \mu_{t+1} \equiv \mu_{t+1} \mod 2 \). Now, let \( \bar{\mu} = (\mu_1, \ldots, \mu_t) \). If \( \mu_{t+1} = 1 \) we have:

\[
\mu A = \left( \bar{\mu} Q + \bar{d} \mid 2\mu_1 \mid \ldots \mid 2\mu_t \right).
\]

Hence,

\[
\mu A \equiv 0 \mod 2 \iff \bar{\mu} Q + \bar{d} \equiv 0 \mod 2 \iff \bar{\mu} Q \equiv \bar{d} \mod 2.
\]

Moreover, it is easy to verify that \( \mu(b - A\bar{x}) = \bar{\mu} w \), so \( \mu(b - A\bar{x}) < 1 \) if and only if \( \bar{\mu} w < 1 \). Hence choosing \( z = \bar{\mu} \) gives:

\[
\bar{x} \notin \bar{P} \iff \exists z \in \{0,1\}^t : Qz \equiv d \mod 2, wz < 1,
\]

which completes the proof. ■

To prove \( NP \)-completeness for MEC, we show that when the instance has the particular form given in the proof of Theorem 12, MEC and MOC are actually the same problem.

**Lemma 13** Let \( P = \{x : Ax \leq b\}, b \) integral, and \( A = (C|2I_m) \) with \( C \) integral. Then \( \bar{P} = P'. \)

**Proof** \( P' \subseteq \bar{P} \) is trivially true in general. For the other inclusion, we will show that any non-redundant inequality in the description of \( P' \) can be obtained with multipliers 0 or 1/2. Let \( u \) be such that \( 0 \leq u < 1 \), \( uA \in \mathbb{Z}^n \). The latter implies that in particular \( u \cdot 2I_m \in \mathbb{Z}^n \), hence \( u \in \frac{1}{2}\mathbb{Z}^n \), which together with \( 0 \leq u < 1 \) implies \( u \in \{0,\frac{1}{2}\}\). ■

**Corollary 14** MEC is \( NP \)-complete.

### 2.1 From membership to optimization

What remains to show is how Theorem 7 follows from Corollary 14. This will come as a consequence of a more general theorem on the equivalence between separation and optimization problems.

**Definition 15** (Optimization problem)

Given: A rational polyhedron \( P \subseteq \mathbb{R}^n, c \in \mathbb{Z}^n \).

Conclude: \( Q \) is empty, or find \( x^* \in P \) achieving \( \max_{x \in P} cx \), or that the latter problem is unbounded.

**Definition 16** (Separation problem)

Given: A rational polyhedron \( P \subseteq \mathbb{R}^n, x^* \in \mathbb{R}^n \).

Conclude: \( x^* \in P \), or output an hyperplane \( ax \leq \beta \) valid for \( P \) such that \( cx^* > \beta \).

Clearly these problems can be considered for families of polyhedra as well. Notice that we were intentionally vague on how the input polyhedron \( P \) is given as input in the previous problems. A classical, "explicit" way, is to give it as a set of inequalities. A more interesting one for our problem, would be to consider the case \( P = Q^{(1)} \) for some rational polyhedron \( Q \), and give the inequality description of \( Q \) as input. The next definition deals with this and other "implicit" ways to describe a polyhedron.
Definition 17 A family of polyhedra \( \mathcal{P} \) is well-described if for any \( P \in \mathcal{P} \cap \mathbb{R}^n \) with input length \( L \) we have:

- \( L \geq n \);
- there exist \( A, b \) rational such that \( P = \{ x \in \mathbb{R}^n : Ax \leq b \} \) and the encoding size of each entry of \( A \) and \( b \) is polynomially bounded by \( L \).

Lemma 18 Let \( \mathcal{Q} \) be a family of rational polytopes. Then \( \mathcal{Q} \) well-describes the family \( \mathcal{P} = \{ P = Q^{(1)} : Q \in \mathcal{Q} \} \).

Proof Let \( Q = \{ x \in \mathbb{R}^n : Ax \leq b \} \in \mathcal{Q} \) and \( Q^{(1)} = \{ x \in \mathbb{R}^n : \bar{A}x \leq \bar{b} \} \). Clearly \( L \geq n \). We know that each inequality \( \bar{a}x \leq \beta \) satisfies \( \bar{a} = uA \in \mathbb{Z}^n, \beta = \lfloor ub \rfloor, 0 \leq u \leq 1 \), and as already seen this implies that the encoding length of \( \bar{a}, \beta \) is polynomial in the encoding length of \( A, b \).

