

Truthful and Near-Optimal Mechanism Design via Linear Programming

RON LAVI, Technion – Israel Institute of Technology
 CHAITANYA SWAMY, University of Waterloo

We give a general technique to obtain approximation mechanisms that are truthful in expectation. We show that for packing domains, any α -approximation algorithm that also bounds the integrality gap of the LP relaxation of the problem by α can be used to construct an α -approximation mechanism that is truthful in expectation. This immediately yields a variety of new and significantly improved results for various problem domains and furthermore, yields truthful (in expectation) mechanisms with guarantees that match the best known approximation guarantees when truthfulness is not required. In particular, we obtain the first truthful mechanisms with approximation guarantees for a variety of multi-parameter domains. We obtain truthful (in expectation) mechanisms achieving approximation guarantees of $O(\sqrt{m})$ for combinatorial auctions (CAs), $(1 + \epsilon)$ for multi-unit CAs with $B = \Omega(\log m)$ copies of each item, and 2 for multi-parameter knapsack problems (multi-unit auctions).

Our construction is based on considering an LP relaxation of the problem and using the classic VCG mechanism to obtain a truthful mechanism in this fractional domain. We argue that the (fractional) optimal solution scaled down by α , where α is the integrality gap of the problem, can be represented as a convex combination of integer solutions, and by viewing this convex combination as specifying a probability distribution over integer solutions, we get a randomized, truthful in expectation mechanism. Our construction can be seen as a way of exploiting VCG in a computationally tractable way even when the underlying social-welfare maximization problem is NP-hard.

Categories and Subject Descriptors: F.2.2 [Analysis of Algorithms and Problem Complexity]: Nonnumerical Algorithms and Problems; I.2.m [Artificial Intelligence]: Miscellaneous; J.4 [Social and Behavioral Sciences]: Economics

General Terms: Theory, Algorithms, Economics

Additional Key Words and Phrases: Combinatorial auction, truthful and computationally-efficient mechanisms

ACM Reference Format:

Lavi, R., and Swamy, C. 2012. Truthful and Near-Optimal Mechanism Design via Linear Programming. *J. ACM* 9, 4, Article 39 (March 2010), 22 pages.
 DOI = 10.1145/0000000.0000000 <http://doi.acm.org/10.1145/0000000.0000000>

1. INTRODUCTION

Mechanism design studies algorithmic constructions under the presence of “selfish players” who hold the inputs to the algorithm. The players are selfish in that they are interested in maximizing their own utility, and instead of revealing the true input, they may declare any false input that will increase their utilities. The goal is to design algorithms that work well with respect to the *true*

A preliminary version [Lavi and Swamy 2005] appeared in the Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science, 2005.

Author’s addresses:

R. Lavi, Faculty of Industrial Engineering and Management, Technion – Israel Institute of Technology. Supported in part by grants from the Bi-national US-Israel Science Foundation, the Israeli ministry of science, and by the Google Inter-university center for Electronic Markets and Auctions. Work done while the author was a postdoctoral scholar at Caltech, Pasadena, CA 91125. Email: ronlavi@ie.technion.ac.il.

C. Swamy, Department of Combinatorics & Optimization, University of Waterloo, Waterloo, ON N2L 3G1. Research supported partially by NSERC grant 327620-09 and an Ontario Early Researcher Award. Work done while the author was a postdoctoral scholar at Caltech, Pasadena, CA 91125. Email: cswamy@math.uwaterloo.ca.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies show this notice on the first page or initial screen of a display along with the full citation. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, to redistribute to lists, or to use any component of this work in other works requires prior specific permission and/or a fee. Permissions may be requested from Publications Dept., ACM, Inc., 2 Penn Plaza, Suite 701, New York, NY 10121-0701 USA, fax +1 (212) 869-0481, or permissions@acm.org.

© 2010 ACM 0004-5411/2010/03-ART39 \$10.00

DOI 10.1145/0000000.0000000 <http://doi.acm.org/10.1145/0000000.0000000>

input, although this information is not publicly known. Mechanism design approaches this goal by specifying along with the algorithm a pricing scheme that can be used to incentivize the players to reveal their true inputs. A *mechanism* consists of an algorithm along with a pricing scheme, whose output specifies both an algorithmic outcome and prices to be charged to the players; the utility that a player derives is the difference between his value for the algorithmic outcome and the price that he is charged. A mechanism is said to be *truthful* if a player always maximizes his utility by declaring his true input, regardless of what the other players declare. Algorithmic mechanism design [Nisan and Ronen 2001] deals with the study of efficiently computable truthful mechanisms. The hope is that by obtaining a truthful mechanism, one can focus on the algorithmic question and set aside the strategic issue, however unfortunately not all algorithms lead to truthful mechanisms. This is best exemplified when the underlying algorithmic problem is *NP*-hard. Over the past several years, approximation algorithms have emerged as an effective algorithmic tool to deal with such computational intractability. However these algorithms have found only limited applicability in the design of truthful mechanisms, especially in “multi-parameter domains”, since many approximation algorithms and techniques do not guarantee certain properties of the algorithm that are required to ensure truthfulness.

Our results. In this paper we give a general technique to convert approximation algorithms into truthful mechanisms. One of the most widely used and remarkably successful techniques in the design of approximation algorithms, is that of expressing a relaxation of the problem as a linear program (LP), and using this to design the approximation algorithm, either via LP rounding or via a primal-dual approach. We show that for a variety of domains, any approximation algorithm for the algorithmic problem, that also bounds the integrality gap of the underlying LP relaxation, can be used to obtain a randomized mechanism for the corresponding mechanism design problem (i.e., where the inputs are held by selfish agents), that is truthful in expectation, and *has performance guarantee matching that of the approximation algorithm*. Truthfulness in expectation means that a player always maximizes his *expected* utility by revealing his true input [Archer and Tardos 2001]. Our main result can be informally stated as follows.

Informal Main Theorem *For packing domains, given any α -approximation algorithm that proves an integrality gap of at most α for the “natural” LP relaxation, one can construct a randomized α -approximation mechanism that is truthful in expectation.*

A key feature of this result is its generality. As mentioned earlier, there are a number of problem domains for which good approximation algorithms are known for the algorithmic problem, but in the mechanism design setting there are no known truthful *and* approximation mechanisms for the corresponding problem. A common problem encountered is the fact that many commonly used approximation algorithms and techniques violate certain monotonicity properties which are required for truthfulness. In cases where truthful and approximation mechanisms are known, the construction often involves clever ways of modifying or designing the approximation algorithm so as to satisfy these properties. As a consequence, in various settings, the approximation guarantees provided by truthful mechanisms fall short of the known guarantees for the algorithmic problem when one does not require truthfulness.

Our theorem not only yields new and improved results for large problem classes such as, (multi-unit) combinatorial auctions, graph routing problems, multi-unit auctions, but in doing so, it bridges the gap between known approximation results and the guarantees obtained by truthful mechanisms. Moreover, it shows that one does not need to specifically tailor the algorithm to ensure truthfulness, and allows one to focus on the algorithmic part of the problem.

We now consider the implications of our theorem, by concentrating on the *multi-unit combinatorial auction* (MUCA) problem, which has been widely studied [Lehmann et al. 2002; Archer et al. 2003; Bartal et al. 2003; Lavi et al. 2003; Briest et al. 2005; Dobzinski et al. 2005]. In an MUCA, m items are to be allocated among n players and each player i has a true value $\bar{v}_i(S)$ for every subset S of items. The value functions are assumed to be non-decreasing, that is, $\bar{v}_i(S) \leq \bar{v}_i(T)$ when

$S \subseteq T$, and normalized, that is, $\bar{v}_i(\emptyset) = 0$. There are $B \geq 1$ copies of each item. An allocation is valid if every item is allocated to at most B players. The goal is to find an allocation S_1, \dots, S_n of the items to the players that maximizes the sum $\sum_i \bar{v}_i(S_i)$, called the *social welfare*. When $B = 1$, the problem is called the *combinatorial auction* (CA) problem.

The problem is computationally hard even when $B = 1$, and the valuations are “short”, i.e., succinctly described. The approximability threshold of this problem is known to be $O(m^{\frac{1}{B+1}})$ [Bartal et al. 2003]; it is hard to approximate any better even when the players are single minded, that is, each player wants a single set S , so $\bar{v}_i(T) = \bar{v}_i(S)$ for $T \supseteq S$ and 0 otherwise. On the positive side various $O(m^{\frac{1}{B+1}})$ -approximation algorithms exist [Raghavan 1988; Kolliopoulos and Stein 2004; Briest et al. 2005], and these algorithms also prove a corresponding integrality gap result. An interesting case is when $B = \Omega(\log m)$ for which the integrality gap becomes $(1 + \epsilon)$ where $\epsilon > 0$ (more precisely $B \geq c(\epsilon) \cdot \log m$ where $c(\cdot)$ is an increasing function of $\frac{1}{\epsilon}$; we denote this simply as $B = \Omega(\log m)$ in the sequel). However *truthfulness* results are mostly known in restricted cases, and are worse. The only result for general valuations is a truthful $O(B \cdot m^{\frac{1}{B-2}})$ -approximation mechanism due to Bartal et al. [2003] when $B \geq 3$. More results are known for special cases: for single-minded players, a truthful $O(\sqrt{m})$ -approximation is known when $B = 1$ [Lehmann et al. 2002], and Briest et al. [2005] recently gave a truthful $O(m^{\frac{1}{B}})$ -approximation for $B \geq 1$ (this does not give a $(1 + \epsilon)$ -guarantee when $B = \Omega(\log m)$). Archer et al. [2003] gave a randomized $(1 + \epsilon)$ -approximation mechanism for the “known” single-minded case when $B = \Omega(\log m)$. Babaioff et al. [2009] consider the “single-value” case and (among other results) give an $O(\log^2 \bar{v}_{\max} \cdot \sqrt{m})$ -guarantee; Dobzinski et al. [2005] obtain an $O(\sqrt{m})$ -approximation for subadditive valuations. In particular, the picture is very partial for non-single-minded players: no truthful approximation mechanism is known for general combinatorial auctions ($B = 1$), and the factors for large B are much worse than the approximation results.¹

Using our construction, and any of the known approximation algorithms, we obtain randomized, truthful in expectation mechanisms for all values of B , where *the guarantees match the approximability threshold*. We summarize our results below for “short” valuations, where the valuations are succinctly describable and the underlying packing LP can be solved efficiently. An important such class is k -minded players: a player desires one of k sets and specifies the value of each; both the sets and the values are private. Section 4.1 gives other examples. We use “truthful” below to denote “truthful in expectation”.

Combinatorial auctions ($B = 1$) We give the *first truthful mechanism* for non-single-minded valuations, and get a $O(\sqrt{m})$ guarantee.

Multi-unit combinatorial auctions We get an $O(m^{\frac{1}{B+1}})$ -approximation, truthful mechanism. This improves upon the ratio of [Bartal et al. 2003]. When $B = \Omega(\log m)$ we get a $(1 + \epsilon)$ -guarantee for valuations more general than the “known” single-minded case, answering an open question in [Archer et al. 2003].

Multi unit auctions Here the m items are identical, and the valuation specifies a value for each quantity of goods received. This generalizes Knapsack, which is the case when all players have a step function (i.e., are single minded), for which a truthful FPTAS was given by Briest et al. [2005]. We give a truthful 2-approximation mechanism for multi-unit auctions, which is the *first truthful, approximation mechanism* for the multi-parameter case.

Graph routing problems These include (see Section 4.3), for example, the edge-disjoint paths problem, where we have an underlying graph and each player desires a path between his source and target nodes. This is a special case of MUCA and the previous guarantees hold.

