

工学院情報通信系
試験科目群「通信情報工学」
各教員の研究内容の紹介

平成27年5月



教授 植松 友彦

研究分野：情報理論, 符号理論, 系列の複雑度
キーワード：データ圧縮, 誤り訂正符号, ユニバーサル符号
ホームページ：<http://www.it.ce.titech.ac.jp/>

1 研究内容と目指すもの

- (1) 情報源の統計的性質によらないユニバーサルデータ圧縮法の研究と開発
- (2) 相関を有する複数の情報源のネットワークに対する効率的な符号化法の研究
- (3) 乱数の生成法と共有法の開発

2 関連する最近の研究テーマ

系列の複雑度の尺度の相互関係について

情報理論においては、系列に対する様々な複雑度の尺度が存在する。これらの複雑度の研究は、理論的な興味のみならず、ユニバーサル情報源符号化、仮説検定問題、予測問題と関連して多くの応用を有していることが知られている。特に、次に挙げる4種の複雑度の尺度は、可変長情報源符号化問題において重要な役割を果たして居る。(i) オーバーラップのある経験エントロピー、(ii) オーバーラップのない経験エントロピー、(iii) マルコフ情報源に関する自己エントロピー、(iv) 系列を相異なる部分列に分解したときの部分列の最大個数。本研究では、可算無限アルファベット上の系列に対して、これらの複雑度の関係について調べ、2つの経験エントロピーとマルコフ情報源に関する自己エントロピーは常に一致し、これらの尺度は、相異なる部分列の最大個数によって下から抑えられることを明らかにしている。更に、これらの尺度と無歪み情報源符号化定理との関係についても調べている。

対称通信路に対するユニバーサルなアフィン符号

1977年にCsiszar, KornerとMartonは、離散無記憶通信路に対してユニバーサル通信路符号化定理を初めて示した。ユニバーサル通信路符号化定理によると、通信路の遷移確率に依存しない符号器と復号器が存在して、かつ、伝送速度が通信路容量よりも真に小さければ、符号長を無限に長くしたとき、復号誤り率が零に近づくという性質を有する。しかしながら、ユニバーサル符号の存在はランダム符号化法を用いて示されていたので、符号器には何ら代数的な構造は課せられていなかった。本研究では、アフィン符号として知られる代数的な構造を有する符号器と最大相互情報量(MMI)復号法と組み合わせたユニバーサル通信路符号を対称通信路に用いた際の復号誤り率の評価を行い、この組合せのユニバーサル通信路符号によって、通信路の遷移確率を符号器ならびに復号器が予め知ることなく、Gallagerの信頼性関数を達成できることを明らかにしている。

情報源ネットワークにおける漸近的にフィードバック零のユニバーサル符号化アルゴリズム

情報源 X を符号化して送信することを考えよう。受信者は情報源 Y を有し、 Y は X と相関があるものとし、 Y は受信者しか参照できない副情報とする。従来の副情報を用いた情報源符号化問題では、送信者と受信者の間の通信路は一方向であると仮定されていた。このことと、送信者が副情報 Y にアクセスできないということから、符号化に先立って符号器は達成可能レートを決めなければならなかった。本研究では、送受信者間の通信路は双方向かつ非対称の伝送速度を有するとし、受信者から送信者へのフィードバックを利用したユニバーサル情報源符号化について検討している。そして、符号器と復号器が情報源 (X, Y) とは独立の乱数を共有しているときに、文字列一致に基づいたプログレッシブな可変長ブロック符号化アルゴリズムと同時典型性を用いた復号法を提案している。提案したプログレッシブな符号器は、符号化を開始する際、達成可能レートを知る必要は無いという特徴を有する。更に、提案したアルゴリズムの解析を行い、ある種のミキシング条件を満足する任意の情報源 (X, Y) について、平均圧縮率は条件付きエントロピーレート $H(X|Y)$ に漸近し、かつフィードバックレートは0に漸近することを明らかにしている。

一般化された相補的分配ネットワークにおけるユニバーサル情報源符号化

相関を有する情報源に関する符号化問題は、1972年にSlepianとWolfによって初めて研究された。彼らの研究以降、相関を有する情報源に関する様々な符号化問題が検討されるようになった。このうち、一般化された相補的分配ネットワークと呼ばれる多端子情報源符号化ネットワークは、図1と2に示されるようなシナリオを取り扱っている。すなわち、幾つかの地上局が離れた場所に設置されており、各々の地上局が、自らのセンサや端末によってデータを収集すると共に、他の地上局の収集したデータを共有するという問題を考える。データの共有を達成するために、各々の地上局は収集したデータを衛星に伝送する。そして、衛星は受信した全てのデータを地上局に放送する。各々の地上局は、自分で収集したデータを副情報として用いて、他の地上局のデータ全てを復元する。本研究では、複数の情報源と複数の送り手から成る一般化された相補的分配ネットワークに対して、情報源の確率分布を知らなくても符号化・復号化が行えるユニバーサル情報源符号化法を提案している。具体的には、まずグラフ理論的な解析に基づいて固定長-固定長(FF)ユニバーサル符号の具体的な構成法を提案している。次に、復号誤り確率と正しく復号される確率の限界を明らかにしている。更に、提案したFF符号化法は、固定長-可変長(FV)ユニバーサル符号の構成にも応用することができ、オーバーフロー確率やアンダーフロー確率が、それぞれ復号誤り確率と正しく復号される確率と同様にして評価できることを示している。

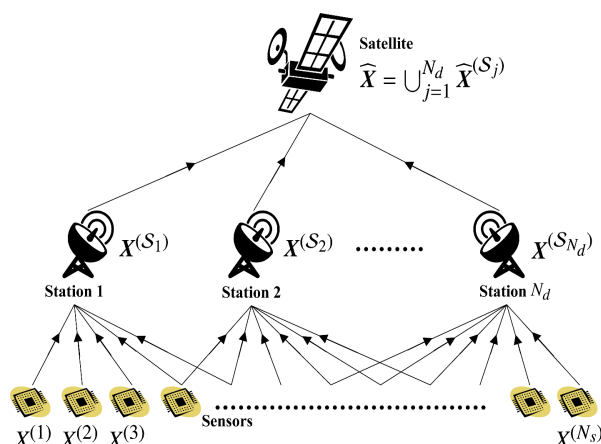


図1 データの収集: 物理的に離れた場所にある各々の地上局はデータを収集し、収集したデータを衛星に伝送する。

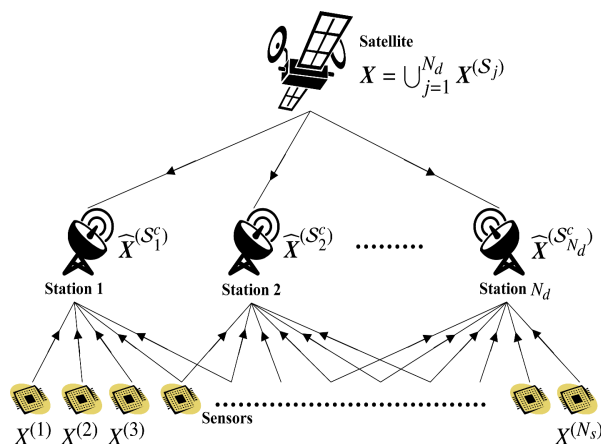


図2 データの分配: 衛星は地上局から送られたデータを符号化して、地上局での共有のために放送する。各々の地上局は、既に所有している自分のデータを副情報として、衛星から送られた符号化データから他の地上局のデータの復元を行う。

3 関連する業績、プロジェクトなど

論文 :S. Kuzuoka and T. Uyematsu, "Relationship among complexities of individual sequences over countable alphabet," IEICE Trans. Fund. vol.E89-A, no.7, pp.2047-2055, July 2006.

T. Uyematsu, "A universal affine code for symmetric channels," Proc. The 31st Symposium on Information Theory and its Applications (SITA2008), pp.89-94, Oct. 2008.

E.-h. Yang, D.-k. He, T. Uyematsu, and R. W. Yeung, "Universal source coding algorithms for source networks with asymptotically zero feedback," IEEE Trans. Inform. Theory, vol.54, no.12, pp.5575-5590, Dec. 2008.

A.Kimura, T. Uyematsu, S. Kuzuoka, and S. Watanabe, "Universal source coding over generalized complementary delivery networks," IEEE Trans. Inform. Theory, vol.55, no.3, pp.1360-1373, March 2009 .

著書:代数系と符号理論, オーム社 (2010)

受賞: 電子情報通信学会論文賞 (1993, 1996, 2002, 2007), 電子情報通信学会業績賞(2008)



教授 尾形 わかは

研究分野：暗号理論, 情報セキュリティ
キーワード：暗号プロトコル, 秘密分散共有法, 検索可能暗号, 証明可能安全性
ホームページ：http://www.security.mot.titech.ac.jp/

1 研究内容を目指すもの

情報化社会においては、情報を秘匿するための暗号、通信相手を確認するためのエンティティ認証、伝送される情報の完全性を保証するためのメッセージ認証が不可欠であり、すでにインターネットや携帯電話において情報やユーザの安全性を守るために、これらの技術が利用されています。このような暗号技術は、単に情報を暗号化したり、相手を認証するだけでなく、様々な機能の実現に応用することができ、一見、実現不可能であると思えることも可能となります。当研究室では、より高い安全性と利便性を持ったサービスを実現するためには、どのように暗号技術が利用可能であるのか、また、どのような弊害が起こり得るのか、それを解明する研究を行っています。

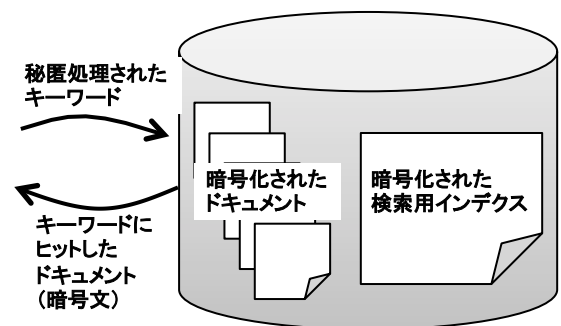
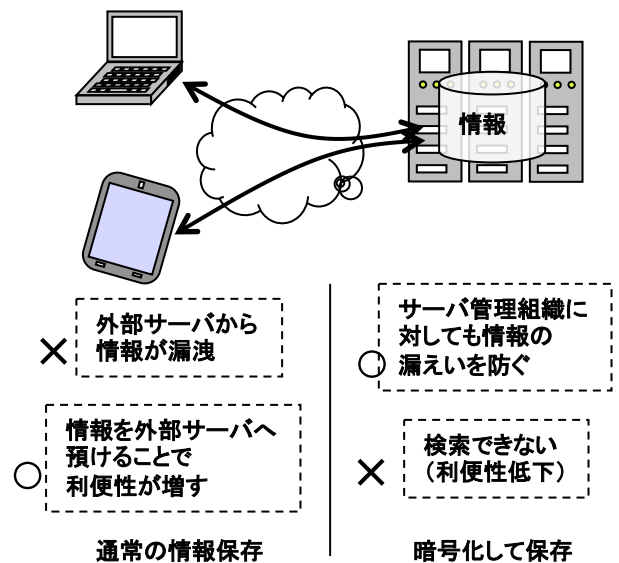
2 関連する最近の研究テーマ

検索可能暗号方式の構築と評価

近年では、個人や企業が大量の情報を外部サーバに預けて保管し、またその情報の処理（検索や加工など）も外部の計算資源を利用して行うことが主流となりつつある。しかし、外部サーバに情報を保存することにより、情報漏洩のリスクが高まる。特に、組織における機密情報や、個人のプライバシー情報を外部に出す場合は、サーバ管理者への漏洩リスクも考慮する必要がある。このような漏えいリスクは、情報の暗号化によって軽減することが可能であるが、通常の暗号方式によって暗号化された情報は、情報の検索や加工などの処理が不可能となり、利便性が大幅に低下してしまう。このような問題を解決するものの一つとして、情報の検索が可能であるように暗号化する仕組みである検索可能暗号がある。