Now, the only missing ingredient is the following celebrated theorem.

Theorem 19 (Equivalence of separation and optimization) Let \( \mathcal{P} \) be a family of well-described polyhedra. Then the optimization problem over \( \mathcal{P} \) can be solved in polynomial time if and only if the separation problem can.

This result allows us to conclude the proof of Theorem 7. Indeed, Corollary 14 shows that problem MEC is \( NP \)-complete already for polytopes, so unless \( P = NP \) there is no polynomial-time algorithm that solves it. But notice that solving the separation problem for some polytope \( P^{(1)} \), when a linear description of \( P \) is given as input, is at least as hard as MEC on input \( P \). Thanks to Theorem 19, we conclude that the Optimization problem for the Chvátal closure is \( NP \)-hard.

2.2 The membership problem when \( P^{(1)} = P_I \)

When \( P^{(1)} = P_I \), there is evidence suggesting that the membership problem should be more tractable than MEC. We consider here the case \( P \subseteq [0,1]^n \).

Definition 20 (Special membership problem for the Chvátal closure (SMEC))

Given: A system of linear inequalities defining a rational polytope \( P \subseteq [0,1]^n \) such that \( P^{(1)} = P_I \), \( x^* \in \mathbb{R}^n \);

Decide: if \( x^* \not\in P^{(1)} \).

Theorem 21 SMEC \( \in NP \cap coNP \).

Proof SMEC \( \in NP \): The multipliers generating a Chvátal cut separating \( x^* \) from \( P^{(1)} \) is a compact "YES" certificate (see the proof that MEC is in \( NP \)).

SMEC \( \in coNP \): A short certificate for \( x^* \in P^{(1)} = P_I \) is a "small" set of points \( x_1, \ldots, x_t \in \mathbb{Z}^n \cap P \) s.t. \( x^* \in conv(x_1, \ldots, x_t) \). Such a set with \( t \leq n + 1 \) exists by Caratheorody’s theorem.

Remark: it is conjecture (and widely believed true) that no \( NP \)-complete problem lies in \( NP \cap coNP \).

In a previous lecture, we saw that the matching polytope of a graph satisfies \( P_I = P^{(1)} \), where \( P \) is the relaxation containing nonnegativity and \( x(\delta(v)) \leq 1 \) for all vertex \( v \). We show here another relevant class of polytopes for which \( P_I = P^{(1)} \). Recall that, for a graph \( G \), \( STAB(G) \) is the convex hull of the characteristic vectors of stable (or independent) sets in the graph. The following is clearly a relaxation for \( STAB(G) \).

\[
\{ x \in \mathbb{R}^n : x \geq 0, x_u + x_v \leq 1 \quad \forall \ uv \in E, \ x(C) \leq \frac{\gamma(C)}{2} \quad \forall \ odd \ cycle \ C \subseteq E \}.
\]
Definition 22 A graph $G$ is t−perfect if and only if $\text{STAB}(G) = t − \text{STAB}(G)$.

Exercise 1 Let $G$ be a graph and $P_G = \{x \in \mathbb{R}^n : x \geq 0, x_u + x_v \leq 1 \forall uv \in E\}$. Then $P_G^{(1)} = \text{STAB}(G)$.

We have seen in Section 2.1 that the two problems of separation and optimization are polynomial-time reducible to each other. Using this fact, the following lemma implies that optimizing over $\text{STAB}(G)$ for a $t$−perfect graph $G$ can be solved in polynomial time.

Lemma 23 The separation problem over $\text{STAB}(G)$ for a $t$−perfect graph $G$ can be solved in polynomial time.

Proof We give an algorithm that, given a graph $G$ and $x^* \in \mathbb{R}^n$, checks in polynomial time if $x^*$ satisfies (1), (2), (3), and outputs a violated inequality if it does not. There are only polynomially many equations in (1) and (2), so we can check all of them by enumeration. Provided that (1) and (2) are satisfied, we define $y_e = 1 - x^*_u - x^*_v \geq 0 \forall e = uv \in E$. Note that for any odd cycle $C \subseteq E$, $|C| - y(C) = 2x^*(C)$. Hence (3) is satisfied if and only if $y(C) \geq 1$ for any odd cycle $C$ in $E$. The problem of finding a minimum weight odd cycle in a graph with non-negative weights can be solved by a polynomial number of shortest path computations (again on a graph with non-negative weights), and the latter can be solved in polynomial time.