¹Section 5 discusses briefly some results obtained subsequent to the publication of the conference version of this paper [Lavi and Swamy 2005]. Notably, however, our method remains the only known general method that provides a unified framework; it also yields the current-best truthful approximation mechanisms for some broad problem domains (e.g., MUCAs).

With arbitrary valuations, the input itself may have exponential length (in m) which therefore renders direct revelation mechanisms infeasible. The problem remains “hard” even when one ignores computational issues: [Nisan 2002] shows that no algorithm with polynomial communication (in m, n) can attain an approximation ratio of $m^{\frac{1}{2}-\epsilon}$ for any $\epsilon > 0$ even when $B = 1$. [Blumrosen and Nisan 2005] introduce the notion of a *demand oracle*, and show that this can be used to solve the associated LP using polynomial number of queries. With such an oracle, our construction still works and yields *iterative* randomized, strategic mechanisms. However, the iterative structure of the mechanism changes the solution concept to an ex-post Nash equilibrium, a well-documented phenomenon in the economics literature (see e.g., [Conitzer and Sandholm 2004]). So we now get truthfulness in expectation as an ex-post Nash equilibrium which roughly means the following: regardless of the other players’ valuations, if they all answer truthfully, then my best response is to answer truthfully. We get the same guarantees as before, using ex-post Nash equilibrium as the solution concept. In particular, this implies that even if a player were told beforehand the valuations that the other players would use to act in the iterative mechanism, he would have no incentive to deviate from his truth-telling strategy. (As an example, consider the regular second-price auction with two players with the following iterative flavor: player X bids first *and then* player Y states his bid; the player with highest bid wins and pays the second highest bid value. Truthfulness fails to be a dominant strategy here. To see this, suppose Y chooses the strategy “if X bids above 5, then I will say 20, otherwise I will say 2”, then, if X ’s true value is higher than 5, his best response is to declare 5. However truthfulness is still an ex-post Nash equilibrium: if Y fixes *any* private value and bids that, then regardless of Y ’s private value X ’s best response is to tell the truth (and vice versa).)

We should emphasize that the requirement that an approximation algorithm should “prove” (or verify) an integrality gap of α is (possibly significantly) more demanding than having an α -approximation LP-rounding algorithm for the problem: an α -integrality-gap verifying algorithm has to find an α -approximate solution for *every* real-valued objective function.² The exact limitations that this imposes are not yet completely understood. Loosely speaking, one can often take advantage of structure in the allocation space (e.g. multiple copies of every item, identical items, etc.), but it is often harder to exploit structure in the valuation space. There are some settings where one can encapsulate the combinatorial structure of the winner determination problem (WDP) with a structured valuation class by formulating a stronger LP-relaxation for WDP, and thereby prove that an approximation algorithm for the structured valuation class is in fact an integrality-gap-verifying approximation algorithm with respect to this *stronger LP-relaxation* (and hence apply our construction); see, e.g., the algorithm for the tollbooth problem on trees in [Elbassioni et al. 2010]. In contrast, and most notably, we do not know if this is possible for submodular and subadditive valuations; that is, whether one can extend or adapt our technique and exploit the known LP-rounding algorithms for WDP with submodular or subadditive valuations to obtain analogous guarantees with truthful (in expectation) mechanisms.

Our construction. At a high level, our construction is quite intuitive and easy to describe. Our starting point is the classic VCG result [Vickrey 1961; Clarke 1971; Groves 1973], which provides a truthful mechanism for the underlying algorithmic problem of maximizing the social welfare, provided that the algorithmic problem can be solved *exactly*. However, in our case and in many others, this problem is *NP-hard*, and approximation algorithms need not give truthfulness. Our first step towards handling this problem is to move to a fractional domain, and to consider a *fractional mechanism* that is allowed to return a fractional feasible solution to the LP relaxation of the problem. In this new domain, since one can solve the LP in polynomial time, we can use VCG to obtain a truthful fractional mechanism. Moreover, since we are in a fractional domain, we can always

²For packing domains, it suffices to consider only nonnegative objective functions; furthermore, for CAs, it suffices to consider normalized, monotone valuation functions; see Section 3.

scale down both the optimal LP solution and the VCG prices by α , and this clearly does not affect truthfulness.

Let x^* be an optimal LP solution. Suppose that the integrality gap of the LP relaxation is $\alpha \geq 1$ and we have an algorithm that “verifies” this gap. At the heart of our construction is a procedure that takes such an α -approximation algorithm and returns in polynomial time a *convex decomposition* of $\frac{x^*}{\alpha}$ into polynomially many integer solutions, that is, it returns λ_l values such that $\frac{x^*}{\alpha} = \sum_{l \in \mathcal{I}} \lambda_l x^l$, where $\{x^l\}_{l \in \mathcal{I}}$ is the set of all integer solutions, $\lambda_l \geq 0$, $\sum \lambda_l = 1$ (with only polynomially many positive λ_l). We show this by strengthening the decomposition technique of Carr and Vempala [2002]. Now one can view this convex combination as specifying a probability distribution over the integer solutions, where exactly one solution x^l is selected with probability equal to λ_l . A simple but powerful observation, is that the randomized mechanism which returns an integer solution according to this distribution, and sets prices in such a way that the expected prices are the VCG prices scaled down by α , is *truthful in expectation*. Furthermore, the expected social welfare of the solution returned is exactly the value of the LP-optimum scaled by α ; thus we get an α -approximation guarantee. The crucial step here is the decomposition procedure which allows us to move from the truthful VCG fractional mechanism to a randomized, truthful in expectation mechanism.

A notable feature is the generality and simplicity of the construction. In essence, we give a way to leverage VCG in a computationally effective manner using approximation algorithms, while maintaining truthfulness. Thus we reap the benefits of both: we get the versatility of the VCG as a mechanism design tool for devising truthful mechanisms, *and* the computational tractability of approximation algorithms. As mentioned earlier, many previous results specifically tailor the algorithm to obtain truthfulness. For example, Archer et al. [2003] consider an LP-relaxation of MUCA with $\Omega(\log m)$ copies and designed a randomized rounding procedure to obtain a $(1 + \epsilon)$ -approximation mechanism that is truthful in expectation and also with high probability. [Briest et al. 2005] showed how to convert certain FPTAS’s into truthful ones, and also gave primal-dual algorithms for some CAs; both results involve tailoring the algorithm so as to ensure truthfulness, but yield deterministic mechanisms. Our construction shows that if one allows randomization, then such “algorithmic artistry” is not required to ensure truthfulness, and allows the algorithm design to concentrate on the approximation component of the problem.

Organization of the paper. We begin in Section 2 by describing the mechanism-design setup, and collecting some basic definitions and facts. Section 3 describes our general method of designing a truthful mechanism based on the LP relaxation of the problem, and Section 4 applies our technique to a variety of problems. While we focus primarily on packing problems, we also show how our ideas can be adapted to yield (partial) results also for *covering problems* (see Section 4.4). We conclude in Section 5 with a brief discussion of some recent results.

2. PRELIMINARIES

In the basic mechanism design setup, we have n players, and a set A of possible outcomes. Each player has a type given by a valuation function $v_i : A \mapsto \mathbb{R}_{\geq 0}$, where $v_i \in V_i$ and V_i is the set of all valid types of player i . Let $V = V_1 \times \dots \times V_n$ denote the space of all players’ valid types. For example, in *combinatorial auctions* we have m items; A is the set of all allocations (S_1, \dots, S_n) of items to players with $S_i \cap S_j = \emptyset$ (assuming a single copy of each item), and $v_i : A \mapsto \mathbb{R}$ is a function that (a) assigns the same value to any two outcomes that allocate the same subset to player i , so one can view v_i as specifying a value for each set S of items, (b) satisfies $v_i(\emptyset) = 0$, and (c) is monotone, i.e., $v_i(S) \leq v_i(T)$ whenever $S \subseteq T$. We use v to denote the tuple (v_1, \dots, v_n) , and v_{-i} to denote the tuple $(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n)$ that excludes i ’s valuation. Similarly $V_{-i} = \prod_{j \neq i} V_j$.

A (direct revelation) mechanism consists of an allocation rule (that is, an algorithm) $f : V \mapsto A$, and a pricing scheme $p_i : V \mapsto \mathbb{R}$ for each player i . Each player i reports a type v_i (possibly deviating from his true type), and the mechanism computes the outcome $f(v)$ and charges price $p_i(v)$ to player i . Throughout we use \bar{v}_i to denote the *true type* of player i . The *utility* that the player

i derives by declaring type v_i is $\bar{v}_i(f(v_i, v_{-i})) - p_i(v_i, v_{-i})$, and each player aims to maximize his own utility. A desirable property for a mechanism to satisfy is *truthfulness*, wherein *each player maximizes his utility by reporting his true type*.

Definition 2.1 (Truthfulness) A deterministic mechanism (f, p) is truthful if for any player i , any $v_{-i} \in V_{-i}$, and any $\bar{v}_i, v'_i \in V_i$ we have $\bar{v}_i(f(\bar{v}_i, v_{-i})) - p_i(\bar{v}_i, v_{-i}) \geq \bar{v}_i(f(v'_i, v_{-i})) - p_i(v'_i, v_{-i})$.

We will be interested in approximating the (optimum) *social welfare* with respect to the players' true types, which is defined as $\max_{a \in A} \sum_i \bar{v}_i(a)$. An important component in our constructions is the VCG family of mechanisms [Vickrey 1961; Clarke 1971; Groves 1973], which shows that if the allocation rule chooses the social-welfare-maximizing outcome from among a (fixed) subset $A' \subseteq A$ of outcomes, then there always exist prices that when combined with f yield a truthful mechanism. We include a short description of this classic result for completeness. Formally, suppose that $f(v) = \arg \max_{a \in A'} \sum_i v_i(a)$. Player i 's payment function $p_i : V_i \mapsto \mathbb{R}$ is then defined by $p_i(v) = -\sum_{j \neq i} v_j(f(v)) + h_i(v_{-i})$, where $h_i : V_{-i} \mapsto \mathbb{R}$ can be any function.

Theorem 2.1 ([Vickrey 1961; Clarke 1971; Groves 1973]) *The VCG mechanism (f, p) defined above is truthful.*

PROOF. Fix any player i , any $v_{-i} \in V_{-i}$, and any $\bar{v}_i, v'_i \in V_i$. Suppose that $f(\bar{v}_i, v_{-i}) = a^*$ and $f(v'_i, v_{-i}) = a'$. By definition, we have that $\bar{v}_i(a^*) + \sum_{j \neq i} v_j(a^*) \geq \bar{v}_i(a') + \sum_{j \neq i} v_j(a')$. So

$$\begin{aligned} \bar{v}_i(f(\bar{v}_i, v_{-i})) - p_i(\bar{v}_i, v_{-i}) &= \bar{v}_i(a^*) - \left(-\sum_{j \neq i} v_j(a^*) + h_i(v_{-i}) \right) \\ &\geq \bar{v}_i(a') - \left(-\sum_{j \neq i} v_j(a') + h_i(v_{-i}) \right) = \bar{v}_i(f(v'_i, v_{-i})) - p_i(v'_i, v_{-i}). \end{aligned}$$

□

In the specific context of combinatorial auctions, a common choice for h_i is as follows. Suppose that $A' = A$ is the set of all allocations. Let $T^{-i} = \{T_j^{-i}\}_{j \neq i}$ be an allocation that maximizes $\sum_{j \neq i} v_j(T_j^{-i})$; that is, T^{-i} is the allocation that would be chosen (by f) if player i does not participate, or equivalently, if he reports a zero value for all subsets of items. Then, we set $h_i(v_{-i}) = \sum_{j \neq i} v_j(T_j^{-i})$. So letting $S^* = (S_1^*, \dots, S_n^*)$ denote the allocation that maximizes the social welfare $\sum_{i=1}^n v_i(S_i)$, player i 's payment is given by

$$p_i(\bar{v}_i, v_{-i}) = \sum_{j \neq i} v_j(T_j^{-i}) - \sum_{j \neq i} v_j(S_j^*).$$

Notice that these prices can be computed efficiently if f can be computed efficiently. Moreover, these prices have the additional property that a player's utility is always nonnegative if he reports his true value (individual rationality), and that $p_i(\bar{v}_i, v_{-i}) \geq 0$ for every i (players never receive money). Thus, if the algorithmic winner-determination problem (WDP) for CAs (i.e., the problem of maximizing social welfare given the players' reported types) can be solved *exactly* and *efficiently*, then the VCG mechanism yields an efficient truthful mechanism that optimizes social welfare. However this algorithmic problem is often *NP-hard*, and it is known that an approximation algorithm for this problem need not necessarily give a truthful mechanism. Nevertheless, our construction shows that VCG can still be leveraged using approximation algorithms and *randomization*.