検索可能暗号の研究においては、安全性と効率のバランスが重要である。最高の安全性は「暗号化された情報や、検索ワードについての情報が一切漏えいしない」ことであり、最高の効率も「検索処理に要する通信量や処理量は、暗号化処理が施されていない場合とほぼ同じである」ことである。このような最高の安全性と効率を兼ね備えた方式が作れるとしたら、いつでもこの方式を利用すれば良い。しかし残念ながら、原理的に、このような方式を構築することは不可能である。そこで、多少の安全性を犠牲にすることで、効率を上げる研究が行われている。我々の研究室では、安全性を段階的に定義し、これを元に既存の検索可能暗号方式の安全性レベルを評価している。また、各安全性レベルが保証される具体的な方式の構築を行っている。これによって、扱う情報の機密度合いと、必要とされる効率性に応じて、利用者が方式を選択可能となる。

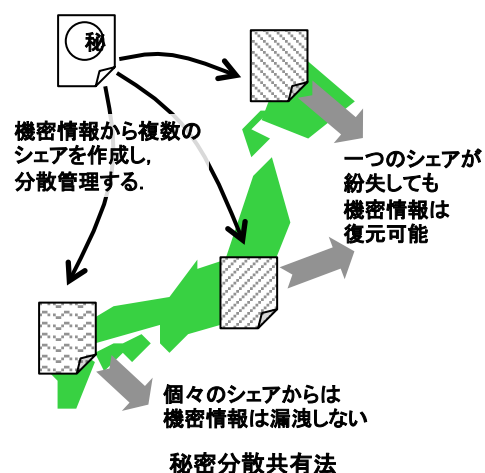
また、これまでの研究では情報の追加をあまり考慮していなかった。実際の利用を考えた場合、保管する情報は絶えず変更・追加される可能性があるため、これらが効率的かつ安全に行えることが必要である。現在、我々の研究室では、情報の追加に着目し、安全性定義の拡張や、方式の提案・評価を行っている。これに加えて、変更や削除も効率的に可能な検索可能暗号方式の構築が、今後の課題である。



検索可能暗号方式

秘密分散共有法

情報の紛失に備えるための一般的な方法は、幾つかのコピーを保存しておくこと(バックアップ)である。しかし、コピーの数を増やすほど、情報漏えいのリスクは大きくなる。秘密分散共有法とは、情報の紛失と漏えいを同時に防ぐことのできる暗号技術である。典型的な秘密分散共有法である「しきい値法」では、秘密情報から幾つかの補助的な情報(=シェア)が次の2つの性質を満たすように作成される。(a) あらかじめ定められた数(しきい値)のシェアからは元の秘密情報を復元できる、(b) しきい値未満のシェアからは元の秘密情報については何もわからない。たとえば、(2,3)しきい値法を用いた場合、秘密情報から3つのシェアが作成され、3つのうちの任意の2つのシェアを組み合わせることで元の秘密情報を復元することができ、一方で個々のシェアからは元の秘密情報については何の情報も得ることもできない。我々の研究室では、秘密分散共有法の安全性機能の補強に関する研究と、効率向上の研究を行っている。



秘密分散共有法の安全性機能の補強

通常の秘密分散共有法では、シェアが改竄されたとしても、これを検知することができない。そのため、各シェアに検証情報を付加することでシェアの改竄を検知する方法が研究されている。我々の研究室では、無限の計算能力を持つ不正者を前提とし、付加する検証情報の大きさの理論限界を導出すること、理論限界とほぼ同じ長さの検証情報の計算方法を提案することなどを行ってきた。最近の成果としては、ビット列を対象とした検証情報の計算方法の提案がある。



また、非同期通信路を用いて秘密を復元しようとした際に、シェアの後出しや持ち逃げが可能となる問題点に対し、解決策を提案することも行っている。

秘密分散共有法の効率化

無限の計算能力を持つ不正者を前提とした場合、分散の効率化には限界があることが知られている。例えば、1GBのデータベースを分散管理する場合には、個々のシェアも1GBのサイズが必要である。3つのシェアを作成した場合にはトータルの必要なストレージ容量は3倍になってしまう。そこで、大きな情報・多数の情報を分散管理するために、計算量理論的な仮定(たとえば、巨大な合成数を素因数分解することは事実上不可能であること)を前提とした方式が提案されている。これらの方式は、暗号方式の構築で用いられる技術を組み合わせることによって成り立っているが、効率の面や安全性の面で問題点を抱える方式も多い。我々の研究室では、計算量理論的な仮定を用いた場合の安全性の定義を厳密に行い、その元で安全性が証明可能な方式の提案をおこなった。

3 関連する業績、プロジェクトなど

論文：

- Wakaha Ogata, Hiroshi Eguchi, "Cheating Detectable Threshold Scheme against Most Powerful Cheaters for Long Secrets," Designs, Codes and Cryptography, Vol.71, No.3, pp.527-539 (2014)
- Wakaha Ogata, Keita Koiwa, Akira Kanaoka, Shin'ichiro Matsuo, "Toward Practical Searchable Symmetric Encryption," Advances in Information and Computer Security, the 8th International Workshop on Security, IWSEC 2013, LNCS Vol.8231, pp.151--167 (2013.11)
- Toshinori Araki, Wakaha Ogata, "A Simple and Efficient Secret Sharing Scheme Secure against Cheating," IEICE Trans. on Fundamentals, Vol.E94-A, No.6 pp.1338--1345 (2011.6)
- Tatsumi Oba, Wakaha Ogata, "Provably Secure On-line Secret Sharing Scheme," IEICE Trans. on Fundamentals, Vol. E94-A, No.1, pp.139--149 (2011.1)

著書：暗号理論の基礎数理，コロナ社（2004）



准教授 笠井 健太

研究分野：符号理論

キーワード：LDPC符号, 多元LDPC符号, 空間結合符号

ホームページ：<http://www.comm.ce.titech.ac.jp/>

1 研究内容を目指すもの

符号理論の目的は、通信路符号化定理などの情報理論が与える情報通信に関する主要な結果を現実的な方法によって実現することです。符号理論は情報通信産業に直接貢献する誤り訂正技術を扱っているので、シンプルで抽象的な問題だけではなく、現実の情報通信産業が直面している複雑な問題に対して実現可能な解決法を与えることが望まれています。一方で、符号理論は情報通信に関する多くの応用問題の基礎をなすために、他の通信工学の分野に比べてより厳密な証明が求められます。符号理論は、工学的重要性和理論体系の美しさによって多くの研究者の魅了し、多くの他分野に影響のある学問分野を形成しています。本研究室では推論に基づく誤り訂正技術を使って、情報通信システムの問題解決に取り組んでいます。

2 関連する最近の研究テーマ

噴水符号：インターネットのパケット通信に適した誤り訂正

インターネットでは、情報はパケットと呼ばれる単位にまとめられて送られます。ネットワーク機器の性能の不足などで、パケットはしばしば消失してしまうことがあります。この時にどのような問題が考えられるでしょうか。例えば、1ギガバイトのファイルを100万個のパケットに分割してサーバから数百万人のユーザに送りたい状況を考えてみましょう。1番目から順に100万番目までのパケットを単純に送るような方法では、1つでもパケットが消失してしまうだけで、サーバに再送要求をしなければならず、サーバでは数百万人分の再送要求を受け付けることになり、現実的ではありません。従来のブロック誤り訂正符号では、ある決められた符号化率で符号化するために、上記の問題を解決することができませんでした。

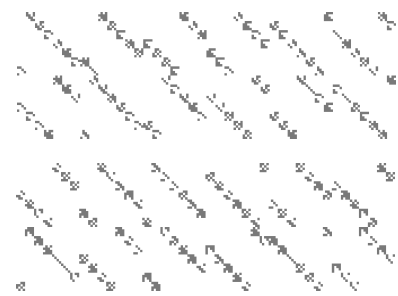
ファイルを非常に小さい符号化率でファイルをパケット列に符号化しブロードキャストする事によってこの問題を解決することができます。この符号化法は、パケットを水滴に例え、噴水(fountain)符号と呼ばれています。受信者は、無限に送られてくるパケット列の中から数パーセントだけ余分に任意のパケットを受信することで、サーバに再送を要求することなしにファイルを完全に受信することができます。本研究室で開発された乗法繰り返し多元LDPC符号を用いた噴水符号は、小さなサイズのファイルに対して世界で最もオーバーヘッドの少ない噴水符号を実現しています。



噴水符号を用いると、サーバでは再送要求に応える必要がなく、多くのユーザそれぞれに対して最適な誤り訂正を実現することができます。受信者はサーバから送信される任意のパケットをファイルサイズより数パーセント多く受信することにより、ファイルを手に入れることができます。

量子誤り訂正符号

量子コンピュータおよび量子通信を実現することにより、従来のコンピュータや通信の枠組みでは実現が困難だと考えられている複雑な計算や安全な通信が実現できます。量子状態は劣化したりノイズの影響で変化することがあるので、量子コンピュータや量子通信を安定的に運用するためには、効率的に復号可能な量子誤り訂正符号が必要となります。本研究室では、**現在世界で最も誤り復号性能が優れた量子誤り訂正符号を開発することに成功しています。**



本研究室で開発された量子誤り訂正符号を定義する2つのパリティ検査行列を表しています。黒が1、白が0を表しています。上の行列のどの行も、下の行列のすべての行と偶数個の共通する位置に1を有するように設計することで、多くの誤りを訂正できるように設計されています。

空間結合符号

事後確率を最大にするシンボルを推定することにより、シンボル復号誤り率を最小にすることができます。しかしこの最大事後確率復号法は、理論上理想的な復号法なのですが、計算量が大きく実現することができません。空間結合符号はこの最大事後確率復号と同じ復号性能を、確率推論に基づく低計算量の復号法により実現することができます。本研究室では、この空間結合符号を通信の様々な問題に適用し理論限界に迫る結果を引き出すことに成功しています。



空間結合符号は次のようなドミノ倒しの話に例えられます。解くべき難しい問題を1列に並べ、隣の問題が解けると次の問題が簡単に解けるように隣同士を結合します。そして、端に簡単に解ける問題を用意しておくことで、ドミノ倒しの様に端から順にすべての問題が解けてしまうという寸法です。

3 関連する業績、プロジェクトなど

論文

- T. Nozaki, K. Kasai and K. Sakaniwa, “Analytical Solution of Covariance Evolution for Irregular LDPC Codes,” IEEE Trans. on Information Theory, accepted, 2012.
- K. Kasai, D. Declercq and K. Sakaniwa, “Fountain Coding via Multiplicatively Repeated Non-Binary LDPC Codes,” IEEE Trans. on Communications, accepted, 2012.
- K. Kasai, M. Hagiwara, H. Imai and K. Sakaniwa, “Quantum Error Correction beyond the Bounded Distance Decoding Limit,” IEEE Trans. on Information Theory, vol. 58, no. 2, pp. 1223–1230, Feb. 2012.
- K. Kasai, D. Declercq, C. Poulliat and K. Sakaniwa, “Multiplicatively Repeated Non-Binary LDPC Codes,” IEEE Trans. on Information Theory, vol. 57, no. 10, pp. 6788–6795, Oct. 2011.

講演（招待）

- K. Kasai, “The Many Applications of Spatially-Coupled Codes,” IEEE Information Theory Workshop, Paraty, Brazil, Oct. 16–20, 2011.