3 Upper bounds on the Chvátal rank of rational polytopes in the 0/1 cube

Recall from Theorem 3 that, for each rational polyhedron, there exists $t \in \mathbb{N}$ such that $P^{(t)} = P_I$. The smallest $t$ for which this holds is called the Chvátal rank of $P$.

Definition 24 The Chvátal rank of a polyhedron $P$ is $r(t) = \min \{t \in \mathbb{N} : P^{(t)} = P_I\}$.

So the rank of $P$ is the number of Chvátal closures one needs to perform, starting from $P$, before obtaining the polytope $P_I$. In general, there is no upper bound depending for the Chvátal rank of polyhedra that only depends on the dimension. One can easily construct example of polytopes in dimension 2 with arbitrarily high Chvátal rank. The goal of this section is to show that, for a rational polytope $P$ contained in the unit cube $[0, 1]^n$, the rank is $O(n^2 \log n)$. Let us first state some lemmas.

Lemma 25 Let $P \subseteq [0, 1]^n$ be a rational polytope with $\dim(P) = d$ such that $P_I = \emptyset$. Then $r(P) \leq d$ if $d \geq 1$ and $r(P) = 1$ if $d = 0$.

Proof Let first $d = 0$, say $P = \{x\}$. Then, since $P_I = \emptyset$, $\exists i : 0 < x_i < 1$. Thus, for some $\epsilon > 0$, $x_i \leq 1 - \epsilon$, $-x_i \leq -\epsilon$ are valid for $P$ and hence $x_i \geq 1, x_i \leq 0$ are both valid for $P^{(1)}$, implying $P^{(1)} = \emptyset$.

The case $d = 1$ is similarly easy, and left as an exercise.

Let now $d \geq 2$. We prove the statement by induction on both $n$ and $d$.

Case 1: $P \subseteq \{x_1 = 0\}$ or $P \subseteq \{x_1 = 1\}$. $P$ can be seen as a $d$−dimensional polytope in dimension $n − 1$. Hence by induction we conclude $P^{(d)} = \emptyset$.

Case 2: $P \not\subseteq \{x_1 = 1\}$, $P \not\subseteq \{x_1 = 0\}$. Let $F_1 = P \cap \{x_1 = 1\}$. Then $F_1$ is a polytope of dimension $\dim(F_1) \leq d − 1$, $F_1 \subseteq [0, 1]^{n−1}$ and $(F_1)_I = \emptyset$, so by induction $F_1^{(d−1)} = \emptyset$. By Lemma 4, we deduce $P^{(d−1)} \cap F_1 = \emptyset$, i.e. $P^{(d−1)} \subseteq \{x : x_1 < 1\}$. Repeating the argument with $F_0 = P \cap \{x_1 = 0\}$ gives us that $P^{(d−1)} \subseteq \{x : 0 < x_1 < 1\}$. As seen before, this implies $P^{(d)} = (P^{(d−1)})^{(1)} = \emptyset$.

A key concept for the current section is that of saturation of a vector. Let $P \subseteq [0, 1]^n$ and $c \in \mathbb{Z}^n$. We say that $c$ is saturated after $t$ rounds if $\max\{cx : x \in P^{(t)}\} = \max\{cx : x \in P_I\}$.

The next lemma can be shown in an analogous fashion to Lemma 4 by building on Lemma 25.

\footnote{Note that both maxima always exist, since we are dealing with polytopes.}
Theorem 28 Let \( t \) be the system is saturated after \( d \gamma - \beta \) rounds. Moreover, if \( \forall \alpha > \beta, \alpha \in \mathbb{R} \), \( P_{\alpha} = \{ x \in P : cx = \alpha \} \) does not intersect any of the facets \( F_{i}^{k} = P \cap \{ x_{i} = \ell \} \) from some \( i \) and \( \ell = 0, 1 \), then \( c \) is saturated after \( 2[\gamma - \beta] \) rounds.

The following lemma can be proved using the Hadamard bound for the determinant of a matrix.

Lemma 27 Every polytope \( P \subseteq \mathbb{R}^{n} \) whose vertices have coordinates \( 0 \) or \( 1 \) can be described by inequalities \( cx \leq \beta \) with \( \log ||c||_{\infty} = O(n \log n) \).

We can now prove the main result of this section.