A *randomized* mechanism can flip coins to determine $f(v)$ and $p_i(v)$, in which case $f(v)$ and $p_i(v)$ are random variables, and a player's utility is also a random variable. For randomized mechanisms, we can consider the notion of *truthfulness in expectation* [Archer and Tardos 2001].

Definition 2.2 (Truthfulness in expectation) A randomized mechanism (f, p) is truthful in expectation if for any player i , any $v_{-i} \in V_{-i}$, and any $\bar{v}_i, v'_i \in V_i$, $\mathbb{E}[\bar{v}_i(f(\bar{v}_i, v_{-i})) - p_i(\bar{v}_i, v_{-i})] \geq \mathbb{E}[\bar{v}_i(f(v'_i, v_{-i})) - p_i(v'_i, v_{-i})]$.

Thus, if a mechanism is truthful in expectation then the expected utility of a player is maximized when he declares his true type \bar{v}_i (regardless of what others declare). A randomized algorithm is often viewed as specifying a probability distribution over deterministic algorithms. It will be useful to view a randomized mechanism in a similar way. For an outcome set A , define the unit simplex $\Delta_A = \{\lambda \in \mathbb{R}^{|A|} : \sum_{a \in A} \lambda_a = 1 \text{ and } \lambda_a \geq 0 \text{ for all } a\}$. If we identify A with the collection $\{e_a \in \mathbb{R}^A\}_{a \in A}$ unit vectors, where e_a is the vector with 1 in the a -th coordinate, then Δ_A is simply the convex hull of this set. Given any randomized mechanism $M^R = (f^R, p^R)$ with outcome set A , we can define a deterministic mechanism M^D with outcome set Δ_A , which outputs the probability distribution of M^R , and charges prices that are the expected prices of M^R . To define M^D precisely, we need to extend the domain V_i to include values for outcomes in Δ_A . We do this in the obvious way: for any $v_i \in V_i$, define $v_i(\{\lambda_a\}_{a \in A}) = \sum_{a \in A} \lambda_a v_i(a)$. We abuse notation and use v_i to denote both a valuation in V_i and its corresponding extension. Now we can define M^D as follows:

- (1) Allocation rule: Define the function f^D by $f^D(v) = \{\lambda_a\}_{a \in A}$ where $\lambda_a = \Pr[f^R(v) = a]$,
- (2) Pricing scheme: For each player i , and valuation vector v , set $p_i^D(v) = \mathbb{E}[p_i^R(v)]$.

We call M^D the deterministic *support mechanism* of M^R . Observe that the criterion for truthfulness of M^D is *exactly* the criterion for the truthfulness in expectation of M^R .

Claim 2.3 A randomized mechanism M^R is truthful in expectation iff its support mechanism M^D is truthful.

The above claim gives a characterization of randomized mechanisms that are truthful in expectation which we use to argue the truthfulness in expectation of the randomized mechanisms we construct.

Converting a support mechanism to a randomized mechanism. Our algorithms will actually construct a deterministic support mechanism. We show how to construct, from a (deterministic) support mechanism M^D , a corresponding randomized mechanism M^R (whose support mechanism is M^D) that preserves various properties of M^D . Let M^D have outcome set Δ_A , so M^R will have outcome set A . The allocation rule is easy to specify: $f^R(v) \in A$ is a random variable with distribution $f^D(v)$, i.e., we output $f^R(v) = a$ with probability λ_a where $f^D(v) = \{\lambda_a\}_{a \in A}$. So $\mathbb{E}[\bar{v}_i(f^R(v))] = \bar{v}_i(f^D(v))$ for any player i , any true type $\bar{v}_i \in V_i$ and any $v \in V$. Since the prices $p_i^R(v)$ will be set so that $\mathbb{E}[p_i^R(v)] = p_i^D(v)$ (because M^D has to be the support mechanism of M^R), the expected utility of player i is also preserved in going from M^D to M^R . One obvious way to set the prices is to deterministically set $p_i^R(v) = p_i^D(v)$ for every v , but the resulting randomized mechanism could violate *individual rationality*. Individual rationality requires that for every player i , i 's utility be non-negative when he declares his *true type*, regardless of the other players' declarations. A randomized mechanism, satisfies individual rationality if for every coin toss, the utility of every player i is non-negative when he declares his true type. Setting $p_i^R(v) = p_i^D(v)$ may violate individual rationality even if M^D is individually rational, since there could be coin tosses where a player receives nothing but pays a positive amount. Perhaps the easiest way to maintain individual rationality is to set price $p_i^R(v) = v_i(a) \cdot \frac{p_i^D(v)}{v_i(f^D(v))}$ if $v_i(f^D(v)) > 0$ and outcome a results (i.e., $f^R(v) = a$), and set $p_i^R(v) = 0$ if $v_i(f^D(v)) = 0$ ($= p_i^D(v)$). Observe that $p_i^R(\bar{v}_i, v_{-i}) \leq \bar{v}_i(f^R(\bar{v}_i, v_{-i}))$ for any coin toss since $p_i^D(\bar{v}_i, v_{-i}) \leq \bar{v}_i(f^D(\bar{v}_i, v_{-i}))$, and clearly $\mathbb{E}[p_i^R(v)] = p_i^D(v)$.

The above construction of M^R from M^D preserves truthfulness (in expectation) by Claim 2.3, individual rationality, and the expected value received by a player. Thus we get the following theorem.

Theorem 2.2 *Given an individually rational, truthful, deterministic support mechanism that computes an α -approximation to the social welfare and has only polynomially many $\lambda_{\alpha,S}$ that are positive, one can obtain in polynomial time an individually rational randomized mechanism that is truthful in expectation, and computes an α -approximation to the social welfare in expectation.*

Given the above theorem, we now focus on the design of a deterministic support mechanism that outputs a probability distribution and prices, with the desired properties. The support mechanism we construct will be mechanism in the VCG family. That is, our allocation rule (which will be efficiently computable) will choose the social-welfare-maximizing outcome from among a subset $\Delta' \subseteq \Delta_A$, and the prices will be the VCG prices (and hence, also efficiently computable; see Theorem 2.1 and the following discussion). Since the outcome set Δ' here corresponds to a collection of distributions over A , such a support mechanism (and the corresponding randomized mechanism) is sometimes called a *maximal-in-distributional-range* (MIDR) mechanism in the literature (see [Dobzinski and Dughmi 2009]).

3. A GENERAL TECHNIQUE FOR CONSTRUCTING TRUTHFUL, APPROXIMATION MECHANISMS

In this section we describe a general technique to obtain randomized mechanisms that are truthful in expectation, and achieve approximation guarantees for the social welfare that, in several cases, match the guarantees that are achieved without worrying about truthfulness. To make our results concrete, we describe our technique for the specific setting of combinatorial auctions (CAs), although our results also hold for other packing problems when the polytope is public knowledge and the objective function is linear. In Section 4, we consider a variety of applications and use our methods to obtain truthful (in expectation) mechanisms that approximate the social welfare.

We can formulate the combinatorial auction problem as an integer program (IP) where we have a variable $x_{i,S} \in \{0, 1\}$ for each player i and set $S \neq \emptyset$ that indicates if i receives set S . Relaxing the integrality constraints to $x_{i,S} \geq 0$ gives the following LP relaxation.

$$\begin{aligned} \max \quad & \sum_{i,S \neq \emptyset} v_i(S) x_{i,S} && \text{(CA-P)} \\ \text{subject to} \quad & \sum_{S \neq \emptyset} x_{i,S} \leq 1 && \text{for each player } i && (1) \\ & \sum_i \sum_{S: j \in S} x_{i,S} \leq 1 && \text{for each item } j && (2) \\ & x_{i,S} \geq 0 && \text{for each } i, S. \end{aligned}$$

Here v_i is i 's reported valuation which satisfies $v_i(S) \leq v_i(T)$ whenever $S \subseteq T$ (and implicitly $v_i(\emptyset) = 0$). Constraints (1) state that each player is assigned at most one set, and (2) ensures that each item j is given to at most one player.

Our approximation guarantee depends on the ‘‘integrality gap’’ of (CA-P), which is ‘‘verified’’ by an α -approximation algorithm, as follows. Let \mathcal{P} denote the feasible region of (CA-P), and $\mathbb{Z}(\mathcal{P}) \subseteq \mathcal{P}$ be the set of integer solutions of (CA-P). The integrality gap of \mathcal{P} is the maximal ratio between the values of the optimal fractional and integer solutions, i.e.,

$$IG_{\mathcal{P}} = \sup_{v=(v_1, \dots, v_n)} \frac{\max_{x \in \mathcal{P}} \sum_{i,S} v_i(S) x_{i,S}}{\max_{x \in \mathbb{Z}(\mathcal{P})} \sum_{i,S} v_i(S) x_{i,S}}$$

where the v_i s are valuations with $v_i(\emptyset) = 0$, $v_i(S) \leq v_i(T)$ for $S \subseteq T$. An α -approximation algorithm “verifies” an integrality gap of (at most) α if, for *any valuation vector* v , the algorithm produces an integer solution of value at least $\frac{1}{\alpha}$ times the fractional optimum of (CA-P).

We emphasize that the supremum is taken over *all* valuations v (satisfying monotonicity and normalization) in evaluating the integrality gap, and an algorithm that verifies this gap must consequently work for all valuations. To clarify this further, consider the structured class of submodular valuations. Various approximation algorithms for submodular valuations are known where the approximation guarantee is proved with respect to the optimum of (CA-P) (e.g., the 2-approximation algorithm in [Lehmann et al. 2006]). However, the integrality gap is defined with respect to *all* monotone valuation functions, and an integrality-gap-verifier must consequently work for all such valuation functions. Thus, an approximation algorithm that proves a guarantee only for a specific valuation class using the fractional optimum as an upper bound *does not* suffice to bound or verify the integrality gap $IG_{\mathcal{P}}$; in order to exploit the structure of a valuation class, we need to design a new LP which encodes this structure into the polytope \mathcal{P} (and give an integrality-gap-verifying algorithm for this new LP). We explain the exact technical reason for this after Lemma 3.4 below.

Our main theorem is as follows.

Theorem 3.1 *Given an α -approximation algorithm that proves an integrality gap of at most α for (CA-P), one can construct a randomized, individually rational, α -approximation mechanism that is truthful in expectation.*

As we demonstrate in the sequel, this theorem and our construction in fact hold for any LP that satisfies the following “*packing property*”: if $x \in \mathbb{Z}(\mathcal{P})$ and $y \leq x$ is integral then $y \in \mathbb{Z}(\mathcal{P})$. The proof for an arbitrary packing LP is essentially the same as the proof we give below for (CA-P).