受賞

- エリクソン・ヤングサイエンティストアワード2010



教授 府川 和彦

研究分野：移動通信, デジタル信号処理, 適応フィルタ, 無線ネットワーク
 キーワード：MIMO, OFDM, 適応等化器, 適応干渉キャンセラ, パケット伝送
 ホームページ：http://www.radio.ce.titech.ac.jp

1 研究内容と目指すもの

- (1) 移動無線における大容量伝送技術の研究
- (2) 移動無線における高信頼伝送技術の研究
- (3) 適応パケット伝送技術の研究

2 関連する最近の研究テーマ

MIMOの最小ビット誤り率規範プリコーディング

MIMO (Multiple Input Multiple Output) とは、図1の上部に示すように、複数の送受信アンテナを用いて信号を空間多重する無線伝送方式で、周波数帯域を広げずに高速伝送が可能となる。

MIMOの伝送特性を改善する送信技術として、送信プリコーディングがある。これは、図1の下部に示すように、送信信号に線形処理を施すもので、その重み付け係数は伝送路に依存する。

当研究室で提案したプリコーディングは、受信機において最尤検出を前提とし、受信レプリカ信号間のユークリッド距離を広げて、最尤検出のビット誤り率を最小にするように、上記の重み付け係数を制御する。具体的には、ペアワイズ誤りに基づくビット誤り率の上限を最小化するように制御する。

さらに、受信側で同一チャネル干渉を受け、この干渉を線形アレー合成で抑圧した後、最尤検出する場合について考察し、ペアワイズ誤りに基づくビット誤り率の上限を最小化するように、プリコーディングの重み付け係数を制御するアルゴリズムを考案した。

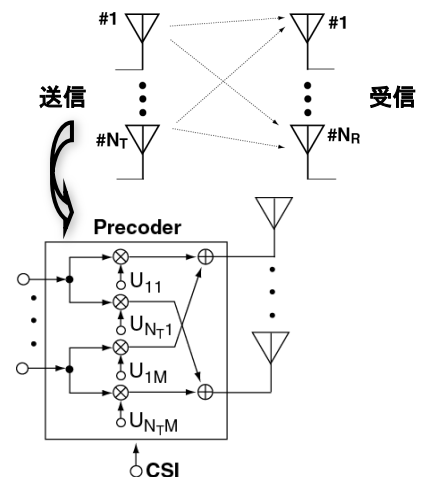


図1 MIMOと送信プリコーディング

MIMOの低演算量・信号検出アルゴリズム

MIMOの最適受信方式として最尤検出が知られているが、その演算量は送信アンテナ数や変調多値数に関して指数関数的に増大し、回路規模が膨大になるという問題がある。一方、演算量がアンテナ数のほぼ2乗に比例する線形受信方式では、雑音強調による平均ビット誤り率特性の劣化が生じる。これらの問題に対し、図2に示すような1次元探索アルゴリズムを提案した。詳しく述べる、線形受信の結果を初期値とし、これを雑音強調の方向に移動させ、それらの硬判定により得られた複数の送信信号候補の中で最も尤度の大きい候補を選ぶことによりビット誤り率を改善し、最尤検出より演算量を大幅に削減できる。

さらに、このアルゴリズムを拡張し、符号化MIMO移動通信において、符号化されたビット系列の復号に不可欠な対数尤度比(LLR)を効率よく求めるアルゴリズムを提案した。近似的なLLRの計算では、符号化されたビットが1か0の条件の下に、対数尤度関数を最大にする送信信号候補の対を求める必要がある。従来の計算法とは異なり、これらの送信信号候補を一括で探索する方法を提案した。具体的には、線形受信の結果を基点として線形受信の雑音強調の方向に探索を行う。冪乗法により、受信信号の自己相関行列の逆行列について、その固有ベクトルを雑音強調の方向ベクトルとして複数求める。次に、各固有ベクトルの方向に1次元探索と硬判定を行い、上記の送信信号候補の対を対数尤度関数に基づき確定する。

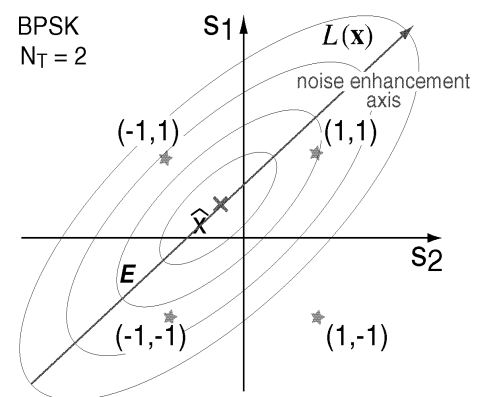


図2 雑音強調の方向への1次元探索

同一チャネル干渉環境におけるMIMO-OFDM最尤受信方式

同一チャネル干渉環境におけるMIMO-OFDM (Orthogonal Frequency Division Multiplexing) の受信方式として、最尤推定に基づく新しい受信機構成を提案した。提案方式の構成を図3に示す。複数のブランチ・メトリック生成器と、メトリックを基に信号判定を行う最尤検出器から構成される。ブランチ・メトリック生成器は、各アンテナの受信信号を白色化フィルタでフィルタリングして合成することにより同一チャネル干渉抑圧を行い、この合成信号からレプリカ信号を減算し2乗することでメトリックを生成する。白色化フィルタのフィルタ係数およびレプリカ信号の生成に必要なインパルス応答の推定は、受信信号並びに既知の送信信号の自己相関行列を固有展開することで行う。次に、演算量削減を図るため、ブランチ・メトリック生成器を1つに減らしパラメータ推定をRLSアルゴリズムで行う簡略化構成を検討した。計算機シミュレーションを行い、従来の干渉抑圧を行わない最尤受信に比べ、本提案方式は同一チャネル干渉によるBER特性の劣化を大幅に改善できることを明らかにした。

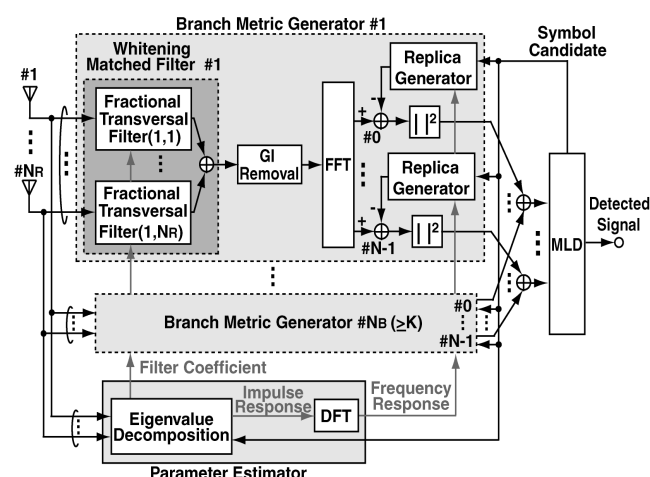


図3 同一チャネル干渉環境におけるMIMO-OFDM最尤受信

マルチユーザ検出とメトリック合成によるARQを用いた移動通信用パケットOFDM伝送方式

OFDM 移動通信用パケット伝送のスループット向上を図るため、パケット衝突時の非線形マルチユーザ検出と、メトリック合成を行うARQを採用したパケット再送方式を提案した。本方式では、まず、パケットの先頭に配置したユーザIDを検出することにより衝突したパケットのユーザを特定し、各衝突パケットをマルチユーザ検出により抽出する。さらに、CRCによりパケット誤りが検出されたときは、図4に示すように、同一パケットが再度衝突するよう再送させ、メトリックを合成することによりARQ再送回数の低減を図る。スループット特性を明らかにするため計算機シミュレーションを行い、従来方式(MUD, NDMA)に比べて2倍以上スループット特性を向上できることを明らかにした。

このパケット再送方式は、パケットが衝突し、誤りが検出されると再度衝突するよう制御するため、プロトコルが複雑になるという欠点がある。再衝突を不要とするため、メトリックを合成するのではなく、ビット対数尤度比を合成するように変更を加えた。これにより、プロトコルが簡単になり、かつパケット再衝突による不要な再送を避けることができ、スループット特性の更なる向上を計算機シミュレーションにより明らかにした。

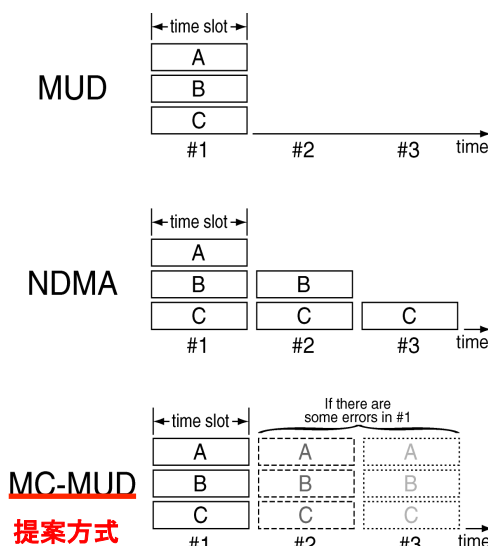


図4 提案と従来のパケット再送方式

3 関連する業績、プロジェクトなど

- 論文: F. Lisheng, K. Fukawa, H. Suzuki, and S. Suyama, "MAP receiver with spatial filters for suppressing cochannel interference in MIMO-OFDM mobile communications," *IEICE Trans. on Communi.*, vol. E92-B, no. 5, pp. 1841-1851, May 2009.
- B. Pitakdumrongkija, K. Fukawa, S. Suyama, H. Suzuki, and A. Umi, "Precoding technique for minimizing BER of MIMO-OFDM system employing MLD under multicell co-channel interference," *IEICE Trans. Commun.*, vol. E92-B, no. 5, pp. 1573-1581, May 2009.
- B. Pitakdumrongkija, K. Fukawa, H. Suzuki, "MIMO-OFDM precoding technique for minimizing BER upper bound of MLD under imperfect CSI," *IEICE Trans. on Communi.*, vol. E91-B, no. 5, pp. 1490-1501, May 2008.
- 著書: デジタル信号処理, 培風館, 2009年.
- 受賞: 電子情報通信学会論文賞 (1995, 2007, 2009), European Wireless Technology Conf. Best Paper Award (2009), 電子情報通信学会業績賞(2009)
- 総務省プロジェクト: ミリ波関連(2007-2011), セルラー高速伝送関連(2009-2012)
- 企業との共同研究: MIMOマルチユーザ検出に関するもの4件



准教授 松本 隆太郎

研究分野：誤り訂正符号, 量子情報理論, ネットワーク符号化, 無線通信
キーワード：量子暗号, 情報理論的セキュリティ, ネットワーク符号化
ホームページ： <http://www.it.ce.titech.ac.jp/>

1 研究内容と目指すもの

- (1) より高い効率を有する量子暗号プロトコルの構成
- (2) ネットワーク符号化によるコンピュータネットワークの高速化
- (3) ネットワーク符号化による通信デバイスの省電力化

2 関連する最近の研究テーマ

暗号の情報理論的な安全性

インターネットなどで現在よく使われているRSAなどの暗号方式は、大きな整数の素因数分解などのいくつかの計算問題を短い時間で解く方法が知られていないことに安全性の根拠を置いている。このような安全性を計算量的安全性と呼ぶが、もし素因数分解などを高速に解く方法が発見されれば計算量的安全性にもとづく暗号方式は使用できなくなってしまう。一方、秘密にしたい情報と悪意を持つ第三者が持つ情報が統計的に独立であれば、悪意を持つ第三者がいかに強力な計算機を持っているとしても秘密にしたい情報を当てずっぽうに推測するよりも正確に知ることはできない。秘密にしたい情報の統計的独立性を保証することによって得られる安全性を情報理論的安全性と呼び、本研究室では情報理論的安全性を保証できる以下のような暗号方式の研究を行っている。

量子暗号(量子鍵配送(QKD)プロトコル)