Theorem 28 Let \( P \subseteq [0, 1]^{n} \) be a rational polytope. Then \( r(P) = O(n^{2} \log n) \).

Proof Let \( P_{I} = \{ x \in \mathbb{R}^{n} : Cx \leq d \} \), with \( C, d \) integral. We show that each inequality \( cx \leq \delta \) from the system is saturated after \( t \) rounds, with \( t = 2n^{2} + 2n \log ||c||_{\infty} \). The statement then follows using Lemma 27.

By flipping the coordinates, we can suppose \( c \geq 0 \). We can proceed by induction on \( n, \log ||c||_{\infty} \). The cases \( n = 1, 2, \log ||c||_{\infty} \leq 1 \) are easy (they can be shown e.g. using Lemma 26), so let us assume \( n \geq 3, \log ||c||_{\infty} \geq 2 \). Write \( c = 2c^{(1)} + c^{(2)} \) where \( c^{(1)} = \lfloor \frac{c}{2} \rfloor, c^{(2)} \in \{0, 1\}^{n} \).

By induction, \( c^{(1)} \) is saturated after \( 2n^{2} + 2n \log ||c^{(1)}||_{\infty} = 2n^{2} + 2n \log ||c^{(2)}||_{\infty} = 2n = k \) rounds. The next claim tells us that, after \( k \) rounds, \( c \) is not too far from being saturated as well.

Claim 29 Let \( \beta = \max\{ cx : x \in P_{I} \}, \gamma = \max\{ cx : x \in P_{I} \} \). Then \( \gamma - \beta \leq n \).

Proof Let \( \tilde{x} \in P^{(k)} \) such that \( c \tilde{x} = \gamma \), and \( \tilde{x} \in P_{I} \) such that \( c^{(1)}\tilde{x} = \max_{x \in P_{I}} c^{(1)}x \), where the latter equality holds since \( c^{(1)} \) is saturated after \( k \) rounds. We have \( \gamma - \beta \leq c(\tilde{x} - \bar{x}) = 2c^{(1)}(\tilde{x} - \bar{x}) + c^{(2)}(\tilde{x} - \bar{x}) \leq n \), where last inequality follows from the fact that \( c^{(1)}(\tilde{x} - \bar{x}) \leq 0 \), and \( ||c^{(2)}||_{1} \leq n \).

The next claim enables us to use the stronger bound from Lemma 26.

Claim 30 For all \( \alpha > \beta, \{ x \in P^{(k)} : cx = \alpha \} \) does not intersect any facet of the cube.

Proof For \( i \in [n] \) and \( \ell = 0, 1 \), let \( F_{i}^{\ell} \) be the face of \( P \) obtained by intersecting \( P \) with \( x_{i} = \ell \). Let \( c^{-i} \in \mathbb{Z}^{n-1} \) be the vector \( c \), minus the \( i \)-th component. By induction hypothesis, it is saturated after

\[
2(n - 1)^{2} + 2(n - 1) \log ||c^{-i}||_{\infty} \leq 2n^{2} + 2 - 4n + 2(n - 1) \log ||c||_{\infty} \leq 2n^{2} + 2n \log ||c||_{\infty} - 2n = k
\]

rounds. Hence \( \max\{ c^{-i}x : x \in (F_{i}^{\ell})^{(k)} \} \leq \beta - \ell \alpha \leq \beta < \alpha \), so the set \( \{ x \in P^{(k)} : cx = \alpha \} \) does not intersect \( F_{i}^{\ell} \). Since the intersection of \( \{ x \in P^{(k)} : cx = \alpha \} \) with the facet of the cube \( \{ x \in \mathbb{R}^{n} : x_{i} = \ell \} \) is contained in \( F_{i}^{\ell} \), the thesis follows.

Using Lemma 26 and the two claims above, we conclude that \( c \) will be saturated after

\[
k + 2[\gamma - \beta] \leq 2n^{2} + 2n \log ||c||_{\infty} - 2n + 2n = 2n^{2} + 2n \log ||c||_{\infty} \text{ rounds},
\]

as required. □
4 Notes

Theorem 12 appeared in [3], while Theorem 14 appeared in [5]. The discussion in Section 2.1 follows the treatment in [2]. Lemma 25 is proved in [1]. Lemma 26 is the union of two lemmas, one from [1] and the other from [6]. Theorem 28 appeared in [6]. Better constants in some of the bounds given here are known.

References