We give an overview of the construction before the formal proof. As mentioned previously, the versatile VCG mechanism, which is the classic positive result in mechanism design for social-welfare maximization problems, forms a crucial component of our construction. We move to a fractional domain and consider a *fractional mechanism* that is allowed to return a fractional feasible solution to (CA-P). With this outcome set, one can solve WDP exactly in polynomial time since one can solve (CA-P) (see Section 4.1), and therefore use VCG to obtain a truthful fractional mechanism M^F which returns allocation x^* , the optimal solution to (CA-P), and prices p^F . Since we are in a fractional domain, we can scale down both the allocation and prices by some $\alpha \geq 1$ without affecting truthfulness. We give a procedure that takes an α -approximation algorithm that proves an integrality gap of α for (CA-P), and returns in polynomial time a convex decomposition of $\frac{x^*}{\alpha}$ into polynomially many integer solutions, i.e., λ_l values such that $\frac{x^*}{\alpha} = \sum_{l \in \mathcal{I}} \lambda_l x^l$, where $\{x^l\}_{l \in \mathcal{I}}$ is the set of all integer solutions to (CA-P), $\lambda_l \geq 0$, $\sum \lambda_l = 1$ (with only polynomially many $\lambda_l > 0$). This is obtained by strengthening the decomposition technique of Carr and Vempala [2002]. This is the crucial step, using which we convert the truthful fractional mechanism M^F to a *truthful deterministic support mechanism* M^D that outputs $\{\lambda_l\}_{l \in \mathcal{I}}$ as the allocation and $\frac{p^F}{\alpha}$ as the prices, while losing a factor of α in the social welfare (and maintaining individual rationality). Now we use Theorem 2.2 to obtain a randomized, truthful in expectation mechanism that achieves an α -approximation to the social welfare. We summarize the construction below.

The truthful α -approximation support mechanism. Given valuations v_1, \dots, v_n ; an α -approximation algorithm \mathcal{A} for WDP that shows an integrality gap of α for (CA-P).

- (1) Use VCG to get a truthful fractional mechanism M^F that outputs allocation $f^F(v) = x^*(v)$, the optimal solution to (CA-P), and prices $p^F(v)$.
- (2) Use \mathcal{A} to obtain the convex decomposition $\frac{x^*}{\alpha} = \sum_{l \in \mathcal{I}} \lambda_l x^l$ with only polynomially many positive λ_l .
- (3) Return the support mechanism $M^D = (f^D, p^D)$ with $f^D(v) = \{\lambda_l\}_{l \in \mathcal{I}}$ and $p^D(v) = \frac{p^F(v)}{\alpha}$ (and use Theorem 2.2 to get the desired randomized mechanism).

Thus we show that any approximation algorithm for maximizing social welfare, that also shows an integrality gap guarantee, can be plugged in to get a randomized truthful mechanism with the same approximation guarantee. Thus, we are able to combine the versatility of VCG as a mechanism design tool for devising truthful mechanisms, *and* the computational tractability of approximation algorithms.

3.1. The fractional mechanism

Recall that \mathcal{P} denotes the feasible region of (CA-P), and $\mathbb{Z}(\mathcal{P}) \subseteq \mathcal{P}$ is the set of integer solutions of (CA-P). We define a fractional mechanism with outcome set \mathcal{P} , and extend the domain V_i to assign values to fractional solutions $x \in \mathcal{P}$: for any $v_i \in V_i$, we define $v_i(x) = \sum_S v_i(S)x_{i,S}$. We again abuse notation and use v_i to denote both the original valuation and its extension. We now define precisely the *fractional VCG mechanism* which is simply VCG in this fractional domain.

The fractional VCG mechanism $M^F = (f^F, p^F)$ is defined as follows: the allocation rule is given by $f^F(v) = x^*(v)$ where $x^*(v)$ is an optimal solution to (CA-P) for valuation $v = (v_1, \dots, v_n)$; the prices are $p_i^F(v) = (-\sum_{i' \neq i} v_{i'}(S)x_{i',S}^* + h_i(v_{-i}))$, where $h_i(v_{-i})$ is any function that does not depend on v_i .

As usual with VCG mechanisms, one can set $h_i(v_{-i}) = \sum_{i' \neq i} v_{i'}(S)y_{i',S}^*$ above, where y^* is the optimal fractional solution when we constrain $x_{i,S} = 0$ for all S , so as to ensure that that players have non-negative utility (individual rationality), and players always have a non-negative payment (they never receive money). We will assume these prices from now on. As shown in Theorem 2.1, the VCG mechanism (family) is truthful. For any $\alpha \geq 1$, we can define an α -scaled fractional VCG mechanism that outputs the outcome $\frac{f^F(v)}{\alpha}$ and prices $\frac{p^F(v)}{\alpha}$. For any $v \in V$ and $\bar{v}_i \in V_i$, since $\bar{v}_i(\frac{f^F(v)}{\alpha}) = \frac{\bar{v}_i(f^F(v))}{\alpha}$ (because $\bar{v}_i(x)$ is linear in x), the α -scaled fractional VCG mechanism is also clearly truthful.

Suppose that we can express $\frac{x^*(v)}{\alpha}$ as a convex combination $\sum_{l \in \mathcal{I}} \lambda_l(v)x^l$ of integral solutions where $\lambda_l(v) \geq 0$, $\sum_l \lambda_l(v) = 1$. (Observe that α must be at least $IG_{\mathcal{P}}$ since such a decomposition of $\frac{x^*(v)}{\alpha}$ implies that there exists an integer solution x^l of value at least $\frac{1}{\alpha} \cdot \sum_i v_i(x^*(v))$.) One then obtains a deterministic support mechanism M^D with allocation rule $f^D(v) = \{\lambda_l(v)\}_{l \in \mathcal{I}}$ and prices $p_i^D(v) = \frac{p_i^F(v)}{\alpha}$. Before detailing the decomposition procedure, we show that M^D is a truthful, α -approximation mechanism.

Lemma 3.1 *Mechanism M^D is truthful and computes an α -approximation to the social welfare.*

PROOF. Essentially, we show that M^D is equivalent to the α -scaled fractional VCG mechanism and retains all its properties. For any declared valuation $v = (v_1, \dots, v_n)$, the value player i gets in M^D is exactly $\frac{\bar{v}_i(f^F(v))}{\alpha}$ since $\bar{v}_i(f^D(v)) = \sum_{l \in \mathcal{I}} \lambda_l(v)\bar{v}_i(x^l)$ by definition, which is equal to $\bar{v}_i(\sum_{l \in \mathcal{I}} \lambda_l(v)x^l) = \bar{v}_i(\frac{x^*(v)}{\alpha}) = \frac{\bar{v}_i(x^*(v))}{\alpha}$. Since the prices are also scaled by α , truthfulness follows from the truthfulness of M^F . Truthfulness also then implies the approximation guarantee since $\sum_i \bar{v}_i(x^*(\bar{v}))$ is an upper bound on the optimum. Note that M^D satisfies individual rationality and no player is paid by the mechanism. \square

Using Theorem 2.2 we can move from M^D to a randomized mechanism, while maintaining truthfulness, the approximation ratio, and individual rationality. Thus we obtain Theorem 3.1. The crucial property that we require here is that for any $\bar{v}_i \in V_i$, and any $v \in V$, $\sum_{l \in \mathcal{I}} \lambda_l(v)\bar{v}_i(x^l) = \frac{\bar{v}_i(x^*(v))}{\alpha}$. A sufficient condition for this is that $\bar{v}_i(x)$ be a linear function of x and that $\frac{x^*(v)}{\alpha}$ be decomposable as $\sum_{l \in \mathcal{I}} \lambda_l(v)x^l$, which is what we use in our construction.

It is instructive to note that our deterministic support mechanism M^D (or the randomized mechanism constructed from it) is in fact a maximal-in-distributional-range (MIDR) mechanism.³ To see this, let \mathcal{P}_I denote the convex hull of integer points in \mathcal{P} (i.e., $\mathbb{Z}(\mathcal{P})$). (Observe that the outcome of any support or randomized mechanism corresponds to a point in \mathcal{P}_I .) Our decomposition lemma (Lemma 3.4) shows that $\mathcal{P}/\alpha \subseteq \mathcal{P}_I$; also, we can efficiently optimize over \mathcal{P}/α since this is equivalent to optimizing over \mathcal{P} . Thus, our support (or the equivalent randomized) mechanism (which returns the optimum over \mathcal{P}/α as its outcome) is simply VCG over the outcome-set \mathcal{P}/α . And the α -approximation ratio follows since the optimum value over \mathcal{P}/α is within an α -factor of the optimum over \mathcal{P} . (The subtle difference between the α -scaled fractional VCG mechanism and the support mechanism M^D (which are essentially identical) is in how they specify the optimal outcome in \mathcal{P}/α : the support mechanism is required to specify this point by decomposing it into a convex combination of points in $\mathbb{Z}(\mathcal{P})$ (which Lemma 3.4 shows can be done efficiently), whereas there is no such requirement in the α -scaled fractional mechanism.) Thus, in essence, our construction uses an α -integrality-gap-verifying approximation algorithm to *exactly optimize* the social welfare *efficiently* over a subset of the convex hull of integer solutions, and hence, implement VCG over a suitable (fixed) outcome set.

3.2. Decomposing the fractional solution

We now prove the main decomposition lemma: we show that an α -approximation algorithm \mathcal{A} that proves an integrality gap of α for (CA-P) can be used to express any fractional solution to (CA-P), scaled down by α , as a convex combination of integer solutions. The proof is based on the method outlined in [Carr and Vempala 2002] where it is shown that for minimization problems, if the integrality gap is $\beta \geq 1$, then for any fractional solution, one can obtain a convex combination of integer solutions such that β times the fractional solution *dominates* (i.e., is component-wise greater than) the convex combination. We need to modify their argument so as to ensure that we get an *exact* decomposition (for our maximization problem), which is crucial for our truthfulness argument to hold. For general maximization LPs, one cannot necessarily get such an exact decomposition of the scaled fractional solution, but only one that dominates the scaled solution. We leverage the packing structure of the problem to get an exact decomposition. Recall that \mathcal{P} denotes the feasible region of (CA-P) and $\mathbb{Z}(\mathcal{P}) = \{x^I\}_{I \in \mathcal{I}}$ is the set of all integer solutions to (CA-P) where \mathcal{I} is an index set for the integer solutions. We exploit the following property, which we call the “*packing property*”: if $x \in \mathbb{Z}(\mathcal{P})$ and $y \leq x$ is integral then $y \in \mathbb{Z}(\mathcal{P})$.

Fix any $x^* \in \mathcal{P}$ such that $E = \{(i, S) : x_{i,S}^* > 0\}$ has size polynomial in m, n . Any basic solution to (CA-P) (or extreme point of \mathcal{P}) satisfies this since by standard polyhedral theory the number of non-zero variables in an extreme point is at most the number of constraints in the LP (which is $m + n$ in our case). Also, it is well known that if an LP with nonnegative variables has an optimal solution, then there is an extreme point that is an optimal solution (and such an extreme point can be found efficiently); a detailed discussion of these issues can be found in any textbook on linear programming (see, e.g., [Chvátal 1983]). The linear program (P) given below yields a convex decomposition of x^* .

