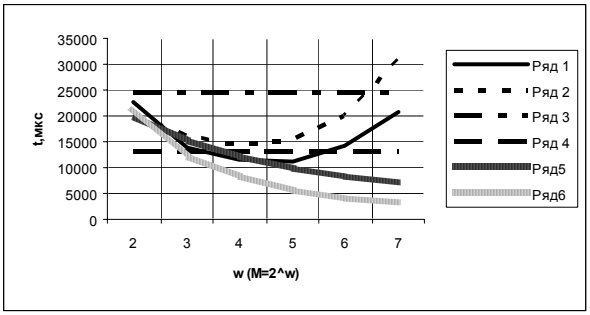


*Рисунок 1 – Результаты тестирования методов експоненцирования:*

ряд 1 – параллельный $2^w$-арный алгоритм на двух процессорах; ряд 2 – однопоточный $2^w$-арный алгоритм (алгоритм 1); ряд 3 – параллельный бинарный алгоритм с предвычислением точек $2^iP$ на двух процессорах; ряд 4 – однопоточный бинарный алгоритм с предвычислением точек $2^iP$; ряд 5 – однопоточный алгоритм максимальной памяти; ряд 6 – параллельный алгоритм максимальной памяти на двух процессорах

нию с рассмотренным параллельным бинарным с одновременным уменьшением размера таблицы предвычислений в 5 раз.

Дальнейшего увеличения скорости можно достигнуть за счет использования дополнительной памяти. Для этого на шаге вычисления частичных произведений можно использовать, например алгоритм максимальной памяти [8]. Как видно из рисунка 1, скорость этого алгоритма постепенно убывает с увеличением $w$. Однако при его использовании значительно возрастает объем таблицы предвычислений, а также время на ее построение.

В дальнейшем необходимо рассмотреть возможность использования предложенных алгоритмов для аппаратной платформы, в частности их реализация на ПЛИС.

### *ПЕРЕЧЕНЬ ССЫЛОК*


1. ДСТУ 4145–2002. Державний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. Київ: – Держстандарт України, 2003. – 39 с.
2. ГОСТ Р 34.10–2001. Государственный стандарт Российской федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки цифровой подписи. М.: Госстандарт России, 2001. – 18 с.
3. ANSI X9.62. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1998. – 182 с.
4. *Кнут Д.* Искусство программирования, том 2. Полученные алгоритмы, 3-е изд.: Уч. пос. М.: Издательский дом «Вильямс», 2001. – 832 с.
5. *Вельшенбах М.* Криптография на Си и С++ в действии. Учебное пособие.– М.: Издательство Триумф, 2004. – 464 с.
6. *Kenji Koyama, Yukio Tsuruoka.* Speeding up elliptic cryptosystems by using a signed binary window method, Advances in Cryptology. – CRYPTO'92, LNCS 740, pp. 345–357, 1993.
7. *Juan Manuel Garcia Garcia, Rolando Mechaca Garcia.* Parallel Algorithm for Multiplication on Elliptic Curves, 2002. – 9 с. http://citeseer.ist.psu.edu/
8. *Бессалов А. В., Телиженко А. Б.* Криптосистемы на эллиптических кривых. Учебное пособие. – Киев. Політехніка, 2004. – 223 с.
9. *Brickel E., Gordon D., McCurley K., Wilson D.* Fast Exponentiation with Precomputation. Advances in Cryptology. – Eurocrypt 92. LNCS 658. 1993. – P. 200–207.