量子暗号の中の代表的な方式である量子鍵配送(QKD)プロトコルは、情報理論的に安全な暗号方式でもある。QKDプロトコルの目的はAliceとBobと呼ばれる正規ユーザーの間でEveと呼ばれる盗聴者に知られないように乱数列を共有することである。共有乱数列はAliceからBobに秘密裏に情報を伝えるために用いることができる。乱数列を共有するために、AliceはBobに単一光子の偏光などの量子力学の性質が強く現れる物理媒体を送る。もしEveがこの物理媒体を測定すると、量子力学の原理により測定された物理媒体の状態が変化してしまう。AliceとBobは送受信状態の変化からEveが得た情報量を推定し、送受信情報を適切に短くすることによってEveが得た情報と統計的に独立な乱数列を生成する。送受信状態の変化の仕方を推定することを通信路推定と呼ぶ。本研究室では、通信路推定に従来は捨てられていたデータを用いるとより正確に通信路推定が可能になるため共有できる乱数の量が増加することを明らかにし(文献[1])、提案した通信路推定法に合わせて物理媒体の送信方法を変えるとさらに共有できる乱数が増加することを示した(文献[2])。

雑音を用いた乱数の共有

前述の量子鍵配送プロトコルの実現には今のところ高価なデバイスを用意する必要がある。情報理論的に安全な鍵共有を比較的安価に実現するために自然界に存在する雑音を利用した鍵共有法がMaurerによって提案されている。Maurerの方法では前述のAlice, Bob, Eveが共通の雑音源(天体や無線LANなどなんでもよい)から信号を受信しているときに、Eveが盗聴することができる公開通信路を用いてAliceとBobが対話することによってEveに知られていない乱数を共有する。実際に受信する雑音は電波などの連続量であるが、Maurerの方法は雑音が離散的なデジタル情報である場合に対してしか検討が行われていなかった。そこで本研究室では文献[3]において雑音源が連続量であるときにEveに知られずに共有できる乱数の量を評価し、また連続的な雑音源を量子化したのちに従来のMaurerの方法を用いる場合に比べて、より多くの乱数を共有できる方式を開発した。

ネットワーク符号化とは

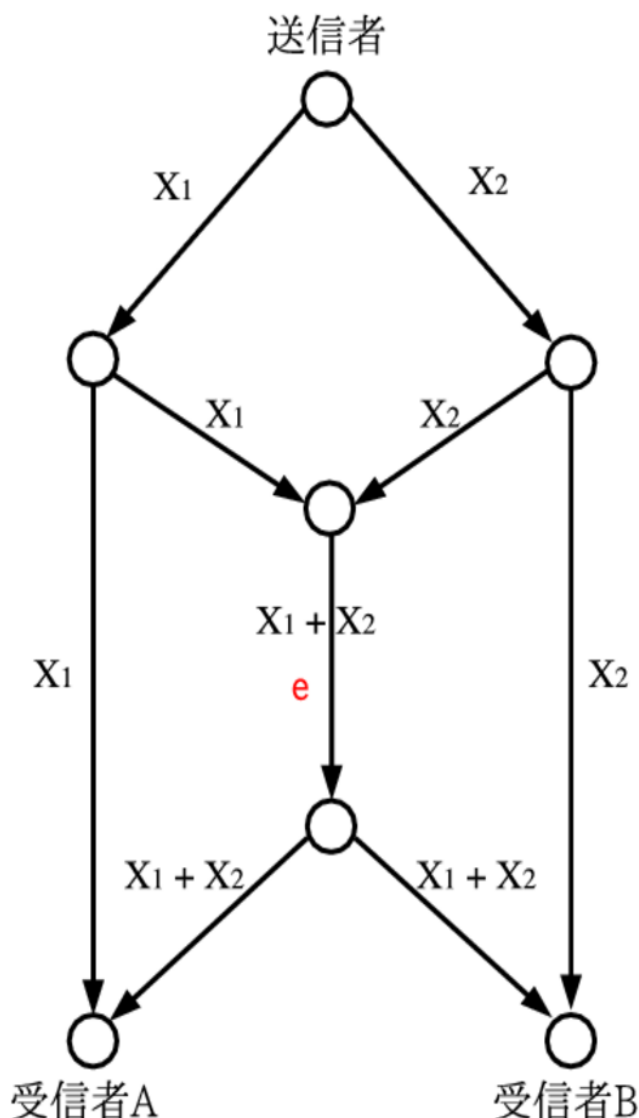
従来のコンピュータネットワークでは情報の中継ノードでは、隣接したノードから受け取る情報を別のノードにそのまま転送することしか許されていなかった。しかし、中継ノードにおいて複数の隣接ノードから受け取った情報を加工してから転送することを許すと、通信速度や消費電力が向上することが近年明らかにされた。

例えば、右図のように、送信者が受信者Aと受信者Bに同一のデータを送信したいとする。中継ノードが受信情報をそのまま転送しなければいけない場合は、情報

X_1 と X_2 の両方を受信者AとBに届けることはできない。しかしながら、リンクeに送出する情報を X_1 と X_2 の和(正確には排他的論理和)とすることにより、送信者Aは X_1 と X_1+X_2 を受け取り、それらから送信情報である X_1 と X_2 を復元することができる。このように中継ノードに複数の隣接ノードからの情報を加工して転送することを許す方式をネットワーク符号化と呼ぶ。

ネットワーク符号化による電力の節約

バッテリーで駆動する多数の観測装置の観測データを、観測装置に中継させてセンターに集約する場合など、ネットワークの中継ノードにおける消費電力をなるべく少なくしたい状況は多くある。消費電力を少なくするためにもネットワーク符号化は有効であることが知られている。ネットワーク符号化を許す場合は許さない場合に比べて必要な電力を何分の一まで削減できるかという限界について、従来知られていた最も優れた方法はネットワーク符号化により1/2.4に電力を削減した。一方本研究室ではオランダのWeber教授および植松教授と共同で、ネットワーク符号化を許す場合の消費電力の許さない場合に対する比率はいくらでも0に近づく場合が存在することを文献[4]で示し、ネットワーク符号化による消費電力の削減には際限が無いことを明らかにした。



3 関連する業績、プロジェクトなど

論文：

[1] S. Watanabe, R. Matsumoto, and T. Uyematsu, "Tomography increases key rates of quantum-key-distribution protocols," *Physical Review A*, vol. 78, no. 4, p. 042316, October 2008.

[2] R. Matsumoto and S. Watanabe, "Narrow basis angle doubles secret key in the BB84 protocol," *Journal of Physics A: Mathematical and Theoretical*, to be published, April 2010.

[3] M. Naito, S. Watanabe, R. Matsumoto, T. Uyematsu, "Secret key agreement by soft-decision of signals in Gaussian Maurer's model," *IEICE Transactions on Fundamentals*, vol.E92-A, no.2, pp.525-534, February 2009.

[4] J. Goseling, R. Matsumoto, T. Uyematsu, J. H. Weber, "On the energy benefit of network coding for wireless multiple unicast," *Proceedings of 2009 IEEE International Symposium on Information Theory*, pp. 2567-2571, July 2009.

受賞：電子情報通信学会論文賞(2001, 2008), 電子情報通信学会喜安善市賞(2008), 丹羽保次郎記念論文賞(2003)



准教授 山岡 克式(やまおか かつのり)

研究分野：情報通信ネットワーク(電話網, インターネット, 新世代ネットワーク)
キーワード：通信品質(QoS)制御, ストリーム通信, コンテンツ流通, WWW, 待ち行列理論
ホームページ：<http://www.net.ce.titech.ac.jp/>

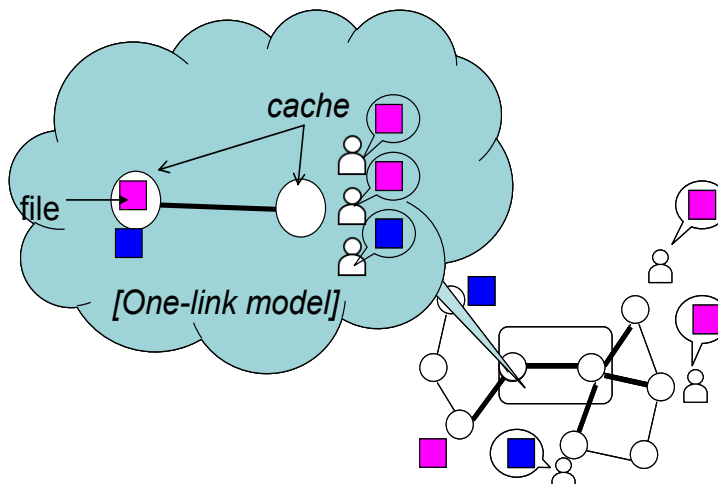
1 研究内容と目指すもの

- (1) 様々な通信の混在する環境で通信品質を維持向上させる網制御方式に関する研究
- (2) コンテンツの効率的なユーザへの配送を実現する制御アルゴリズムに関する研究
- (3) リアルタイムストリームの通信品質向上を目的としたプロトコル中継処理に関する研究

2 関連する最近の研究テーマ

ホップ・バイ・ホップファイル配送システムにおける効率的なコンテンツ配送アルゴリズムの研究

キャッシュ技術を用いて負荷分散を行う方式として、ユーザ要求によりファイルをユーザに配送する際に、その配送経路上のノードのキャッシュにファイルの複製を保存する方式が多く実装研究されている。P2PではFreenet や Winny等、また、Web サーバプロキシシステムやCDNでは、トランスパレントプロキシシステム等が挙げられる。この方式を用いることで、ユーザ要求に応じて、効率良く複製の分散配置を行う事が可能である。この方式を用いたファイル配送システムを、本研究ではホップ・バイ・ホップファイル配送システムと定義し、対象システムとした。



このシステムにおいて、ユーザの満足度を向上するためには、ファイル型のコンテンツは全データの取得が完了して初めて実行処理が可能のため、ユーザがリクエストを送信してから、全データを受信するまでの時間であるサービス時間の平均値を小さくする必要がある。また、リクエストが殺到するノードの上リリンクはボトルネックリンクとなる。本研究では、ボトルネックとなる One-linkに着目し、サービス時間の平均値を低減することを目的とする。

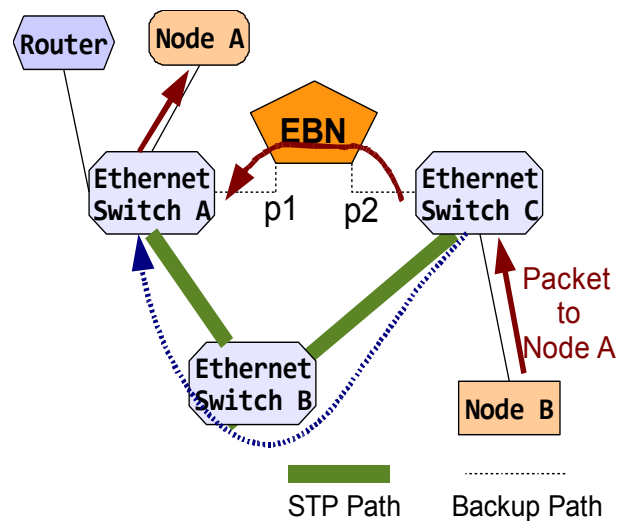
本研究では、リクエスト数/ファイル長が降順にファイルを送信した場合に、次のリクエスト到着までの間の局所最適解を得るという定理を発見し、正しいことを証明した。これをもとに、新たにリクエストが到着した際に、この値のソートを行いこの値が一番大きいファイルの配送を割り込み配送させることで、リクエストが到着する毎に、局所最適解を順次得る方式の提案を行った。その結果、ユーザの満足度を上げるために、クライアントーサーバシステム等で用いられているスケジューリングSRPT等と異なる、ホップ・バイ・ホップファイル配送システム特有の性質を考慮した提案スケジューリングを用いて、最適解に極めて近い性能を出すことに成功した。