³This also implies the polynomial-time construction of individually-rational and truthful prices, as noted in [Dobzinski and Dughmi 2009]. More specifically, if every distribution in the support of an MIDR mechanism has only polynomially many sets (this is true for the algorithms constructed in this paper, as explained below), then there exists a pricing scheme that can be computed efficiently. Roughly speaking, this can be done by dividing the expected payment proportionally among all sets in the support, in a similar way to our price construction in section 2.

$$\begin{array}{ll}
\min & \sum_{l \in \mathcal{I}} \lambda_l \quad (\text{P}) \\
\text{s.t.} & \sum_l \lambda_l x_{i,S}^l = \frac{x_{i,S}^*}{\alpha} \quad \text{for all } (i, S) \in E \\
& \sum_l \lambda_l \geq 1 \quad (3) \\
& \lambda_l \geq 0 \quad \text{for all } l \in \mathcal{I}. \quad (4)
\end{array}
\qquad
\begin{array}{ll}
\max & \frac{1}{\alpha} \cdot \sum_{(i,S) \in E} x_{i,S}^* w_{i,S} + z \quad (\text{D}) \\
\text{s.t.} & \sum_{(i,S) \in E} x_{i,S}^l w_{i,S} + z \leq 1 \quad \text{for all } l \in \mathcal{I} \\
& z \geq 0 \quad (5) \\
& w_{i,S} \text{ unconstrained} \quad \text{for all } (i, S) \in E.
\end{array}$$

The primal (P) has an exponential number of variables, so we consider its dual (D). The dual has an exponential number of constraints and a *variable* $w_{i,S}$ for each constraint (3), and one can view w as a valuation. We show that a separation oracle for the dual can be obtained by using algorithm \mathcal{A} with valuation w , so the ellipsoid method can be used to solve (D) and hence (P) (we also show that the optimal value is 1). One potential problem encountered is that the $w_{i,S}$ values could be negative, whereas \mathcal{A} is only designed to handle non-negative valuations. However it is easy to argue that one can instead use \mathcal{A} with the non-negative valuation w^+ given by $w_{i,S}^+ = \max(w_{i,S}, 0)$, and this yields a separation oracle. (Alternatively, one could first compute λ_l values such that $\sum_{l \in \mathcal{I}} \lambda_l x^l \geq \frac{x^*}{\alpha}$, so the dual variables $w_{i,S}$ are now non-negative, and then use the packing property to modify these λ_l values and get an exact decomposition.)

Claim 3.2 *Let $w = \{w_{i,S}\}_{(i,S) \in E}$ be any weight vector. Define w^+ by $w_{i,S}^+ = \max(w_{i,S}, 0)$. Given any integer solution $\hat{x} \in \mathbb{Z}(\mathcal{P})$, one can obtain $x^l \in \mathbb{Z}(\mathcal{P})$ such that $\sum_{(i,S) \in E} x_{i,S}^l w_{i,S} = \sum_{(i,S) \in E} \hat{x}_{i,S} w_{i,S}^+$.*

PROOF. Set $x_{i,S}^l = \hat{x}_{i,S}$ if $w_{i,S} \geq 0$ and 0 otherwise. Clearly, $\sum_{(i,S) \in E} x_{i,S}^l w_{i,S} = \sum_{(i,S) \in E} \hat{x}_{i,S} w_{i,S}^+$. Since $x^l \leq \hat{x}$ is integral, by the packing property $x^l \in \mathbb{Z}(\mathcal{P})$. \square

Claim 3.3 *For any weight vector $w = \{w_{i,S}\}_{(i,S) \in E}$, one can compute in polynomial time $x^l \in \mathbb{Z}(\mathcal{P})$ such that $\sum_{(i,S) \in E} x_{i,S}^l w_{i,S} \geq \frac{1}{\alpha} \cdot \max_{x \in \mathcal{P}} \sum_{(i,S) \in E} x_{i,S} w_{i,S}$.*

PROOF. Let $O^* = \max_{x \in \mathcal{P}} \sum_{(i,S) \in E} x_{i,S} w_{i,S}$. Let w^+ be as defined in Claim 3.2. Clearly w^+ is component-wise greater than w and $\sum_{i,S} x_{i,S} w_{i,S}^+ = \sum_{(i,S) \in E} x_{i,S} w_{i,S}^+$ for any x . If \mathcal{A} only expects a non-negative valuation as input, then we can simply run \mathcal{A} on w^+ to get an integer solution \hat{x} such that $\sum_{(i,S) \in E} \hat{x}_{i,S} w_{i,S}^+ \geq \frac{O^*}{\alpha}$. But in our case \mathcal{A} requires a valuation that satisfies monotonicity, so we cannot directly feed it w^+ . However one can simply “monotonize” w^+ : for each i define valuation \tilde{v}_i by $\tilde{v}_i(S) = \max_{T \subseteq S: (i,T) \in E} w_{i,T}^+$ where the maximum is 0 if there is no $T \subseteq S$ such that $(i, T) \in E$. We use \mathcal{A} on valuation \tilde{v} to compute an α -approximate integer solution \tilde{x} , so $\sum_{i,S} \tilde{x}_{i,S} \tilde{v}_{i,S} \geq \frac{O^*}{\alpha}$ since $\tilde{v}_{i,S} \geq w_{i,S}^+$ for every (i, S) . It is easy to transform \tilde{x} to \hat{x} so that $\sum_{(i,S) \in E} \hat{x}_{i,S} w_{i,S}^+ = \sum_{i,S} \tilde{x}_{i,S} \tilde{v}_{i,S}$. We set $\hat{x}_{i,S} = \tilde{x}_{i,S}$ if $(i, S) \in E$ or $\tilde{x}_{i,S} = 0$, otherwise set $\hat{x}_{i,T'} = 1$ for $T' = \arg \max_{T \subseteq S: (i,T) \in E} w_{i,T}$, and $\hat{x}_{i,S} = 0$. Finally, we use Claim 3.2 to convert \hat{x} to a solution $x^l \in \mathbb{Z}(\mathcal{P})$, which gives the desired integer solution. \square

Lemma 3.4 *One can obtain in polynomial time a decomposition $\frac{x^*}{\alpha} = \sum_{l \in \mathcal{I}} \lambda_l x^l$ where $\lambda_l \geq 0$ for every l (with only polynomially many positive λ_l) and $\sum_{l \in \mathcal{I}} \lambda_l = 1$.*

PROOF. We first show that the optimal value of (D), and hence of (P) by strong duality, is exactly 1. So an optimal solution to (P) yields the convex decomposition. Setting $z = 1, w_{i,S} = 0$ for all $(i, S) \in E$ gives a feasible solution with value 1. We claim that any feasible solution (w, z) has value at most 1. Suppose $\frac{1}{\alpha} \cdot \sum_{(i,S) \in E} x_{i,S}^* w_{i,S} + z > 1$. Using Claim 3.3 one can find an integer solution x^l such that $\sum_{(i,S) \in E} x_{i,S}^l w_{i,S} \geq \frac{1}{\alpha} \cdot \sum_{(i,S) \in E} x_{i,S}^* w_{i,S} > 1 - z$, contradicting the feasibility of (w, z) .

The above argument shows that we can add the inequality $\frac{1}{\alpha} \cdot \sum_{(i,S) \in E} x_{i,S}^* w_{i,S} + z \geq 1$ to the dual program (D) without altering anything. We will run the ellipsoid method on (D) to identify a dual program with a polynomial-size set of inequalities (5), that is equivalent to (D). These inequalities will be the violated inequalities returned by the separation oracle during the execution of the ellipsoid method, that are used to cut the ellipsoid. Taking the dual of this compact program gives a primal program with a polynomial number of variables and constraints which we can solve to get λ_l values that sum to 1; this gives the desired decomposition. The separation oracle that we use is as follows: at a point (w, z) , if $\frac{1}{\alpha} \cdot \sum_{(i,S) \in E} x_{i,S}^* w_{i,S} + z > 1$, then we can find an x^l and a corresponding violated constraint using Claim 3.3; otherwise we use the half space $\frac{1}{\alpha} \sum_{(i,S) \in E} x_{i,S}^* w_{i,S} + z \geq 1$ to cut the current ellipsoid. \square

With the full proof in mind, it is clear why we need the requirement that the algorithm \mathcal{A} should verify the integrality gap for all (monotone) valuation functions. In the dual LP (D), we have a variable $w_{i,S}$ for every positive $x_{i,S}^*$ variable of (CA-P). These variables $w_{i,S}$ are viewed as a valuation function and the “gap verifier” \mathcal{A} is invoked on an input derived from these $w_{i,S}$ variables in Claim 3.3 to find a violated constraint of (D). But since the $w_{i,S}$ variables are unconstrained, \mathcal{A} must work for arbitrary valuation functions (nonnegativity and monotonicity are “manually” added using the packing property of the domain). Thus, the integrality gap must be “verified” for all valuation functions. To design a similar mechanism for a restricted class of valuations, one must design a new LP that reflects the restricted structure.

4. APPLICATIONS

4.1. General and multi-unit combinatorial auctions

In multi-unit combinatorial auctions (MUCAs) we have m items with B copies of each item, and n players, and each player desires at most one copy of an item. With $B = 1$ we get the regular combinatorial auction. The LP relaxation for MUCA is similar to (CA-P), but the RHS of constraints (2) changes to B . The integrality gap of this relaxation is a function of B : (i) the integrality gap is $O(m^{\frac{1}{B+1}})$ for any $B \geq 1$; (ii) the integrality gap is $(1 + \epsilon)$ when $B = \Omega(\log m)$ (more precisely $B \geq c(\epsilon) \cdot \log m$ where $c(\cdot)$ increases with $\frac{1}{\epsilon}$) for any $\epsilon > 0$. Moreover there are algorithms that “verify” this gap, e.g., the derandomization of “standard” randomized rounding [Raghavan 1988], the rounding approach of [Kolliopoulos and Stein 2004], or the recent primal-dual algorithm of [Briest et al. 2005].

We can use the above approximation algorithms to construct randomized, strategic, approximation mechanisms for CAs and MUCAs, with arbitrary valuation functions. There are two (linked) issues here: (1) the representation of the input, and (2) the computational effort needed to solve (CA-P). With general valuations, representation becomes an issue since the length of the valuation can be exponential in m , which therefore also renders direct revelation mechanisms intractable. Two ways to address this have been considered: (a) assuming that we have “short” valuations that can be succinctly described (with a suitable bidding language), thus allowing for direct revelation mechanisms; (b) assuming that we have some oracle access to the valuation, so the mechanism now needs to be an iterative mechanism. It is well known in the economics literature that the issue of “one-shot” vs. iterative mechanisms also affects truthfulness properties. To specify our results precisely and address (1) and (2), we consider these two settings separately.

Short valuations. We first consider the case when the valuations are succinctly describable. An important such valuation class is that of single-minded bidders where each player wants just one set (or any superset) and specifies that set along with its value. More generally players could specify $k \geq 1$ subset-value pairs $(S_1, w_1), \dots, (S_k, w_k)$, which yields two well-studied classes of valuations; (a) an *XOR* valuation where the player desires *one* of these k subsets (the “ k -minded case”), so $v(T) = \max_{i: S_i \subseteq T} w_i$; (b) an *OR* valuation where the player is willing to receive *any* collection of disjoint sets from S_1, \dots, S_k and the values add up, so $v(T) = \max_{\text{disjoint sets } S_{i_1}, \dots, S_{i_\ell} \subseteq T} (v(S_{i_1}) + \dots + v(S_{i_\ell}))$. It is easy to see that for both these classes of valuations, one can devise a demand oracle for the valuation from the above description with running time polynomial in k for an *XOR* valuation, and exponential in k for an *OR* valuation. Hence, one can solve the LP (CA-P) in polynomial time [Blumrosen and Nisan 2005] (see also “General valuations” below) in the following two cases: (a) *XOR* valuations, when $k = \text{poly}(m, n)$; and (b) *OR* valuations, when $k = O(\log(m + n))$. We use “short” valuations below to encode both, succinctness of descriptions, and the requirement that (CA-P) can be solved in time polynomial in m and n .