Надійшла 9.08.04
Після доробки 18.05.05

*В статті розглядаються методи експоненціювання точки еліптичної кривої, зокрема методи з фіксованою точкою. Пропонується паралельний $2^w$-арний p-кратний метод, що забезпечує кращі швидкісні характеристики, ніж існуючі методи.*

*The methods of exponentiation of elliptic curve point are considered. In particular, the methods with fixed point are considered. The parallel $2^w$-arity p-order method are offered. It provides the best run-time in comparison with other known methods.*

*УДК 65.011.56.012:004(045)*

П. М. Павленко

# УПРАВЛІННЯ 3D МОДЕЛЯМИ В ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ АВТОМАТИЗОВАНОЇ СИСТЕМИ ТЕХНОЛОГІЧНОЇ ПІДГОТОВКИ ВИРОБНИЦТВА

*Розглянуті можливості моделювання в сучасних CAD системах. Представлено метод управління 3D моделями в інтегрованих АСТПВ. Наведені рекомендації по практичному використанню 3D моделей.*

### *ВСТУП*

Одним з етапів життєвого циклу виробу є технологічна підготовка виробництва (ТПВ), рівень якої багато в чому визначає якість продукції, що вироб-

ляється, строки її виходу на ринок і в кінцевому рахунку, конкурентоспроможність підприємства в цілому. Побудові та впровадженню автоматизованих систем технологічної підготовки виробництва (АСТПВ) приділялось багато уваги в 70–80-х роках двадцятого століття. Але можливості сучасних інформаційних технологій на базі CAD/CAM/CAE систем і комунікаційних технологій та радикальні зміни в промисловому виробництві, привели до появи нових понять в АСТПВ. Серед них – трьохвимірна комп'ютерна модель виробу (далі 3D модель) і сам процес моделювання в середовищі АСТПВ.

## *ПОСТАНОВКА ЗАВДАННЯ*

У технічній літературі найчастіше поняття 3D моделі трактується неоднозначно, що зв'язано з досить швидкою (за останні 10 років) зміною змісту цього поняття [1, 2]. У зв'язку з цим, доцільно провести короткий аналіз процесу розвитку методів об'ємного моделювання і структури 3D моделі, виділити ключові параметри, за допомогою яких можливе управління 3D моделями в інформаційному середовищі АСТПВ і вирішення принципово нових задач ТПВ.

## *РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ*

Перші 3D моделі мали каркасно-поверхневе представлення. У процесі такого моделювання спочатку будується каркас – просторова конструкція, що складається з відрізків прямих, дуг окружностей і сплайнів. Каркас відіграє допоміжну роль і є основою для наступної побудови поверхонь, що «натягаються» на елементи каркаса. Особливість каркасно-поверхневого моделювання полягає в тому, що елементи створюваної моделі ніяк не зв'язані один з одним. Зміна одного з елементів не спричиняє автоматичної зміни інших, що дає визначену волю дій, але одночасно значно ускладнює роботу з моделлю і вимагає великих витрат на її модифікацію. Це привело до появи технології твердотільного параметричного моделювання і можливостей управління цим процесом моделювання [3].

Твердотільне моделювання має у своїй основі ідеологію, що істотно відрізняється від ідеології каркасно-поверхневого моделювання. Твердотільна модель являє собою цілісний об'єкт, що займає замкнуту частину простору. Завжди можна точно сказати, чи знаходиться крапка всередині твердого тіла, на його поверхні чи поза тілом. При зміні в моделі будь-якого елемента будуть змінюватися всі інші елементи, що зв'язані з ним. В результаті зміниться форма твердого тіла, але збережеться його цілісність.

Твердотільне моделювання припускає можливість установки параметричних залежностей між елементами твердого тіла чи декількох тіл. При цьому зміна одного з параметрів (наприклад, довжини елемента) приводить до відповідної перебудови всіх параметрично зв'язаних елементів. Таке моделювання, назване параметричним, дає конструктору додаткові зручності. Так, можна установити параметричні залежності між елементами твердотільної зборки і, тим самим, автоматизувати контроль збирання виробу. Крім того, у твердотільної моделі зберігається історія її побудови, що дозволяє повертатися на кожній із кроків проектування і змінювати форму моделі методом зміни чисельних значень чи параметрів заміни елементів, що входять у його історію.