L2待機リンク有効活用を実現するEthernet Bypassに関する研究

Ethernet Switchにより構成されているEthernetネットワークに、ループが存在すると、例えばEthernetブロードキャストアドレス宛てのEthernetフレームが、永遠にループしてしまう。それを防ぐために、ループが存在しないツリートポロジを作成するためにSTP(Spanning Tree Protocol)が提案され、標準的に実装されている。しかし、STPによって無効化されたパスは、障害時の代替パスには利用されるが、通常時は待機状態となり通信には利用されない。これによって、ツリートポロジの根となるEthernet Switchにトラヒックが集中してしまい輻輳が発生したり、最も近いパスとなる物理パスがSTPによって無効化されていることにより、迂遠なパスを経由するなどの問題が生じる。

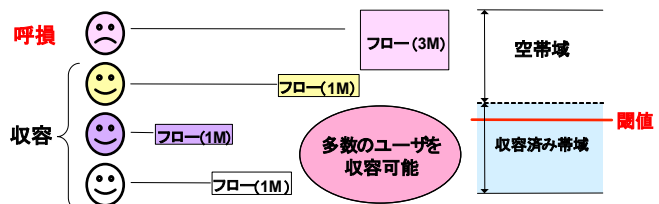
そこで本研究では、通常の通信はSTPによって作られたツリー状のパスを利用しつつ、選択したユニキャスト通信やそれぞれのIP Multicast通信のフローを対象として、STPによって無効化されたパスを利用し、トラフィックを分散することによるフレームの効率的な転送を実現する。

図に示すように、Node BからNode Aにパケットを送信するとき、標準の状態ではSTPによって決定されたパスを利用し、Ethernet Switch A,B,Cの3つのEthernet Switchを経由する。このとき、STPで待機状態であるが、迂回路として利用したいリンクにEthernet Bypass Node(EBN)を挿入する。EBNは、Node Bでパケットの送信先を管理しているARPテーブルをNode A宛てのパケットをEBNのp2宛てに送信するように、書き換えることによって、Node Bから見てEBNのp2にNode A存在すると認識させる。そして、EBNはp2宛て届いたNode A宛てのパケットをp1に送信することによって、Node BからNode A宛てのパケットの迂回を実現する。



ユーザ間対等に基づく全ユーザ満足度向上を目標とした多元トラヒック受付制御方式に関する研究

受付制御方式は、従来、資源の帯域利用効率向上が主目的となっていたが、帯域が通信の価値をそのまま表すとは限らない昨今では、従来方式を用いると、個々のユーザに対して大きな不満を生じさせる問題が生じる。本研究では、このユーザ満足度に着目し、網が現在おかれている状況を考慮しながら、全ユーザ満足度の向上を目的とした新しい受付制御方式を提案する。



本研究では基礎検討として、異なる要求帯域(広帯域フローと狭帯域フロー二種類に限定)に対し、收容時に同じ満足度を得る(対等)と仮定し、この考えの基、全ユーザ満足度を向上させるために、網内へのトータルで呼損となる確率(トータル呼損率)を最小にする新しい受付制御方式の解析を行った。この受付制御方式では、新規フロー到着時に、その時点での收容済み帯域が、制御パラメータである閾値より大きい場合、到着フローが広帯域フローの場合に呼損として取り扱うことで、トータル呼損を低減するため、適切な閾値設定が必要となる。

そこでまず、待ち行列理論M1M2/M1M2/S/S即時システムによるモデル化から理論式を立式し、数値計算の総当たりにより最適な閾値を導出し、その最適閾値を利用することにより、提案手法を用いない場合のトータル呼損率(rnon)より大幅な減少、かつトータル呼損の最小化を実現した。

さらに、数値計算による総当たりは、計算量が多く、実用的ではない。これに対し、様々なトラヒック状況に関して、最適閾値およびその最適閾値により得られる最小トータル呼損率の特性を解析した結果、最小トータル呼損率とほぼ同じトータル呼損率を実現する準最適閾値は、2次式により近似できることが明らかになった。そこで、最小トータル呼損率より1%以内の呼損率劣化を許容し、この劣化許容以内のトータル呼損率を実現する閾値を、「準最適閾値」と定義し、各トラヒック状況に対応する準最適閾値を容易に得られる近似式を、理論解析結果から最小自乗近似を用いて導出した。

3 関連する業績、プロジェクトなど

論文：“Local Optimal File Delivery Scheduling in a Hop by Hop File Delivery System on a One Link Model”, Hiromi Tsurumi, Takamichi Miyata, Katsunori Yamaoka, Yoshinori Sakai, IEICE Transactions on Communications, Vol.E92-B, No.1, pp.34-45 (2009)

“A Solution for Irregular IP Multicast Packet Flooding -For Heavy Traffic IP Multicast Communication-“, Makoto Misumi, Shin-ichi Nakagawa, Ken-ichi Chinen, Yoichi Shinoda, Katsunori Yamaoka, IEICE Transactions on Communications, Vol.E92-B, No.1, pp.68-76 (2009)

“Single-Fiber Access/Metro WDM Ring Architecture for Asymmetric Traffic Applications in Next Generation Networks”, Mitsumasa Okada, Katsunori Yamaoka, Yoshinori Sakai, IEEE/OSA Journal of Lightwave Technology, Vol. 27. No.9. pp. 1181-1196 (2009)

“Flow-admission control based on equality of heterogeneous traffic (two-type flow model)”, Sumiko Miyata, Katsunori Yamaoka. IEICE Transactions on Communications, Vol.E93-B No.12 pp.3564-3576 (2010)

著書:デジタル情報流通システム, 東京電機大学出版会 (2005)

受賞: IEEE CQR2009 Best Paper Award, 国際コミュニケーション基金優秀研究賞(2007), 東工大挑戦的研究賞 (2006)



教授 山田 功

研究分野：信号処理工学, 最適化工学, 逆問題
キーワード：信号処理, 最適化, 逆問題, 情報通信システム
ホームページ：<http://www.sp.ce.titech.ac.jp/>

1 研究内容を目指すもの

- (1) 信号処理工学の諸問題の数理解法の探求とその体系化に関する研究
- (2) 不動点理論や計算代数学を基盤とした高性能な信号処理アルゴリズムや最適化アルゴリズムの開発
- (3) 信号処理や最適化アルゴリズムの画像処理, 音響処理, リモートセンシング, 通信・ネットワークへの応用

2 関連する最近の研究テーマ

信号処理工学の諸問題のアルゴリズムに関する数理解法

信号処理工学(Signal Processing)の歴史はガウスによる「最小二乗推定」とフーリエによる「直交関数展開」のアイデアに遡ることができます。これら2つのアイデアが共にヒルベルト空間の「直交射影定理(一般のベクトル空間に拡張されたピタゴラスの定理)」によって明快に解釈できることはよく知られています。さらに、現代の情報通信システムを支えている信号処理方式の多くも「直交射影定理」の応用と見ることができます。「直交射影定理」の持つ汎用性と有効性は「(i)ヒルベルト空間とその閉部分空間が持つ柔軟な情報表現能力」と「(ii)閉部分空間中の大域的最近点決定問題と等価な線形方程式」を振り所としており、多種多様な信号処理問題が共通の「最適化原理と計算アルゴリズムのパッケージ」によって解決されてきたのです。これらの特長は新世代の信号処理方式の構築にあたって十分に尊重・踏襲されるべきでしょう。私たちは「無限集合の精密表現を可能にする数理」と「最適化の数理」の斬新な融合を進めることにより、強力な「最適化原理と計算アルゴリズムのパッケージ」を創造し、信号処理工学の未解決問題を見通しよく解決することに挑戦しています。以下、私たちの研究テーマの例を提唱する信号処理アルゴリズムと共に紹介します。

不動点集合上の凸最適化問題を解決するアルゴリズムと信号処理問題への応用

私たちは、20世紀の後半から急激な発展を遂げた非線形解析学の成果をサーベイすることによって、極めて多くの重要な問題(例えば、凸最適化問題、連立凸不等式)が非拡大写像の不動点を求める問題に帰着されてきたことに気が付きました。この事実、これまで精密な表現が不可能と思われてきた多くの無限集合が「非拡大写像の不動点集合(全ての不動点を集めてできる集合)」として統一的に表現できることを教えてくれています。私たちは、最適化理論の主役「最急降下法の学習則」と不動点理論の主役「非拡大写像の計算」を融合することによって、「ハイブリッド最急降下法」を開発し、世界に先駆けて「非拡大写像の不動点集合上の凸最適化問題」を解決することに成功しています。ハイブリッド最急降下法は、逆問題や信号処理工学の諸問題に無限の応用が可能であり、既に、国内外の研究者によってアレイアンテナのロバストビーム形成問題、画像の雑音除去問題、ネットワーク最適化問題等に適用され、著しい有効性が実証されています。また、多くの数学者・数理工学者によって、様々な一般化が試みられており、分野の垣根を超え、国際的に注目されています。さらに、私たちは、ハイブリッド最急降下法のアイデアを拡張することにより、「凸関数列の漸近的最小化」を達成する「適応射影劣勾配法」を提案し、その収束定理が強力な適応学習アルゴリズムを導くための指導原理になっていることを明らかにしています。適応射影劣勾配法は音響エコー消去問題、オンラインパターン認識問題、MIMO通信システムの干渉抑圧問題等に適用され、優れた性能が確認されています。

低階数最小分散擬似不偏推定法とその応用 — 線形ロバスト推定問題の新解法

悪条件(ill-condition)の線形逆問題に「(出力誤差の二乗平均値の最小化原理に基づいた)線形最小二乗推定法」を適用すると「パラメータ推定値と真値との二乗平均誤差」は線形モデルの係数行列が持つ「非零特異値」の逆数の二乗のオーダとなり、満足いく結果を与えないことが知られています。1970年にMarquardtは低階数行列の中に最小二乗推定法に優る推定法の例を示しています。私たちは「低階数行列の中で最適な推定行列とは何か」を明らかにするために、推定値のバイアスを最小に抑えた上で分散の最小化を図る「最小分散不偏推定法の方針」と小さな特異値の影響の回避を目的とした「低階数推定法の方針」を融合した「低階数最小分散擬似不偏推定法(MV-PURE)」を提案しています。私たちはMV-PUREをバイアス生成行列の全てのユニタリ不変ノルムを同時最小化した上で推定値の分散の最小化を達成する「階層構造を持つ非凸最適化問題の解」として定義し、それを陽に表現することに成功しています。さらに、実際にMV-PUREと既存のロバスト推定法を「MIMO通信システムの最適受信問題」や「脳波の信号処理問題」に応用することにより、モデルミスマッチに対して格段にロバストな優れた推定がMV-PUREによって実現されることを確認しています。

Monotone approximation to an unknown desired information to be estimated, say *estimandum*, is one of the most favorable properties for signal processing algorithms. In particular, in adaptive filtering or adaptive system identification problems (e.g., adaptive channel equalization, adaptive echo cancellation, etc), the algorithms are required, at each time, to offer a tentative approximation of an estimandum. By utilizing a priori knowledge as well as the latest statistical knowledge obtained from observed data, the algorithm is desired to update the previous estimate to better one which is closer to the estimandum. A practical scenario to realize such a monotone approximation is divided into the following two steps: (Step 1) define a set, say a target set, which is sufficiently small but contains candidates consistent with all available knowledge on the estimandum, and (Step 2) realize a mapping T which shifts any point not in the target set strictly closer to every point in the target set and does not move any point in the target set (See Figure 1). If the estimandum surely belongs to the target set, the above scenario automatically realizes a monotone approximation to the estimandum. The mapping satisfying the condition in Step 2 is called *attracting mapping* in modern fixed point theory. Obviously a point does not move by the mapping if and only if it is already in the target set. Therefore *the target set must be the fixed point set of the attracting mapping*.

Based on this simple observation, we established an unified scheme called the *Adaptive Projected Subgradient Method* (APSM); this scheme is a time-varying extension of the Polyak's subgradient algorithm, for nonsmooth convex optimization problem with a fixed target value, to the case where the convex objective itself keeps changing in the whole process. Under this simple umbrella of the APSM, a unified convergence analysis has been established for a wide range of adaptive algorithms. Moreover the APSM has been serving as a guiding principle to create various powerful adaptive algorithms for acoustic systems, wireless communication systems, distributed learning for diffusion network, online learning in Reproducing Kernel Hilbert Spaces, etc.