Theorem 4.1 *For MUCAs with “short” valuations and B copies of each item, we obtain randomized, truthful in expectation mechanisms with the following approximation factors: (i) a factor of $O(m^{\frac{1}{B+1}})$ for any $B \geq 1$; and (ii) a $(1 + \epsilon)$ -guarantee for any $\epsilon > 0$ when $B = \Omega(\log m)$.*

We obtain the *first truthful mechanisms* with non-trivial approximation guarantees for *all values* of B , and with short valuations, improve upon the deterministic $O(B \cdot m^{\frac{1}{B-2}})$ -approximation ratio of Bartal et al. [2003] for general valuations. In particular, when $B = \Omega(\log m)$ we get the *first truthful (in expectation) $(1 + \epsilon)$ -approximation mechanism* for short multi-parameter valuations, answering an open question in [Archer et al. 2003] about devising mechanisms for valuations more general than the “known” single-minded case (i.e., the sets are public). More work has been directed toward the single-minded case defined in [Lehmann et al. 2002] who gave a deterministic mechanism with an $O(\sqrt{m})$ guarantee when $B = 1$. Archer et al. [2003] obtained a $(1 + \epsilon)$ -approximation mechanism when $B = \Omega(\log m)$, for the “known” single-minded case that is truthful both in expectation and with high probability. Recently, Briest et al. [2005] gave a deterministic $O(m^{\frac{1}{B}})$ -approximation mechanism for the unknown single-minded case. We give a unified way to obtain randomized, truthful in expectation mechanisms and get approximation guarantees that match the known inapproximability results [Bartal et al. 2003].

General valuations. We now consider the setting with general valuations with an oracle access to the valuations. Two kinds of oracle access were considered by [Nisan and Segal 2006; Blumrosen and Nisan 2005]: *value queries*, where the query asks for the value of a set S , and *demand queries*, where the query specifies item prices p_1, \dots, p_m , and asks a player i to return a subset S that maximizes $v_i(S) - \sum_{j \in S} p_j$. Demand queries are very natural from an economic perspective and are known to be strictly more powerful than value queries [Nisan and Segal 2006; Blumrosen and Nisan 2005]. Blumrosen and Nisan [2005] show that LP (CA-P) can be solved with a polynomial number of demand queries using the ellipsoid method, since they yield a separation oracle for the dual of (CA-P). This addresses issue (2).

As mentioned previously, direct revelation mechanisms become ineffective with general valuations. Using Theorem 3.1 we can construct strategic, iterative mechanisms for general valuations using demand queries. It is well known in the economics literature (see e.g., [Conitzer and Sandholm 2004]) that moving from direct-revelation to iterative mechanisms often leads to a weakening of the solution concept, from dominant strategies to *ex-post Nash equilibrium*. Our mechanisms yield truthfulness in expectation as an *ex-post Nash equilibrium*, which means the following: for any player i , and *any type profile* $v_{-i} \in V_{-i}$ of the other players, if the other players act according to their types in this profile in the iterative mechanism, then i ’s best response (for maximizing expected utility) is to be truthful. In particular, this means that truthful revelation is a Nash equilibrium with no *ex-post regret*, that is, even if a player were told beforehand the types that the other

players would use to act in the iterative mechanism, he would have no incentive to deviate from his truth-telling strategy.⁴

Theorem 4.2 *For MUCAs with “general” valuations and demand oracles, and B copies of each item, we obtain randomized mechanisms for which truthfulness in expectation is an ex-post Nash equilibrium, with the following guarantees: (i) an $O(m^{\frac{1}{B+1}})$ -guarantee for any $B \geq 1$; and (ii) a $(1 + \epsilon)$ -guarantee for any $\epsilon > 0$ when $B = \Omega(\log m)$.*

Very little is known about truthful and approximation mechanisms with general valuations. For $B \leq 2$ and general valuations, no strategic mechanisms were known previously. Bartal et al. [2003] gave a deterministic, truthful $O(B \cdot m^{\frac{1}{B-2}})$ -approximation for general valuations using demand oracles, and Dobzinski et al. [2005] gave a deterministic, truthful $O(\sqrt{m})$ -approximation for $B = 1$ and subadditive valuations using value oracles. We improve upon the performance guarantee of [Bartal et al. 2003] for all B , and get the same guarantee as [Dobzinski et al. 2005] for general valuations but using demand oracles, randomization, and a different solution concept.

4.2. General multi-unit auctions and multi-parameter knapsack

In a *multi-unit auction*, there are m identical items, and each player i has a value $v_i(j)$ for getting j items, $1 \leq j \leq m$, where the $v_i(\cdot)$ s are non-decreasing functions. The goal is to distribute the m items, allocating x_i items to player i , so as to maximize $\sum_i v_i(x_i)$. This problem is solvable in time polynomial in m , so if each $v_i(j)$ is explicitly specified then one can implement VCG. We will consider valuations that are specified more succinctly, e.g., step functions, piecewise linear functions with a “small” number of pieces, *XOR*, *OR* valuations or their combinations etc., or valuations given via an oracle access. We want mechanisms that run in time polynomial in n and the size of the specification.

If all value functions are step functions (single-minded players), then this is exactly the knapsack problem, for which Briest et al. [2005] gave a truthful FPTAS. Kothari et al. [2003] gave an “approximately truthful” FPTAS for the special case of “marginal decreasing valuations”. We obtain the *first* truthful, approximation mechanisms for general multi-unit auctions (i.e., multi-parameter knapsack problems). We consider the following natural LP relaxation for this problem:

$$\begin{aligned} \max \quad & \sum_{i,j} v_i(j)x_{ij} && \text{(KN-P)} \\ \text{subject to} \quad & \sum_j x_{ij} \leq 1 && \text{for each player } i \\ & \sum_{i,j} j \cdot x_{ij} \leq m \\ & x_{i,j} \geq 0 && \text{for each } i, j. \end{aligned}$$

Here variable x_{ij} indicates if player i gets j items. When the $v_i(\cdot)$ s are step functions this LP reduces to the standard LP relaxation for Knapsack, for which a simple greedy algorithm proves an integrality gap of at most 2 (see, e.g., [Kellerer et al. 2004]). Lawler [1979] describes an algorithm that bounds the integrality gap of (KN-P) by 2, which is attributed to d’Atri [1977]. We give a somewhat simpler exposition of this algorithm as a greedy algorithm that generalizes the 2-approximation algorithm for Knapsack. Using this, we obtain the *first truthful, approximation mechanisms for non-single-minded players* and get a guarantee of 2. Lavi et al. [2003] showed that with two players, if all items must always be allocated, then with *OR* valuations, no *deterministic* truthful mechanism can obtain an approximation ratio better than 2. As in Section 4.1, “short” valuations will mean that the valuation is given succinctly and we can solve the LP in polynomial time.

⁴Recall the example given in the introduction, which considers the regular second-price auction with two players with an iterative flavor.

Since items are identical, a demand oracle here fixes a price $p \geq 0$ and asks player i to return a quantity j that maximizes $v_i(j) - p \cdot j$.

Theorem 4.3 *There is a randomized, 2-approximation mechanism for multi-unit auctions, which (i) is truthful in expectation for “short” valuations; and (ii) has truthfulness in expectation as an ex-post Nash equilibrium for general valuations with demand oracles.*

We now give the greedy algorithm which proves an integrality gap of 2 for (KN-P). Let OPT be the value of the LP-optimum. Define the marginal value function of i given quantity j , $v_i(\cdot|j)$, as follows: for any $x \geq 0$, $v_i(x|j) = v_i(x + j) - v_i(j)$.

- (1) Initialize $M \leftarrow m$. Each player i starts off with $q_i = 0$ items. While $M > 0$ we repeatedly do the following: (a) find i^*, j^* that maximizes $v_i(j|q_i)/j$; (b) if $j^* \leq M$, set $q_{i^*} \leftarrow q_{i^*} + j^*$ (i.e., allocate j^* more items to i^*); (c) decrement M by j^* .
- (2) Let $\text{Greedy} = \sum_i v_i(q_i)$ be the value of this allocation, and let $\text{Max} = \max_i v_i(m)$. If $\text{Max} > \text{Greedy}$, allocate all items to the player with the maximum $v_i(m)$, otherwise return (q_1, \dots, q_n) as the allocation.

Lemma 4.1 *The above algorithm finds an allocation with value at least $OPT/2$.*

PROOF. We will exhibit a feasible dual solution with value at most twice the value obtained by the algorithm, hence the claim will follow. The dual program is

$$\begin{aligned} \min \quad & \sum_i \alpha_i + m \cdot \beta \\ \text{subject to} \quad & \alpha_i \geq v_i(j) - j \cdot \beta \quad \text{for all } i, j \\ & \beta, \alpha_i \geq 0 \quad \text{for all } i. \end{aligned}$$

Suppose the algorithm stops at the *end* of iteration $s + 1$, that is, *after* M it is decremented in iteration $s + 1$, we have $M \leq 0$. Let (i_l, j_l) be the (i^*, j^*) pair in iteration l for $l = 1, \dots, s + 1$. Recall that q_i is the number of items allocated to player i . Let $q_{i,k}$ denote the quantity $\sum_{l=1}^k j_l$, and let $p_i = q_{i,s}$. So $\sum_{l=1}^{s+1} j_l = \sum_i p_i + j_{s+1} \geq m$. Note that $p_i \leq q_i$, and it could be that $p_i < q_i$ — this can happen only if $\sum_{l=1}^{s+1} j_l = m$ and $i = i_{s+1}$, so $q_i = p_i + j_{s+1}$. We will exhibit a feasible dual solution of value at most $2 \max\{\sum_i v_i(p_i), \text{Max}\}$. Define $\beta = v_{i_{s+1}}(j_{s+1}|q_{i_{s+1}})/j_{s+1}$, and $\alpha_i = v_i(p_i) - p_i \cdot \beta$ for every i . Before verifying feasibility, we show that this proves the lemma:

$$\sum_i \alpha_i + m \cdot \beta \leq \sum_i (\alpha_i + p_i \cdot \beta) + j_{s+1} \cdot \beta = \sum_i v_i(p_i) + v_{i_{s+1}}(j_{s+1}|q_{i_{s+1}}) \leq 2 \max\left\{\sum_i v_i(p_i), \text{Max}\right\}.$$

Consider any iteration $l = 1, \dots, s$. Let $i = i_l, q = q_{i,l-1}$ and $i' = i_{l+1}, q' = q_{i',l}$. We claim that $v_i(j_l|q)/j_l \geq v_{i'}(j_{l+1}|q')/j_{l+1}$. This is clear from the definition of (i^*, j^*) if $i \neq i'$, otherwise this follows since $q' = q + j_l$, and $v_i(j_l|q)/j_l \geq v_i(j_l + j_{l+1}|q)/(j_l + j_{l+1}) = (v_i(j_l|q) + v(j_{l+1}|q'))/(j_l + j_{l+1})$.