Однак, компоненти твердотільних моделей мають певні обмеження по складності просторових форм, що представляються ними. Це привело до створення технології гібридного моделювання. При гібридному моделюванні забезпечується можливість одночасної роботи з твердотільними об'єктами і з поверхнями. При цьому можна «відрізати» поверхнею частину твердого тіла, перетворювати замкнутий поверхнями обсяг у тверде тіло і т. п. Гібридне моделювання дозволяє сполучити всі зручності твердотільного моделювання з можливістю побудови об'єктів як завгодно складної геометричної форми [3].

Параметричний підхід, реалізований у методах твердотільного і гібридного моделювання, дає можливість автоматичного повторення методу побудови геометрії при зміні одного чи декількох його аргументів, у межах можливості самого методу. Розроблювач виробу, таким чином, одержує можливість варіювати різними параметрами з метою оптимізації цільової якості. В якості параметрів (аргументів) можуть виступати геометричні елементи (крапки, прямі, криві, площини, поверхні), чисельні параметри з одиницями виміру (відстані, кути) і чисельні параметри без розмірності.

Подальшим розвитком параметричного підходу з'явилася алгебраїчно-сценарійна параметризація [3]. Вона дозволила збагатити історію побудови найпростішими асоціативними зв'язками між елементами і визначальними їхніми розмірами. Це було важливе розширення «специфікації геометричного визначення». Можливості модифікації геометрії істотно підвищилися. Одним із проявів алгебраїчно-сценарійної параметризації стало моделювання на основі стандартизованих схем побудови («Feature Based Design»). Воно дало можливість конструктору зберігати зразок методу геометричної побудови для його наступного повторного застосування.

В даний час компанії, розроблювачі найбільш могутніх CAD/CAM-систем (таких як CATIA, Unigraphics), прагнуть проводити свої рішення у відповідності

з міжнародними інтеграційними ISO стандартами, наслідком чого є значне ускладнення представлення моделі в CAD/CAM-системі. Так, у системі CATIA V5 модель виробу може бути представлена сукупністю наступних видів інформації:

– об'ємне тіло чи таке, що не має об'єму як результат булівих операцій над складовими його форм;

– об'ємне тіло чи таке, що не має об'єму як результат застосування певного методу його побудови;

– аргументи побудови тіла у вигляді геометричних елементів;

– аргументи побудови тіла у вигляді логічних і чисельних параметрів;

– плоскі параметричні ескізи з геометричними відносинами між елементами;

– керуючі параметри;

– функції (відносини) між елементами;

– масиви значень для наборів параметрів;

– аналізатори, що стежать за застосуванням умовних правил;

– контролери, що приводять у дію визначені функції на основі виконання (невиконання) умовних правил;

– результати абсолютного чи відносного аналізу, призначені для використання як аргументи в інших функціях;

– посилання і зв'язки, що залучають зовнішні чи вилучені елементи (параметри) в якості аргументів побудови даної форми;

– методи, формалізовані явно (придатні для повторного застосування) – «Power Copy»;

– скрипти (програми), що беруть участь в роботі методів і виконуються, як програмний код.

Всі деталі (і геометричні форми, що їх представляють) розрізняються по їхній приналежності до конструктивно-технологічного класу. Ці класи узагальнюють в одну категорію всю безліч деталей, що мають стійкі конструктивні і технологічні ознаки: вид заготовки, спосіб матеріалізації форми, виробниче оснащення і характерні фізичні процеси. Їхнє геометричне визначення, відповідно, може мати свої терміни, методи й аргументи побудови. Наприклад, листова деталь з алюмінієвого сплаву має свою особливу специфікацію, відмінну від, наприклад, механічної деталі чи електрокабеля.

Дане представлення моделі не тільки сприяє використанню інформації про виріб на різних етапах його життєвого циклу, але й дозволяє реалізувати сучасний рівень автоматизації проектування, не обмежений рішенням задач моделювання і креслення, що припускає реалізацію таких можливостей, як паралельне проектування, нагромадження і використання корпоративних знань, автоматичне проведення змін на всіх етапах процесу проектування, різноманітна візуалізація проекту.

