未踏を歩く

スーパークリエイターはどこにいる

2

未踏ソフトウェア創造事業
紀PMグループ
http://www.ipa.go.jp/NBP/15nendo/15mito/

本連載では，未踏ソフトウェア創造事業に採択された開発者の皆さんに，プロジェクトの内容を紹介していただきます．今回は紀PMのグループです．

放送型配信における鍵漏洩抑止スキームの拡張

筆者は，放送型配信における不正利用を抑止するための暗号化鍵配信システムを開発しています．この鍵の特徴は，暗号化する鍵1つに対し，解読する鍵を必要に応じて多数作ることが可能な点にあります（図1）．マンションの共同玄関や企業のセキュリティルームのドアに使われている錠前と似ていますが，本方式は鍵を10^{18}個ほど作ることができます．

対象となる放送型配信は，映画や音楽などのコンテンツをデジタル形式で，皆に同時に送り届けるものです．ポイントは，通常のテレビやラジオと違い，デジタルであること，通常のストリーミング配信と違い，皆に同時に，ということです．BS/CS放送も条件にあてはまりますが，IPマルチキャストによる放送（たとえばインターネットラジオ）もおもなターゲットであると考えています．

鍵の実装には，有限体上の楕円曲線上のペアリングと呼ばれる演算を用います．2002年度はこれまでの世界最速のものに比べ約3割高速なものを実装しました．本年度はこの方式の理論的な弱点，不足していた機能および外部インターフェースの補強，ハードウェア上の実装を行う予定です．

【渡辺秀行，光成滋生，石田計，高島研也】

Javaによる分散協調制約解消システム

制約解消システムとは，簡単に言うと「ユーザは解決したい問題を制約の形（連立不等式など変数の間の関係を表す算術式や論理式）で記述するだけで，あとは制約ソルバがその制約を満たす解を求めてくれる」という便利なもので，生産スケジューリング，資源割り当てなどの問題解決に利用されています．

このプロジェクトの目的は，分散コンピューティング環境において，複数の制約ソルバを協調的／競争的に並行動作させることにより，単一のアルゴリズムをチューニングする以上の効果を得ることです．開発中のHECSシステム（http://kaminari.istc.kobe-u.ac.jp/hecs/）では，現在のところ整数制約ソルバ，ブール値制約ソルバ，実数制約ソルバが利用できます．

具体的な目標は3つあって，①「解の交換，CPU資源の割り当て，ソルバの選択／切り替え」機能を持つ賢いリアルタイムスケジューラの開発，②比較的大きな計算機リソース（Sun Enterprise 5000，Beowulf PCクラスタなど）を利用したシステムの適用実験，③より多く人に使ってもらえるように，OpenOffice Calcのアドインとして利用可能にすることです．これらを実現してHECSシステムを完成し，その有用性を示したいと考えています．

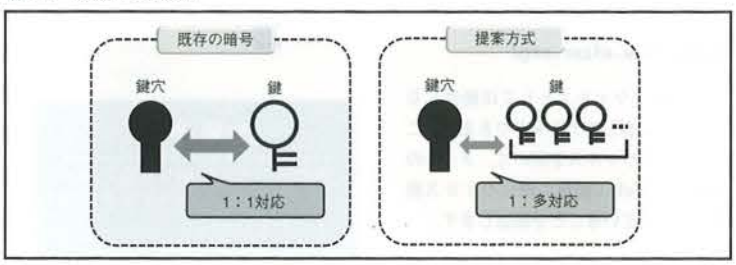
【番原睦則，田村直之，井上克巳，川村尚生，玉置久】

自然な訳文を生成する翻訳システムの開発

2002年度から継続しているこのプロジェクトの第一の目的は，翻訳者が出したい訳を生成できる枠組みを探求し，それをできる限りソフトウェアとして実現することです．プロジェクトリーダーの武舎は，20年前から，英→日，英→韓，英→中などの翻訳ソフトウェアの開発を行い，また自ら20冊を超える翻訳書や著書を出版しています．さらに，翻訳者養成用通信教育のテキスト執筆も経験しています．今年から加わった河村も，プログラム開発の傍ら，書籍や雑誌記事などの翻訳を行ってきました．

現在の翻訳ソフトウェアは「高速辞書引きソフトウェア」として利用すれば，それなりに役に立ちます．たとえば，長い専門用語でも登録さえすれば正しく「翻訳」してくれます．改めて調べなくて済みますし，

●図1　多数の鍵に対応



入力の手間も省けます．しかし，単語のレベルを超えて文全体を見た場合，原文の構文が透けて見えるような「直訳」しか出してくれません．直訳ではない，頭にすっと入ってくる読みやすい訳文を生成するにはどのようなしくみが必要なのか．それを自らの翻訳過程を参考にして，探求し，プログラムとして表現します．もちろん，プロの翻訳者並みの翻訳はできないのですが，それに近づくことによって，この技術の応用分野が広がっていくのです．