Now fix any i . For $j \geq p_i$, by the definition of β we have $\beta \geq v_i(j - p_i|p_i)/(j - p_i)$ or equivalently, $\alpha_i \geq v_i(j) - j \cdot \beta$. Consider the piecewise-linear function f_i passing through the points $(q_{i,l}, v_i(q_{i,l}))$, $l = 0, \dots, s$ (where $q_{i,0} = 0$). By our earlier claim, $f_i(\cdot)$ is a *concave* (increasing) function, and each segment of $f_i(\cdot)$ has slope at least β . These two facts imply that the line passing through $(p_i, f_i(p_i))$ with slope β lies above the $f_i(\cdot)$ curve in $[0, p_i]$. Also note that for any $j \leq p_i$, $f_i(j) \geq v_i(j)$ since if $j \in [q_{i,l}, q_{i,l+1}]$ for some l , then $f_i(j) = v_i(q_{i,l}) + (j - q_{i,l}) \cdot \frac{v_i(j_{l+1}|q_{i,l})}{j_{l+1}} \geq v_i(q_{i,l}) + (j - q_{i,l}) \cdot \frac{v_i(j - q_{i,l}|q_{i,l})}{j - q_{i,l}} = v_i(j)$. Combining these facts, we get that for any $j \leq p_i$, $f_i(p_i) - (p_i - j) \cdot \beta \geq f_i(j) \geq v_i(j)$ which when rearranged gives $\alpha_i \geq v_i(j) - j \cdot \beta$. \square

4.3. Graph routing problems

We now consider two closely related problems, *edge-disjoint-paths* (EDP) and *all-or-nothing multi-commodity flow* (ANF). In both EDP and ANF we have a graph $G = (V, E)$ with capacities $u_e \geq 1$ on the edges. The players are (s_i, t_i) source-sink pairs where $s_i, t_i \in V$. Each player has a value w_i . Both (s_i, t_i) and the value w_i are private information; a special case is the “known” case where the (s_i, t_i) pairs are public and only w_i is private. The social-welfare maximization problem is to select a maximum-weight routable set. In EDP, a set is routable if each (s_i, t_i) pair in the set can be assigned an s_i - t_i path and at most u_e paths use edge e ; in ANF, for each (s_i, t_i) pair in the set we need to route one unit of flow from s_i to t_i respecting edge capacities, possibly splitting the flow across several paths. For the mechanism-design problem, we define the outcome set carefully to ensure that only players’ values for an outcome, and not the set itself, depends on his private information. For EDP, an outcome is an allocation of edges (as paths) to players such that each edge e is used at most u_e times (and player i receives value w_i if he is allocated an s_i - t_i path); for ANF, an outcome is a flow-vector allocation to each player, such that the total flow through each edge e is at most u_e (and player i receives value w_i if his flow-vector sends one unit of flow from s_i to t_i).

We apply our techniques to obtain two types of results for EDP and ANF. Let $B = \min_e u_e$. First, we observe that Theorem 4.1 yields a truthful (in expectation) $O(m^{\frac{1}{B+1}})$ -approximation mechanism for both problems. Next, we show that for the *known* case, we can translate the improved guarantees of [Chekuri et al. 2005] for EDP and ANF on certain graph classes to the mechanism-design setting to obtain truthful mechanisms with *matching* approximation guarantees for EDP and ANF (on the appropriate graph classes).

Both EDP and ANF admit the following flow-path based LP relaxation. We use P below to index the collection Path of all (simple) paths in G .

$$\begin{aligned}
 \max \quad & \sum_{i,P} v_i(P) f_{i,P} && \text{(Route-P)} \\
 \text{subject to} \quad & \sum_P f_{i,P} \leq 1 && \text{for each player } i \\
 & \sum_i \sum_{P:e \in P} f_{i,P} \leq u_e && \text{for each edge } e \in E \\
 & f_{i,P} \geq 0 && \text{for each } i, P.
 \end{aligned}$$

Let Path_i denote the collection of s_i - t_i paths. Here $f_{i,P}$ denotes the amount of flow on path P , and $v_i(P) = w_i$ if $P \in \text{Path}_i$, and is 0 otherwise. It is easy to see that an integral solution corresponds to an EDP solution, and a solution where $\sum_P f_{i,P}$ is integral for each player i corresponds to an ANF solution. Observe that EDP is a structured MUCA with short valuations (since one can construct a demand oracle for player i , given $(s_i, t_i; w_i)$), and (Route-P) is simply a specialization of (CA-P) (where items are edges, and $v_i(S) = w_i$ if S contains an s_i - t_i path, and is 0 otherwise). Also, a solution to EDP is also clearly a solution to ANF. Thus, Theorem 4.1 yields a randomized, truthful $O(m^{\frac{1}{B+1}})$ -approximation for both problems.

Chekuri et al. [2005] use the above LP to obtain approximation guarantees of (i) $O(\log m)$ for EDP on planar graphs when $B \geq 2$; and (ii) $O(\log^2 m)$ for ANF on general graphs, and $O(\log m)$ for planar graphs. (The guarantees are stated for $w_i = 1$, but it is implicit that the algorithms generalize to arbitrary w_i .) Notice however that this *does not* imply analogous bounds on the integrality gap of (Route-P) for these graph classes since the valuation functions arising in EDP and ANF are *structured valuations*. (In fact, it is not hard to cast MUCA as EDP, so the integrality gap of (Route-P) with $u_e = B$ for all e is $\Theta(m^{\frac{1}{B+1}})$.) However, we show that in the known case, our techniques can be used to obtain matching approximation guarantees in the mechanism-design setting.

The key observation is that since each player i ’s (true) value depends (linearly) only on the *amount of flow* routed from s_i to t_i (which are publicly known) and not on the actual flow-paths that are

chosen, it suffices to obtain a “partial” decomposition such that the (total flow routed for an (s_i, t_i) pair by the convex combination) = (total flow routed for (s_i, t_i) by the LP)/ α . To see this formally, recall that (see Lemma 3.1) to translate the fractional VCG mechanism to (a support mechanism, and hence) a truthful-in-expectation mechanism, we require a convex combination $\sum_{l \in \mathcal{I}} \lambda_l(v) x^l$ that satisfies $\sum_{l \in \mathcal{I}} \lambda_l(v) \bar{v}_i(x^l) = \bar{v}_i(f^*(v))/\alpha$ for each player i , where $\bar{v}_i(f)$ is the true value of player i for a feasible solution f to (Route-P), and $f^*(v)$ is an optimal solution to (Route-P) for the valuation-profile v . In the known case, $\bar{v}_i(f) = \bar{w}_i(\sum_{P \in \text{Path}_i} f_{i,P})$, and so a “partial” decomposition of $f^*(v)$ suffices to yield this property; but if (s_i, t_i) is private information, then this is no longer true, and one needs to resort to a “complete” decomposition (which requires an integrality-gap-verifying algorithm for (Route-P)).

We now argue briefly that an α -approximation algorithm for EDP or ANF based on the LP (Route-P) can be used to obtain a partial decomposition (with the same α), enabling us to translate the approximation guarantees of [Chekuri et al. 2005] to the mechanism-design setting. Similar results are known with demands d_i when $\max d_i \leq B$ and these also transfer to the mechanisms. For notational convenience, given a solution f to (Route-P), we introduce auxiliary variables $x_i := \sum_{P \in \text{Path}_i} f_{i,P}$ to denote the total flow routed for player i . The set of “integer” solutions $\{(f^l, x^l)\}_{l \in \mathcal{I}}$ that the decomposition uses is (i) the set of integer solutions to (Route-P) for EDP; and (ii) the set of solutions to (Route-P) with integral x_i s for ANF. (Note that for EDP, the corresponding set satisfies the packing property, and for ANF, the projection of the set to the x -space satisfies the packing property.) To partially decompose a solution (f^*, x^*) , we solve the following primal and dual LPs.

$$\begin{aligned} \min \quad & \sum_{l \in \mathcal{I}} \lambda_l & (\text{P}') \\ \text{s.t.} \quad & \sum_l \lambda_l x_i^l = \frac{x_i^*}{\alpha} \quad \text{for all } i \\ & \sum_l \lambda_l \geq 1 \\ & \lambda_l \geq 0 \quad \text{for all } l \in \mathcal{I}. \end{aligned}$$

$$\begin{aligned} \max \quad & \frac{1}{\alpha} \cdot \sum_i x_i^* \pi_i + z & (\text{D}') \\ \text{s.t.} \quad & \sum_i x_i^l \pi_i + z \leq 1 \quad \text{for all } l \in \mathcal{I} \quad (6) \\ & z \geq 0 \\ & \pi_i \text{ unconstrained} \quad \text{for all } i \in E. \end{aligned}$$

Arguments that are almost identical to those in Section 3.2 apply to this pair of LPs. Their optimal value is 1, and it is not hard to see that an LP-based α -approximation algorithm for EDP or ANF can be used to find a violated inequality (6) when $\frac{1}{\alpha} \cdot \sum_i x_i^* \pi_i + z > 1$. So we obtain a separation oracle for (D') as before, and this can be used to obtain a compact dual LP, and hence, a compact primal LP (with optimal value 1) whose solution yields the partial decomposition.

Previous truthful mechanisms for EDP were: for the “known” case, a deterministic $O(\sqrt{m})$ -approximation when $d_i = 1$ using the greedy algorithm in [Lehmann et al. 2002], and a deterministic $O(m^{\frac{1}{B-1}})$ -approximation mechanism [Briest et al. 2005] when $B > 1$; in the “unknown” case [Bartal et al. 2003] gave an $O(B \cdot (\frac{m}{\min d_i})^{\frac{1}{B-2}})$ -approximation when $B > 2$. [Babaioff et al. 2009] give a deterministic $O(\log^2 w_{\max} \cdot \sqrt{m})$ -approximation mechanism for $B = 1$ under the concept of undominated strategies.

4.4. Covering problems

While we focus on packing problems, another broad class of optimization problems that has natural game-theoretic aspects is covering problems. Our techniques can be adapted to yield some partial results for this class of problems. As an illustrative example, consider the *set cover* problem, which can be used to abstract the following setting. A buyer needs to compose a team of workers that together cover a set of capabilities. Each worker offers some of these capabilities, and incurs a certain cost if hired as part of the team. The optimization problem is to select a minimum-cost set of workers that cover the required capabilities. In the mechanism-design setting (sometimes referred to as a *procurement auction*), the workers' costs and/or capabilities are private information, and one therefore seeks to construct a truthful mechanism that achieves a "good" approximation ratio. (As in the case of graph routing problems, we need to define the outcome set carefully so that only players' values for an outcome and not the set itself depends on private information.) If the integrality gap of the LP relaxation of the covering problem is $\alpha > 1$ (as verified by an α -approximation algorithm), then it is not hard to see that (by dovetailing the arguments in Section 3.2), given an LP-solution x , one can decompose $\alpha \cdot x$ into a convex combination of integer solutions where *multiple copies* of a worker may be purchased. That is, these integer solutions (and hence, the random integer solution specified by the convex combination) are only feasible for the original problem provided a worker may be hired multiple times; in such cases our method yields an α -approximation, truthful (in expectation) mechanism.

An example of such a setting is the *multiset multicover problem with multiplicities*, where each capability must be covered a certain number of times, each worker's private information is a vector specifying the amounts of the different capabilities he offers, and there is no limit on how many copies of a worker may be chosen. Another example is the class of *network design problems*, where each worker owns edges of an underlying known graph: the identity of the edges owned and their costs are private, and the goal is to select a minimum-cost edge-set satisfying certain connectivity requirements, possibly with other side constraints such as degree bounds. Such network design problems often come in two flavors, one where there is a bound on the number of times an edge may be selected, and one where there is no such bound. Our technique yields truthful, approximation mechanisms for the latter class of problems with guarantees matching that of the best known LP-based (integrality-gap-verifying) approximation algorithm for the problem.