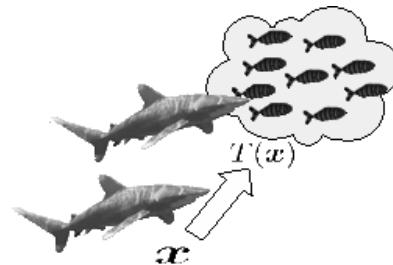
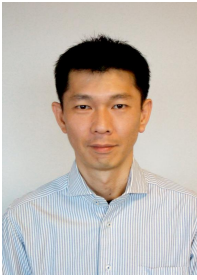


Fig.1 What is the best possible strategy for a starving shark ? Maximal satisfaction is expected by approaching monotonically every fish. This is realized by an *attracting mapping*.

3 関連する業績、プロジェクトなど

- ・論文: I. Yamada, "The hybrid steepest descent method for the variational inequality problem over the intersection of fixed point sets of nonexpansive mappings," *Studies in Computational Mathematics*, vol.8, pp. 473-505, Elsevier, 2001.
- T.Piotrowski and I.Yamada, "MV-PURE Estimator : minimum-variance pseudo unbiased reduced-rank estimator for linearly constrained ill-conditioned inverse problems," *IEEE Trans. Signal Process.*, vol.56, pp. 3408-3423, 2008.
- S.Gandy, B. Recht, I. Yamada, "Tensor completion and low-n-rank tensor recovery via convex optimization," *Inverse Problems*, 27(2), 025010, 2011. DOI: 10.1088/0266-5611/27/2/025010
- S.Theodoridis, K.Slavakis, I.Yamada, "Adaptive learning in a world of projections: a unifying framework for linear and nonlinear classification and regression tasks," *IEEE Signal Process. Mag.*, vol. 21, pp. 97-123, 2011.
- I. Yamada, M. Yukawa, M. Yamagishi, "Minimizing the Moreau envelope of nonsmooth convex functions over the fixed point set of certain quasi-nonexpansive mappings," In: *Fixed-Point Algorithms for Inverse Problems in Science and Engineering* (Bauschke et al, Eds.) pp.343-388, Springer, 2011.
- K. Slavakis and I. Yamada, "The adaptive projected subgradient method constrained by families of quasi-nonexpansive mappings and its application to online learning," *SIAM J. Optim.*, vol. 23, pp. 123-152, 2013.
- T. D. Nguyen and I. Yamada, "Adaptive normalized quasi-Newton algorithms for extraction of generalized eigen-pairs and convergence analysis," *IEEE Trans. Signal Process.*, vol.61, pp.1404-1418, 2013.
- D. Kitahara and I. Yamada, "Algebraic phase unwrapping along the real axis - Extensions and Stabilizations," *Multidimens. Syst. Signal Process.*, (43 pages, 2013), Springer. DOI: 10.1007/s11045-013-0234-7
- S. Ono, T. Miyata, I. Yamada, "Cartoon-Texture Image Decomposition Using Blockwise Low-Rank Texture Characterization," *IEEE Trans. Image Process.*, vol.23, pp. 1128-1142, 2014.
- 著書: 山田功, *工学のための関数解析*, 数理工学社 (2009)
- 受賞: 電子情報通信学会論文賞 (1991, 1995, 2006, 2009), 国際コミュニケーション基金優秀研究賞 (2004), ドコモ・モバイル・サイエンス賞[基礎科学部門] (2005), 藤野研究賞(2008), 電子情報通信学会業績賞(2009).



教授 一色 剛

研究分野：VLSI設計手法, システムレベル設計手法・設計環境

キーワード：システム・オン・チップ, マルチプロセッサ用並列コンパイラ, シミュレーション

ホームページ：<http://www.vlsi.ce.titech.ac.jp/>

1 研究内容と目指すもの

- (1) システム・オン・チップにおけるアーキテクチャ・アプリケーション設計最適化手法・設計環境
- (2) マルチプロセッサシステム・オン・チップ用高速シミュレーション手法
- (3) アプリケーション特化プロセッサのアーキテクチャ・コンパイラ同時合成手法

2 関連する最近の研究テーマ

マルチプロセッサシステム・オン・チップ(MPSoC)のシステムレベル設計最適化手法の開発

現在の携帯情報端末や情報機器は非常に複雑で高機能な組み込みシステムが搭載されており、そのハードウェアは最先端のVLSI技術を駆使したシステム・オン・チップ(SoC)によって実現されている。その上で様々なアプリケーションを実行する環境を提供し、必要な処理スループットを確保した上で低消費電力化を実現するために、最近のSoCは複数のプロセッサを搭載したMultiprocessor SoC (MPSoC)構成を採用するケースが多くなってきている。このような複雑なMPSoCの開発には、高性能プロセッサ開発、プロセッサ間通信方式、高性能バスアーキテクチャやメモリアーキテクチャといったハードウェアアーキテクチャ設計だけでなく、その上で実行されるアプリケーションやミドルウェアの設計が必要であり、市場競争力のある高付加価値なMPSoCの開発のためには、ハードウェアとソフトウェアの協調設計手法・同時最適化手法を確立することが極めて重要な課題である。

本研究室では、このようなMPSoCのシステムレベル設計最適化手法の確立を目指し、以下の項目について研究を進めている：

- ・ 並列処理ソフトウェア開発環境(並列プログラミングモデル, 並列コンパイラ, 並列処理シミュレータ)
- ・ 高速通信機能を搭載したプロセッサ開発(基本命令セット, 通信・同期用拡張命令セット, 高速データ通信制御回路, プロセッサ記述言語を用いたプロセッサアーキテクチャ定義, プロセッサ論理回路自動生成)
- ・ 電子システムレベル(ESL)CADツールと連携したMPSoCアーキテクチャの自動生成及びシステムレベルシミュレーション環境構築
- ・ ハードウェアアーキテクチャ探索やアプリケーションソフトウェアチューニングを目的とした高速システムパフォーマンス見積りのためのシステムワークロードシミュレーション手法
- ・ 画像処理, 3Dグラフィックスや無線通信処理を中心としたアプリケーション特化MPSoCの設計開発

これらの研究活動は、ドイツ・アーヘン工科大を初めとする他大学との共同研究や、国内外の産業界との共同研究を通じて積極的に展開している。

Tightly-Coupled Thread (TCT)モデルによる並列処理ソフトウェア開発環境

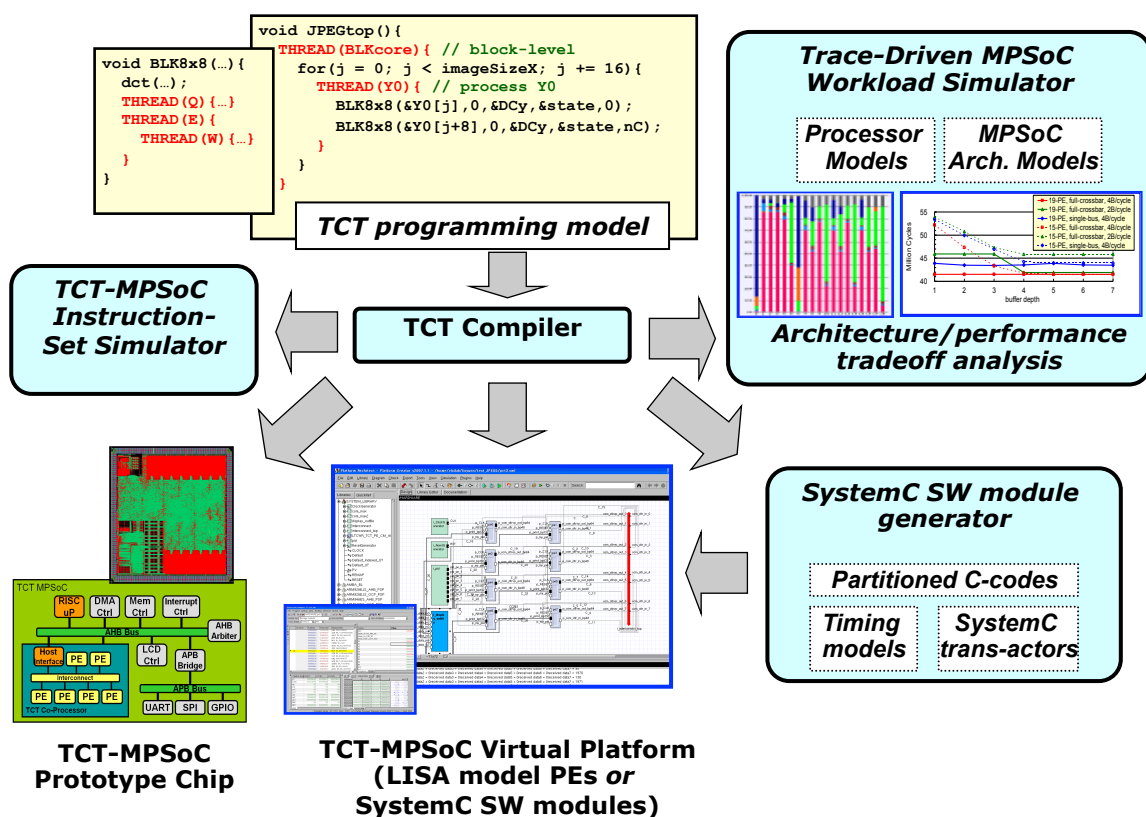
当研究室で開発されたTightly-Coupled Thread (TCT) モデルとは、組み込みシステム用ソフトウェア言語として最も普及しているC言語を用いた新しい並列プログラミングモデルである。通常の逐次処理Cプログラムの上に、プログラムの分割境界を「スレッドスコープ」によって記述するだけで、データ通信や同期といった並列プログラミングで最も難しいプログラミング記述を必要としないことが大きな特徴であり、我々のTCTコンパイラによってスレッド間のデータ依存性解析やポインター解析によって必要なデータ通信や同期を自動的に抽出し、並列プログラムが自動的に生成される。このTCTプログラミングモデルとTCTコンパイラ技術により、これまでに蓄積されてきた膨大なソフトウェア資産(逐次処理ソフトウェア)を並列処理プログラムに変換することが可能となり、MPSoC用アプリケーションの開発効率を大幅に向上することができる。

TCTコンパイラが生成する並列プログラムを実行する通信機能付きプロセッサモデルも開発されており、並列プログラム実行をサイクル精度で擬似実行するマルチプロセッサ命令セットシミュレータによってその動作検証が可能である。

マルチプロセッサシステム用ワークロードシミュレーションフレームワーク

多数のプロセッサや回路モジュールを搭載したMPSoCの動作検証は、非常に膨大なシミュレーション時間を要し、MPSoCの設計開発効率を著しく低下させる大きな原因となっている。シミュレーション時間短縮のためには、プロセッサ動作検証のための高速命令セットシミュレーション技術が有効であるものの、多数のプロセッサや複雑なバス構造を有するシステムの動作検証にはなお長時間のシミュレーションが必要であり、アーキテクチャの設計空間探索やソフトウェアチューニングを行うには不十分である。当研究室で開発しているワークロードシミュレーションフレームワークは、各プロセッサ上で実行されるソフトウェアの動作モデルを「ワークロードモデル」として抽象化し、システムバスのデータトラフィックを高精度に再現することによって、従来のシステムシミュレーションと比べて数百倍の動作検証スピードを達成した上で非常に高精度のパフォーマンス見積りを可能としている。

このワークロードシミュレーションフレームワークをベースに、最適なマルチプロセッサアーキテクチャ(プロセッサ構成、システムバス構成、メモリアーキテクチャ構成)の設計最適化を行う設計環境を整備し、アプリケーション設計環境と統合した設計開発メソッドロジーの構築に取り組んでいる。