Будь-який об'єкт в описі продукту наділений негеометричними характеристиками, як мінімум, наступних категорій:

– *графічні атрибути*, що представляють об'єкт засобами діалогу системи;

– *ідентифікація*, що визначає систему іменування, позначення і представлення продукту в службовій документації;

– *фізичні властивості*, що визначають механічні й геометричні характеристики компонентів виробу: обсяг, площа поверхні, координати центра ваги, орієнтація векторів моментів інерції й інші;

– *технологічні властивості*, що визначають виробничі характеристики компонентів виробу: термообробка, покриття, маркірування, таврування, чистота поверхні, допуски й інші;

– *адміністративні властивості*, що визначають характеристики об'єкта стосовно до процесів його життєвого циклу: статус готовності, ревізія, авторизація, сертифікація й інші;

– *функціональні властивості*, що характеризують цільові параметри виробу: продуктивність, ресурс, питома собівартість експлуатації й інші. Більшість з них мають безпосереднє відношення до економіки промислового бізнесу і контролюються особливо ретельно;

– *спеціальні (нерегулярні) властивості*, проголошені для даного виробу в зв'язку з якимись унікальними його особливостями.

Особливо важливо те, що між різнорідними характеристиками можуть бути виражені відносини різних типів – логічні, алгебраїчні, засновані на масивах значень чи обумовлені сценаріями – скриптами. Ці відносини, що мають вид правил, являють собою форму організації конструкторсько-технологічних знань про виріб.

При аналізі структури 3D моделей, які розглядаються, виникає питання: що дають ці засоби для автоматизації рішення конструкторських і технологічних задач в АСТПВ?

Відзначимо, що важливість представлення і використання знань в задачах АСТПВ розглядалася досить давно. В численних роботах пропонувалося використання знань у вигляді таблиць рішень, правил, семантичних мереж і фреймів для задач проектування оснащення, інструмента і технологічних процесів [1, 2]. Використання декларативних знань забезпечувало гнучкість створюваних систем, їх адаптованість до особливостей предметної області і правилам прийняття проектних рішень. Однак, відсутність на той період засобів створення 3D моделей виробів не дозволяло одержати значимий практичний ефект від виконаних розробок.

З іншого боку, автоматизація конструкторського проектування лише за рахунок побудови 3D моделей і наступного одержання креслень також у багатьох ви-

падках не приносить належного ефекту в силу недостатньо високого рівня автоматизації. Часткове поліпшення дає розробка і використання спеціальних процедурних додатків до CAD-системи (наприклад, конструювання пакета прес-форми з використанням баз нормалізованих деталей); істотно більший ефект може дати інтегроване використання набору процедурних додатків. Однак, цей підхід не може бути реалізований для всіх видів проектних процедур ТПВ, як у силу їхнього великого числа, так і через слабку формалізацію і типізацію багатьох проектних рішень.

Новий метод вирішення задач автоматизації проектування в ТПВ, за рахунок інтегрованого використання 3D моделей і баз знань, здатний привести одночасно і до гнучкості створюваної системи, і до істотного загального підвищення рівня автоматизації. При цьому, за рахунок формалізації і збереження корпоративних знань для підприємства, багато в чому вирішується серйозна проблема недостачі висококваліфікованих конструкторів і технологів [4].

Загальна схема інтегрованого використання 3D моделей і баз знань приведена на рис. 1. Тут під додатком розуміється деяка проектна процедура АСТПВ, реалізована засобами прикладного програмного інтерфейсу (API) CAD-системи, яка вирішує конкретну задачу конструкторського чи технологічного проектування з використанням бази корпоративних знань.