We also remark that for *single-dimensional* covering problems—e.g., network design problems where each edge is a separate player and its cost is private information—we can adapt our proofs to show that one can decompose $\min\{\alpha \cdot x, \mathbf{1}\}$ into a convex combination of *feasible* integer solutions to the problem (that is, we no longer need to buy multiple copies). (Here $\mathbf{1}$ denotes the all ones vector and \min denotes component-wise minimum.) The resulting randomized mechanism then satisfies *value monotonicity*, a necessary and sufficient condition for truthfulness, and we again get a general result: *given an LP-based α -approximation for a covering problem, one can get an α -approximation truthful mechanism for the analogous single-dimensional mechanism-design problem.* As an application, we mention that this immediately yields the first truthful, approximation mechanisms for the single-dimensional mechanism-design version of *survivable network design* (possibly with degree constraints) with approximation guarantees matching those of the algorithmic problem.

A very interesting open problem is to design a truthful approximation mechanisms for multidimensional covering problems when such multiplicities are not allowed.

5. CONCLUSIONS AND DISCUSSION

We have presented a general method for devising randomized, truthful-in-expectation mechanisms for packing problems that allows one to exploit approximation algorithms and obtain matching approximation guarantees for the mechanism-design problem. Given an α -approximation algorithm that also bounds the integrality gap of the LP-relaxation of a packing problem by α , we show how to design a truthful mechanism with the same approximation ratio. Our method proceeds by decomposing the optimal *LP-solution* scaled down by α into a convex combination of integer solutions,

which can then be viewed as a probability distribution over integer solutions. We show that the payments of the fractional VCG mechanism (whose outcome is the LP-optimum) can be modified and combined with the above randomized algorithm to yield a randomized mechanism that is truthful in expectation. We demonstrate the usefulness of our technique on a variety of problem domains: combinatorial auctions, multi-unit auctions, multi-unit combinatorial auctions, and graph-routing problems (edge-disjoint-paths (EDP), all-or-nothing multicommodity flow (ANF)). In many cases, the approximation guarantees we obtain are the best possible if one requires polynomial-time computation (unless $P=NP$).

It is instructive to note that our method can also be viewed as constructing a *maximal-in-distributional-range* (MIDR) mechanism (see [Dobzinski and Dughmi 2009]). That is, instead of presenting our method as one where we first obtain the fractional VCG mechanism and then translate this to a randomized mechanism, we can view our construction as one that uses an α -integrality-gap-verifying approximation algorithm to *exactly optimize* the social welfare over a subset of the convex hull of integer solutions, and hence, implement VCG over a suitable (fixed) outcome set. To see this, let \mathcal{P}_I denote the convex hull of integer points in \mathcal{P} (i.e., $\mathbb{Z}(\mathcal{P})$), where \mathcal{P} is the polytope of feasible solutions to the LP-relaxation of the packing problem. Observe that the outcome of any randomized or support mechanism corresponds to a point in \mathcal{P}_I . Our decomposition lemma (Lemma 3.4) shows that $\mathcal{P}/\alpha \subseteq \mathcal{P}_I$; also, we can efficiently optimize over \mathcal{P}/α since this is equivalent to optimizing over \mathcal{P} . Thus, our randomized (or deterministic support) mechanism (which returns the optimum over \mathcal{P}/α as its outcome) is essentially VCG over the outcome-set \mathcal{P}/α . (And the α -approximation ratio follows since the optimum value over \mathcal{P}/α is within an α -factor of the optimum over \mathcal{P} .)

Subsequent to the publication of the conference version of this paper [Lavi and Swamy 2005], various other solutions have been obtained for combinatorial auctions and multi-unit auctions. For combinatorial auctions, [Dobzinski et al. 2006; Dobzinski 2008] obtain the same approximation guarantees that we obtain but under the stronger solution concept of universal truthfulness. For multi-unit auctions, [Dobzinski and Nisan 2007] give a deterministic truthful 2-approximation, and [Dobzinski and Dughmi 2009] obtain an FPTAS that is truthful in expectation (also via an MIDR mechanism). These mechanisms are however *tailored* to the specific problem considered; in contrast, our method is the only (currently known) *general* method to convert approximation algorithms to truthful mechanisms (with matching approximation guarantees) for multidimensional problem domains. It is also worth noting that our mechanisms have remained the state-of-art for other problem domains, most notably, multi-unit combinatorial auctions, where no other truthful mechanism achieves similar approximation guarantees.

One of the insights to emerge from our work is that fractional truthful mechanisms combined with a suitable rounding scheme can be an effective tool in truthful mechanism design even for multidimensional domains. The versatility and usefulness of this approach has been reinforced in various subsequent works, such as [Lavi and Swamy 2009; Golovin 2007; Dughmi and Ghosh 2010; Hoefer et al. 2011]. The latter three papers [Golovin 2007; Dughmi and Ghosh 2010; Hoefer et al. 2011] all devise truthful-in-expectation mechanisms for their respective problems (stochastic market planning, generalized assignment problem, secondary spectrum auctions) by first devising a fractional truthful mechanism and then adapting our rounding ideas to convert this into the desired randomized mechanism. Lavi and Swamy [2009] consider a special case of the minimum-makespan scheduling problem on unrelated machines. In their case, constructing a fractional truthful mechanism is non-trivial since makespan minimization is not a social-welfare-maximization problem, and the rounding scheme is tailored to the problem at hand and different from the one proposed here.

ACKNOWLEDGMENTS

We thank Bruce Shepherd for very useful discussions about the results in [Chekuri et al. 2005]. We also thank the anonymous referees for their useful suggestions.

REFERENCES

- ARCHER, A., PAPADIMITRIOU, C., TALWAR, K., AND TARDOS, É. 2003. An approximate truthful mechanism for combinatorial auctions with single parameter agents. In *Proceedings of the 14th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. 205–214.
- ARCHER, A. AND TARDOS, É. 2001. Truthful mechanisms for one-parameter agents. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*. 482–491.
- BABAIOFF, M., LAVI, R., AND PAVLOV, E. 2009. Single-value combinatorial auctions and implementation in undominated strategies. *Journal of the ACM* 56(1), 4:1 – 4:32.
- BARTAL, Y., GONEN, R., AND NISAN, N. 2003. Incentive compatible multi-unit combinatorial auctions. In *Proceedings of the 9th Conference on Theoretical Aspects of Rationality and Knowledge (TARK)*. 72–87.
- BLUMROSEN, L. AND NISAN, N. 2005. On the computational power of iterative auctions. In *Proceedings of the 6th ACM Conference on Electronic Commerce (EC)*. 29–43.
- BRIEST, P., KRYSIA, P., AND VÖCKING, B. 2005. Approximation techniques for utilitarian mechanism design. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC)*. 39–48.
- CARR, R. AND VEMPALA, S. 2002. Randomized metarounding. *Random Structures and Algorithms* 20(3), 343–352.
- CHEKURI, C., KHANNA, S., AND SHEPHERD, F. 2005. Multicommodity flows, well-linked terminals and routing problems. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC)*. 183–192.
- CHVÁTAL, V. 1983. *Linear programming*. WH Freeman.
- CLARKE, E. 1971. Multipart pricing of public goods. *Public Choice* 8, 17–33.
- CONITZER, V. AND SANDHOLM, T. 2004. Computational criticisms of the revelation principle. In *Proceedings of the 5th ACM Conference on Electronic Commerce (EC)*. 262–263.
- D’ATRI, G. 1977. The generalized knapsack problem. Communication at the Annual meeting of CNR-GNIM, Rimini, Italy.
- DOBZINSKI, S. 2008. Two randomized mechanisms for combinatorial auctions. In *Proceedings of the 11th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX)*. 89–103.
- DOBZINSKI, S. AND DUGHMI, S. 2009. Truthful randomized mechanisms for combinatorial auctions. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*. 505–514.
- DOBZINSKI, S. AND NISAN, N. 2007. Mechanisms for multi-unit auctions. In *Proceedings of the 8th ACM Conference on Electronic Commerce (EC)*. 346–351.
- DOBZINSKI, S., NISAN, N., AND SCHAPIRA, M. 2005. Approximation algorithms for combinatorial auctions with complement-free bidders. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC)*. 610–618.
- DOBZINSKI, S., NISAN, N., AND SCHAPIRA, M. 2006. Truthful randomized mechanisms for combinatorial auctions. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC)*. 652–661.
- DUGHMI, S. AND GHOSH, A. 2010. Truthful assignment without money. In *Proceedings of the 11th ACM Conference on Electronic Commerce (EC)*. 325–334.
- ELBASSIONI, K., FOUZ, M., AND SWAMY, C. 2010. Approximation algorithms for non-single-minded profit-maximization problems with limited supply. In *Proceedings of the 6th Workshop on Internet and Network Economics (WINE)*. 462–472.
- GOLOVIN, D. 2007. Stochastic packing-market planning. In *Proceedings of the 8th ACM Conference on Electronic Commerce (EC)*. 172–181.
- GROVES, T. 1973. Incentives in teams. *Econometrica* 41, 617–631.
- HOEFER, M., KESSELHEIM, T., AND VÖCKING, B. 2011. Combinatorial auctions for secondary spectrum auctions. In *Proceedings of the 23rd Annual ACM Symposium on Parallelism in Algorithms and Architectures (SPAA)*.
- KELLERER, H., PFERSCHY, U., AND PISINGER, D. 2004. *Knapsack problems*. Springer-Verlag.
- KOLLIPOULOS, S. AND STEIN, C. 2004. Approximating disjoint-path problems using greedy algorithms and packing integer programs. *Mathematical Programming, Series A* 99, 63–87.
- KOTHARI, A., PARKES, D., AND SURI, S. 2003. Approximately-strategyproof and tractable multi-unit auctions. In *Proceedings of the 4th ACM Conference on Electronic Commerce (EC)*. 166–175.
- LAVI, R., MU’ALEM, A., AND NISAN, N. 2003. Towards a characterization of truthful combinatorial auctions. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*. 574–583.
- LAVI, R. AND SWAMY, C. 2005. Truthful and near-optimal mechanism design via linear programming. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*. 595–604.
- LAVI, R. AND SWAMY, C. 2009. Truthful mechanism design for multidimensional scheduling via cycle monotonicity. *Games and Economic Behavior* 67(1), 99–124.
- LAWLER, E. 1979. Fast approximation algorithms for knapsack problems. *Mathematics of Operations Research* 4(4), 339–356.

- LEHMANN, B., LEHMANN, D., AND NISAN, N. 2006. Combinatorial auctions with decreasing marginal utilities. *Games and Economic Behavior* 55(2), 270–296.
- LEHMANN, D., O'CALLAGHAN, L., AND SHOHAM, Y. 2002. Truth revelation in approximately efficient combinatorial auctions. *Journal of the ACM* 49(5), 1–26.
- NISAN, N. 2002. The communication complexity of approximate set packing and covering. In *Proceedings of the 29th International Colloquium on Automate, Languages and Programming (ICALP)*. 868–875.
- NISAN, N. AND RONEN, A. 2001. Algorithmic mechanism design. *Games and Economic Behavior* 35, 166–196.
- NISAN, N. AND SEGAL, I. 2006. The communication requirements of efficient allocations and supporting prices. *Journal of Economic Theory* 129(1), 192–224.
- RAGHAVAN, P. 1988. Probabilistic construction of deterministic algorithms: approximating packing integer problems. *Journal of Computer and Systems Sciences* 37, 130–143.
- VICKREY, W. 1961. Counterspeculation, auctions and competitive sealed tenders. *Journal of Finance* 16, 8–37.

Received May 2010; revised June 2011; accepted August 2011