3 関連する業績、プロジェクトなど

- [1] S. Wisayataksin, D. Li, T. Isshiki, and H. Kunieda, "Entropy Decoding Processor Modern Multimedia Applications", IEICE Trans. Fundamentals, vol.E92-A, no.12, pp.3248-3257 (2009)
- [2] M. Z. Urfianto, T. Isshiki, A. U. Khan, D. Li, and H. Kunieda, "Decomposition of Task-Level Concurrency on C T. Isshiki, "Efficient MPSoC Design Space Exploration on the Tightly-Coupled Thread Workload Simulation Framework", 9th International Forum on Embedded MPSoC and Multi-Core (2009)
- [3] T. Isshiki, D. Li, H. Kunieda, T. Isomura, K. Satou, "Trace-Driven Workload Simulation Method for Multiprocessor System-On-Chips", Proceedings of 46th Design Automation Conference (2009)
- [4] Programs Applied to the Design of Multiprocessor SoC", IEICE Trans. Fundamentals, vol.E91-A, no.7, pp. 1748 - 1756 (2008)
- [5] S. Wisayataksin, D. Li, T. Isshiki, and H. Kunieda, "Low Cost SoC Design of H.264/AVC Decoder for Handheld Video Player", IEICE Trans. Fundamentals, vol.E91-A, no.4, pp.1197-1205 (2008)
- [6] M. Z. Urfianto, T. Isshiki, A. U. Khan, D. Li, and H. Kunieda, "A Multiprocessor SoC Architecture with Efficient Communication Infrastructure and Advanced Compiler Support for Easy Application Development", IEICE Trans. Fundamentals, vol.E91-A, no.4, pp.1185-1196 (2008)



教授 上野 修一

研究分野: 並列・VLSI計算論, 量子・ナノ計算論
キーワード: 3次元集積回路, ナノ回路, 量子回路, 可逆回路
ホームページ: <http://www.lab.ce.titech.ac.jp/ueno/japanese/indexj.html>

1 研究内容と目指すもの

- (1) 3次元集積回路のレイアウト設計のアルゴリズムと計算複雑度
- (2) ナノ回路の耐故障設計のアルゴリズムと計算複雑度
- (3) 量子・可逆回路の論理合成のアルゴリズムと計算複雑度

2 関連する最近の研究テーマ

3次元チャネル配線に関する研究

未来の集積回路として3次元集積回路が注目されています。現在の集積回路と比較すると、配線長が短く、消費電力も少なく、さらに小さな体積で大規模システムを設計できることなどの長所があるために、世界的に活発に3次元集積回路の研究が進められています。大規模システムは階層的に設計されますが、3次元集積回路を階層的に設計する際に3次元チャネル配線問題が登場します。3次元チャネルは3次元格子グラフでモデル化されますが、その上面と下面の格子点に端子が配置されています。配線で結ばれるべき端子の集合をネットといいます。3次元チャネル配線問題の目的は、高さが最小の3次元チャネル内で各ネットの端子を木(配線)で結ぶことです。ただし、異なるネットの木は互いに点非共有でなければなりません。

私たちは、この問題がNP困難であることを証明しました。(論文[8]) したがって、この問題は大変難しいわけですが、私たちは効率的な配線アルゴリズムを設計しました。すなわち、3次元チャネルの上面と下面が $2n \times 2n$ の正方格子で、端子は奇数座標の格子点に配置されている場合には、任意の2端子ネットの集合を高さ $3n$ の3次元チャネル内で配線する多項式時間アルゴリズムを設計しました。(論文[9])

ナノPLAの耐故障設計に関する研究

未来の集積回路としてナノPLAも注目されています。ナノPLAは規則的な構造をしているので設計が容易であるという長所がありますが、微細な構造であるために耐故障設計が不可欠です。ナノPLAの耐故障設計に付随して重要な二つの問題があります。一つは論理関数を欠陥のない部分回路に実現する論理マッピング問題です。もう一つは、規模が最大の欠陥のない部分ナノPLAを探索する問題です。スイッチの欠陥と配線の欠陥が共に存在する場合には、前者は2部グラフの部分グラフ同型問題として定式化され、後者は完全2部部分グラフ問題として定式化されるので、これらの問題はNP困難であることが知られています。

私たちは、配線の欠陥だけを仮定した場合でさえも論理マッピング問題はNP困難であることを証明しました。一方、配線の欠陥だけを仮定した場合には、規模が最大の欠陥のない部分ナノPLAを探索する問題は多項式時間で解けることを明らかにしました。これは、配線の欠陥があるナノPLAを表現する2部グラフが直交半直線グラフという特別な交差グラフであることに起因します。(論文[4])

直交半直線グラフに関する研究

ナノPLAの耐故障設計などへの応用のために、私たちは直交半直線グラフを新たに導入しました。これは、平面上の水平及び垂直半直線の交差グラフです。すなわち、半直線を点として、対応する半直線が交差するとき、点对を辺で結んで得られる2部グラフを直交半直線グラフといいます。応用上重要な効率的なアルゴリズムを設計するためには、この直交半直線グラフの構造を調べる必要があります。

私たちは、水平半直線は右向きのみで、垂直半直線は上向きのみである場合の直交半直線グラフ(これを2方向直交半直線グラフといいます)の様々な構造を明らかにしました。すなわち、2方向直交半直線グラフの隣接行列による特徴付け、点集合の順序構造による特徴付け、円弧グラフによる特徴付け、及び禁止部分グラフによる特徴付けなどを示しました。これらの特徴付けから、2方向直交半直線グラフの認識問題と同型問題が多項式時間で解けることが分かりました。さらに、禁止部分行列に関する長い間の懸案が解決できることも分かりました。(論文[1])

可逆回路の故障検出に関する研究

可逆回路は、全単射である論理関数を計算するので、情報の損失がありません。可逆回路は量子回路の特別な場合ですが、量子回路、低消費電力回路、及び信号処理などに応用があるために、可逆回路の論理合成や故障診断などが活発に研究されています。

私たちは、可逆回路の縮退故障を検出するための最小完全テスト集合を求める問題がNP困難であることを証明しました。(論文[6]) また、可逆回路の族に対する万能テスト集合を新たに導入し、様々な可逆回路の族に対して、万能テスト集合の大きさを明らかにしています。(論文[2])

3 関連する業績、プロジェクトなど

論文:

- [1] A.M.S. Shrestha, S. Tayu, and S. Ueno, On Two-Directional Orthogonal Ray Graphs, Proc. of the IEEE International Symposium on Circuits and Systems, 2010, to appear.
- [2] S. Tayu, S. Fukuyama, and S. Ueno, Universal Test Sets for Reversible Circuits, IEICE Technical Report, Vol.109, No.300, pp.59–64, 2009.
- [3] S. Tayu, T. Oshima, and S. Ueno, On the Three-Dimensional Orthogonal Drawing of Outerplanar Graphs, Proc. of the IEEE International Symposium on Circuits and Systems, pp.836–839, 2009.
- [4] A.M.S. Shrestha, S. Tayu, and S. Ueno, Orthogonal Ray Graphs and Nano-PLA Design, Proc. of the IEEE International Symposium on Circuits and Systems, pp.2930–2933, 2009.
- [5] S. Tayu, K. Nomura, and S. Ueno, On the Two-Dimensional Orthogonal Drawing of Series-Parallel Graphs, Discrete Applied Mathematics, Vol.157, pp.1885–1895, 2009.
- [6] S. Tayu, S. Ito, and S. Ueno, On Fault Testing for Reversible Circuits, IEICE Trans. Inf. & Syst., Vol.E91–D, pp. 2770–2775, 2008.
- [7] S. Tayu, K. Nomura, and S. Ueno, On the Three-Dimensional Orthogonal Drawing of Series-Parallel Graphs, Proc. of the IEEE International Symposium on Circuits and Systems, pp.212–215, 2008.
- [8] S. Tayu and S. Ueno, On the Complexity of Three-Dimensional Channel Routing, Proc. of the IEEE International Symposium on Circuits and Systems, pp.3399–3402, 2007.
- [9] S. Tayu, P. Hurtig, Y. Horikawa, and S. Ueno, On the Three-Dimensional Channel Routing, Proc. of the IEEE International Symposium on Circuits and Systems, pp.180–183, 2005.

著書:情報基礎数学 昭晃堂(2007), 情報とアルゴリズム 森北出版(2005)

受賞:情報処理学会30周年記念論文賞(1990), 電子通信学会論文賞(1986)



教授 高木 茂孝

研究分野：電子回路, 集積回路, 回路理論

キーワード：アナログ集積回路, フィルタ, 増幅回路, 発振回路, A-D変換回路

ホームページ：http://www.ec.ce.titech.ac.jp/

1 研究内容と目指すもの

人間が認識する光や音などの信号はアナログ信号であり、自然界と信号処理システムとのインタフェースとしてアナログ回路は不可欠な要素です。また、同一の信号処理をアナログ回路とデジタル回路で行えば、物理現象を利用したアナログ回路のほうが遙かに高速です。さらに、デジタル回路を高速に動作させると、信号波形がなまり、1または0を判別することは至難の業です。この判別をできる限り精度良く行うのがアナログ回路技術です。アナログ回路技術は、システムLSIを支える基盤技術であり、我々の研究室では、特にアナログ集積回路の高性能化を目的に研究を行っています。

2 関連する最近の研究テーマ

レベルクロッシングアナログ-デジタル変換回路

振動を検知する防犯用あるいは地震用センサが出力する信号はアナログ信号であり、通常は大きな振幅の変化がなく、振動が発生したときだけ振幅が大きく変化する信号です。一方で、センサは小型、長寿命であることが望まれていますので、消費電力をできるだけ低減することが大きな課題となっています。このような背景の下で、センサからの出力信号に大きな変化があったときだけ、その信号を処理することで消費電力を低減する手法が知られています。たとえば、図1に示すように、センサからの信号 V_{in} が「1」という値を上回った時刻 t_1 で V_{UP} という信号を出力し、さらに「2」という値を上回った時刻 t_2 で再び V_{UP} という信号を出力し、次に「1」という値を下回った時刻 t_3 や「0」という値を下回った時刻 t_4 では V_{DN} という信号を出力したとします。このように、ある値を上回ったか、下回ったかということと、ある値を上回ったか、下回った時刻を伝えることができれば、もとのアナログ信号を再現することができます。一般にこれらの情報はデジタル信号として伝えられます。このようにして、アナログ信号をデジタル信号に変換する回路をレベルクロッシングアナログ-デジタル変換回路(レベルクロッシングA-D変換回路)と呼びます。この回路は、アナログ信号に大きな変化があったときだけ動作すればよいので、消費電力を大幅に低減できる可能性があります。

我々の研究室では、レベルクロッシングA-D変換回路の構成について研究し、従来回路と比較して、消費電力が約64%、回路規模が約34%で動作し、高精度で高速である、図2の回路を発表しました。ただ、この回路は定常的に電力を消費するため、CMOS論理回路のように、アナログ信号が大きく変化したときだけ電力を必要とする構成を今後検討し、一層の特性改善を実現したいと考えています。