詳細は http://www.musha.com/ をご覧ください．

【武舎広幸，河村政雄】

レジームスイッチング資産運用法を実装した基本システムの開発

現在，銀行にお金を預けていても，お金が増えることはほとんどありません．また，年金基金や保険会社も，株価低迷やゼロ金利政策で当てにならない状況にあります．そのため，あなたが豊かな老後を送るためには，自分で資産を効率的に運用するしかないのです．

資産運用を行うにあたっては，近年，難解な数式を駆使する金融工学という理論が盛んに用いられるようになってきていますが，金融工学と言うと，デリバティブズなどのイメージのためか，ギャンブル性の強いものだと思われるかもしれません．

しかし，金融工学とはリスクを的確に把握しながら，収益をコントロールするためのツールです．そして，この金融工学の理論をWeb上のシステムとして実装することにより，誰でも簡単に金融工学を用いた資産運用を行うことが可能になります．

とくに，本システム（Regitz）の特徴は，景気の状態（レジーム）を把握するアルゴリズムを実装している点です．景気が良い状態なのか，悪い状態なのか，その経済シナリオ＝レジームをあらかじめ知る，つまり，将来の景気予報を行うことが可能です．そのうえで価格モデルを切り替え，ポートフォリオを最適化する，つまり，どの資産をどれだけ持っていれば，リスクを抑えながら収益をどれくらいあげられるか，について事前に知ることができます．

このシステムの登場により，皆さんの資産運用がうまくいくことを願っています．

【石島博，谷山智彦】

ポートフォリオ運用のための相関構造解析可視化ツール

金融分野は莫大なシステム投資をしており，銀行をはじめとする金融機関はIT産業の優良な顧客です．ところが，ほとんどの人は金融機関のシステムが重要であることは認識しているものの，コンピュータの最先端技術を金融機関が必要としているとは考えていません．これは，金融機関がコンピュータをおもにお金や顧客の管理業務（バックオフィス業務と呼ぶ）に対して活用しているためです．それでは，金融機関はコンピュータ技術をバックオフィス業務だけに活用すれば良いのでしょうか？ その答えが現在の金融技術の日米格差に現れています．

'80年代，米国の金融機関はNASAのエンジニアを積極的に登用し，当時の最先端技術を金融業務（とくに金融派生商品などの分析）に適用しました．これは米国が金融不況に喘いでいる最中の未踏領域へのチャレンジでした．それが金融工学という実務に則した新技術として開花し，今日に至っています．

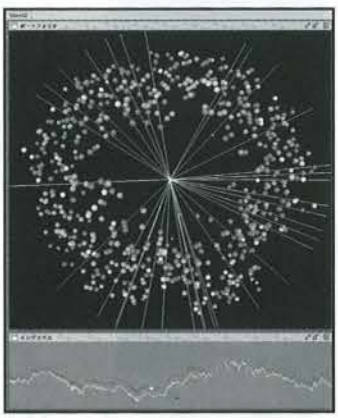
我々は，当時に比べて圧倒的なコンピュータパワーを獲得しています．そして日本には製造業で培った世界レベルの工学技術があります．その工学技術を金融分野に実践することが我々のチャレンジです．

具体的には，複数の株式を保有（ポートフォリオと呼ぶ）した場合に考えるべきリスクや期待される収益を直感的に示すGUI（図2）の開発，および固有値解析をベースとした効率的なリスク管理を行うための基礎エンジンの開発をターゲットとしています．

本プロジェクトの情報は，http://www.cmdr.co.jp/で参照できます．

【尹熙元，藤原義久，相馬亘】

●図2　リスクや収益の表示



COLUMN

未踏って何？

未踏ソフトウェア創造事業は，情報処理振興事業協会（IPA）が行う，独創的なソフトウェア開発者の支援活動です．法人でなくても，個人またはグループで応募することができます．とくに資格は必要ありません．アイディアと開発力があれば採択される可能性があります．

採択を決めるのはIPAではなく，IPAに任命されたプロジェクトマネージャ（PM）です．IPAがPMに口を挟むことはなく，すべてPMの裁量で決まります．いろいろなPMがいますから，好みのPMを選んで応募することができます．採択後のアドバイスもPMが行います．IPAの事業なのだからいろいろうるさく言われるのでは，といった心配は無用です．場合によっては，IPA以上に厳しいPMもいるかもしれませんが…．

開発費はもらえます．融資ではありません．開発費はプロジェクトの内容によって異なってくるので一概には言えませんが，贅沢をしなければ開発期間中は開発に集中することができるはずです．

開発費がもらえるだけではなく，成果は開発者のものになります．成果を元に事業を起こしても良し，オープンソースとして公開し，たくさんの人に使ってもらってもOKです．

2003年度の採択者の平均年齢は30.8歳です！ぜひあなたも思い切って応募してみてください．