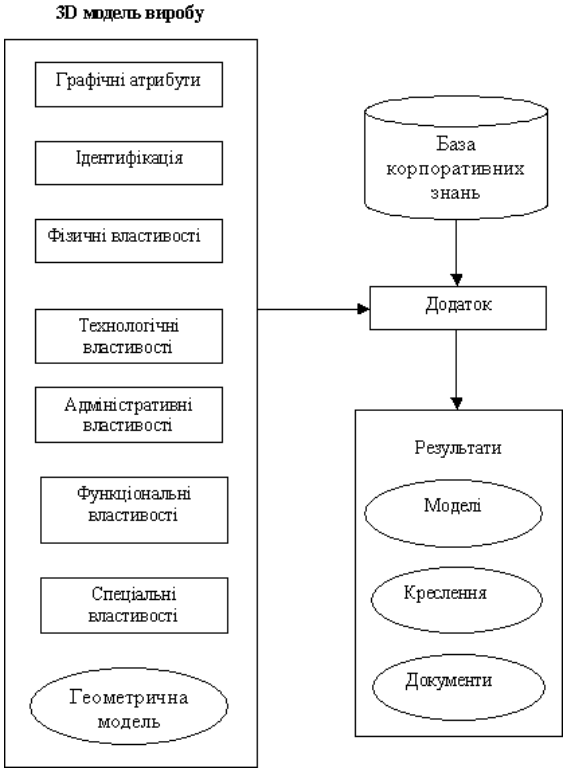


*Рисунок 1 – Схема інтегрованого використання 3D моделі і бази знань*

На приведеній схемі не конкретизовано, чи є 3D модель моделлю основного виробу чи моделлю виробу ТПВ – це залежить від характеру розв'язуваної додатком задачі. Додаток може використовувати у своїй роботі декілька моделей, а також допоміжну ін-формацію – наприклад, геометричні чи технологічні шаблони.

Таким чином, 3D модель виробу фактично є джерелом інформації для вирішення всіх основних задач ТПВ, таких як проектування нестандартного обладнання, оснастки, технологічних процесів, керуючих програм для верстатів з ЧПК та інших. Використання центральної ролі 3D моделі виробу в АСТПВ дозволяє автоматизувати процеси управління ТПВ. Так, автором розроблені проектні процедури і програми для PDM Smar Team [5], що реалізують свою функцію управління 3D моделями в ході конструкторсько – технологічного проектування.

## *ВИСНОВОК*

Застосування нового методу використання та управління 3D моделями дозволяє будувати прикладні САПР, що працюють «від технічного завдання» і генерують всі необхідні геометричні моделі, креслення, технологічні процеси, текстові чи текстово-графічні документи. Реалізація кожної конкретної САПР вимагає значних зусиль, однак в результаті досягаються високий рівень автоматизації проектних рішень і гнучкість системи, а також створюються умови для рішення кадрових проблем у сфері ТПВ.

## *ПЕРЕЛІК ПОСИЛАНЬ*

1. *Норенков И. П., Кузьмик П. К.* Информационная поддержка наукоемких изделий. CALS-технологии. М.: Изд-во МВТУ им. Н. Э. Баумана, 2002. – 320 с.
2. *Евгенев Г. Б.* Системология инженерных заданий. М.: Изд-во МГТУ им. Баумана, 2001. – 376 с.
3. *Очередько С. А.* Глобальная трансформация промышленного бизнеса и новая концепция управления жизненным циклом изделия / Информационные технологии в наукоемком машиностроении. Компьютерное обеспечение индустриального бизнеса. / Под общ. ред. А. Г. Братухина. – Киев: Техника, 2001, с. 626–646.
4. *Павленко П. Н., Яблочников Е. И.* Техническая подготовка производства в едином информационном пространстве. // Оборудование и инструмент для профессионалов, № 4 (51), 2004. – С. 30–35.
5. *Павленко П. Н., Дмитриев Н. М.* Современные формы технической подготовки производства. // Оборудование инструмент для профессионалов. – № 6(52). – 2004. – 62 с.

Надійшла 14.06.04
Після доробки 29.03.05

*Рассмотрены возможности моделирования в современных CAD системах. Представлен метод управления 3D моделями в интегрированных АСТПП. Приведены рекомендации по практическому использованию 3D моделей.*

*The opportunities of modeling in modern CAD systems are considered. The method of management by 3D models in integrated ASTPM is submitted. The recommendations are given for practical use of 3D models.*