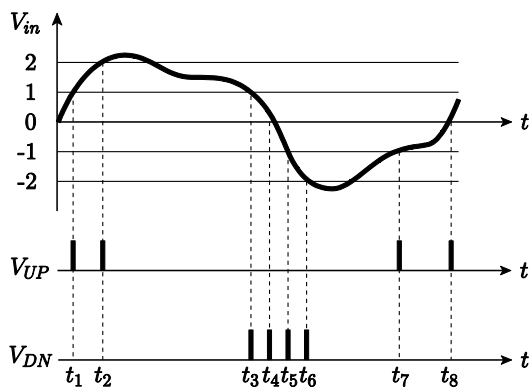


図1: レベルクロッシングA-D変換回路の動作

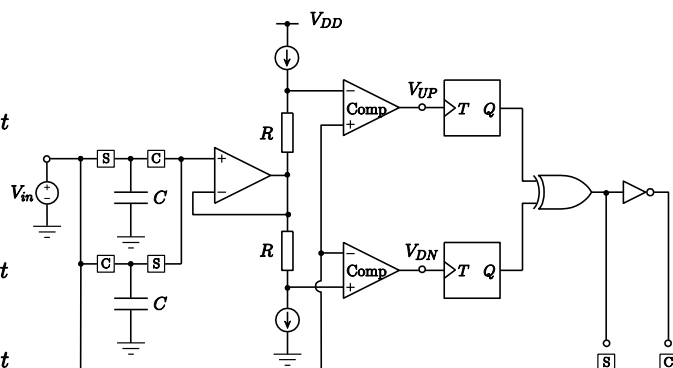


図2: 開発したレベルクロッシングA-D変換回路

高性能能動インダクタ回路の構成

最近の集積回路プロセスでは、インダクタをスパイラル形状にして集積回路上に実現できるようになりました。しかし、このようなインダクタは大面積を占め、実用となるのは約1GHz以上の周波数の信号に対してだけです。しかも、損失も大きく、理想的なインダクタとは特性がだいぶ異なります。高性能インダクタが1GHz以上の高い周波数帯域で使用できれば、受信機に欠かすことのできない低雑音増幅回路の特性改善、発振回路の位相雑音の低減、特性の安定したフィルタの実現などが期待できます。従来から、トランジスタなどの能動素子と容量を用いてインダクタと等価な働きをする回路を構成できることは知られていました。我々の研究室では、図5の従来回路の冗長な部分を排除し、さらに、回路的な工夫により図6の回路を導出しました。図5と図6の台形は電圧制御電流源を表し、 G が伝達コンダクタンスです。図5と図6はともに、インダクタと等価な働きをしますが、伝達コンダクタンスが半分になりますと、消費電力も半分になりますので、提案回路は従来回路と比べて消費電力が約33%削減できます。この回路を1GHz以上の信号を処理する高周波回路へ応用することが今後の課題です。

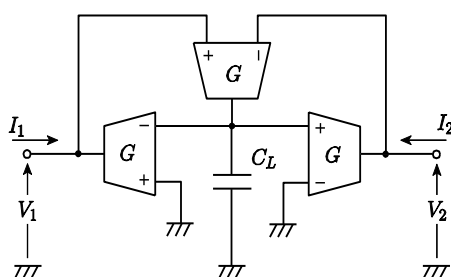


図5：従来の能動インダクタ回路

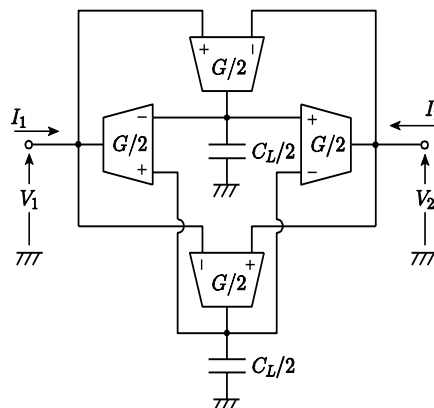


図6：提案した能動インダクタ回路

超低周波信号処理用スイッチトキャパシタフィルタの構成

アナログ回路は高周波信号処理だけでなく、センサなどからの微小信号を検出、増幅するためにも不可欠です。我々の研究室では、スイッチトキャパシタフィルタと呼ばれる回路のセンサなどへの応用を目指しています。スイッチトキャパシタフィルタは、基準周波数と容量比で特性が決まるため、集積回路上で構成しても高精度な回路が実現できます。しかし、基準周波数を変えずにフィルタの遮断周波数を低くすると、大きな容量比が必要となり、集積回路上で容量が占める面積が増大します。この問題を解決するために、我々の研究室では、電荷の部分転送手法を提案しました。図7はフィルタを構成する回路の一部です。数字が書かれた正方形がスイッチを表しています。C3と書かれた容量がある場合は無い場合よりもC0へ転送される電荷が減少していることが簡単な計算でわかります。しかし、人間や車などの動き検出に用いるためには、一層の総容量値の低減が必要です。

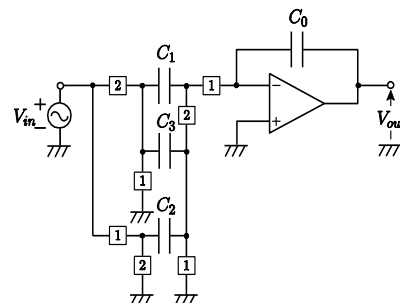


図7：スイッチトキャパシタ回路

3 関連する業績、プロジェクトなど

論文等: P. Nogas, S. Takagi, H. Sato, N. Retdian, "Performance Comparison of Three Asynchronous Level-Crossing ADC Designs," 電気学会研究会資料, ECT-14-030, pp.161-166, 2014.

N. Retdian, K. Takagi, S. Takagi, "Capacitance Spread Reduction Technique for Low-Cost Switched-Capacitor Filters Implementation," Proceedings of European Conf. on Circuit Techniques and Designs, Aug. 2009.

佐藤, 高木, 藤井, "アクティブインダクタの対称構成による低消費電力化," 電気学会論文誌C, Vol.129, No.8, pp.1534-1540, 2009.

著 書: MOSアナログ電子回路, 昭晃堂 (1998), デジタル集積回路入門, 昭晃堂 (2000), 線形回路理論, 昭晃堂 (2004), アナログ電子回路, 培風館 (2008), アナログ電子回路入門, 理工学社 (2012) など

受 賞: 電子情報通信学会論文賞 (1995, 2000), IPアワード開発奨励賞 (2000), 電気学会電子・情報・システム部門特別貢献賞 (2012), 電気学会フェロー (2013) など



教授 高橋 篤司

研究分野：VLSI設計手法, 同期式回路

キーワード：EDA, 論理設計, レイアウト設計,

ホームページ：<http://www.eda.ce.titech.ac.jp/takahashi/japanese/indexj.html>

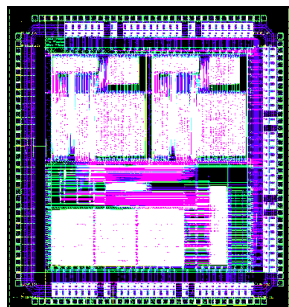
1 研究内容と目指すもの

- (1) デジタル集積回路システムのナノテクノロジー時代に対応する設計方法論の確立
- (2) 不確実性の増大に対応する可変レイテンシ回路の実現
- (3) 最先端テクノロジーの要求に応え人手設計を凌駕する性能を持つ配置配線アルゴリズムの開発

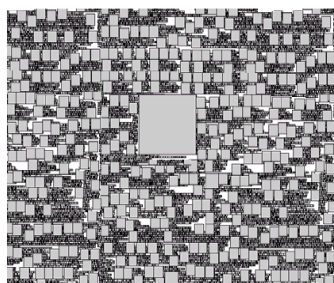
2 関連する最近の研究テーマ

一般同期方式に基づくデジタル集積回路設計方法論

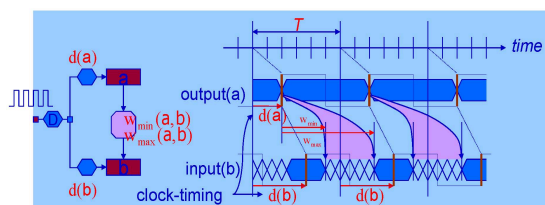
クロック信号を集積回路全体に同時に分配することを前提とする完全同期方式に基づく設計方法論は、集積回路を効率よく設計するための手段として、特に意識されることなく広く一般に用いられてきた。しかし、回路素子の微細化、回路の高速化によりクロック信号の集積回路全体への同時分配は、1990年代には困難となっていた。完全同期方式に基づく設計方法論はあくまでも手段ではあったが、あまりに広く一般に用いられていたため、その設計方法論を維持することが集積回路設計の大きな目的となるなどし、現在でも、完全同期方式に基づく設計方法論は広く一般に用いられている。しかし、必ずしも高性能な集積回路を実現しているとは言えない。当研究室では、クロック信号を集積回路の各部分に適切なタイミングで分配することで高性能な集積回路を効率よく実現する、一般同期方式に基づく設計方法論の確立を目指している。【論文4-6】



集積回路



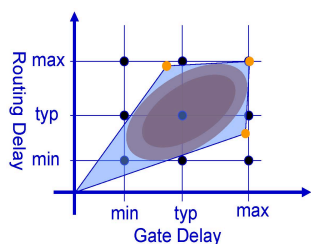
回路モジュール配置



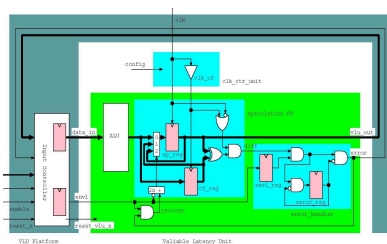
タイミングチャート(一般同期)

可変レイテンシ回路の実現

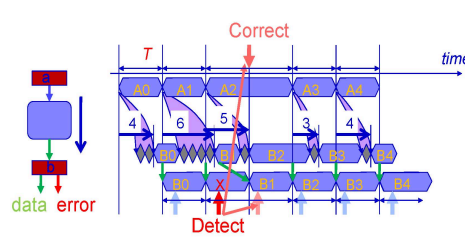
遅延は様々な要因によって変化し、回路の微細化、高速化に伴いばらつきの影響が大きくなっている。回路動作の正当性は想定されるすべての状況において保証されなければならないが、最悪状況の平均的状況からの逸脱が大きい現状では、常に回路に同一の動作をさせることは、回路性能の向上の大きな妨げとなっている。当研究室では、エラー検出回復方式に基づき回路動作を遅延の変化に応じて変更する高性能な可変レイテンシ回路の実現を目指している。



遅延分布(配線遅延, 素子遅延)



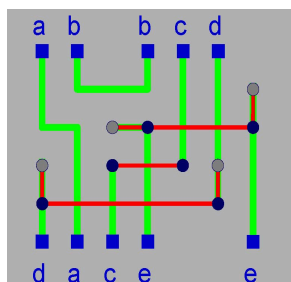
エラー検出回復方式



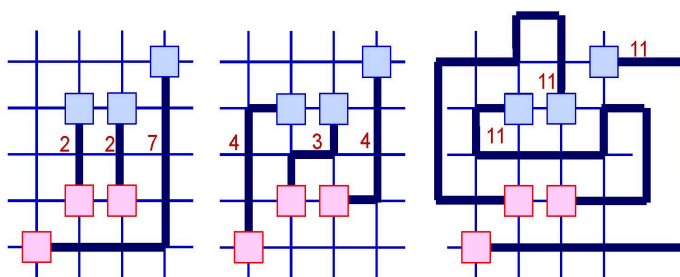
タイミングチャート(可変レイテンシ)

特定用途向け配線アルゴリズム開発

集積回路チップ内では、数多くの配線を実現しなければならないため、人手設計がほぼ不可能となり、配線が多層化するなど配線資源に比較的余裕があるため、配線設計の自動化が進展した。しかし、問題規模が比較的小さく、様々な仕様を満たすことが要求される場合、自動配線アルゴリズムの性能は人手に及ばない。そのため、人手設計がまだ一般的である場面も多いが、設計期間の短縮、大規模化への対応のため、自動配線アルゴリズムの性能向上が望まれている。当研究室では、プリント基板配線、パッケージ配線など人手設計がまだ一般的である配線問題に対して、問題の特徴を生かし、人手設計のノウハウを様々な形で組み込んだ、最短配線、等長配線、指定長配線など様々な要求仕様を満たす配線を生成するための配線アルゴリズムの開発を、配置設計との連携や全体の設計フローの構築を含めて進めている。



チャンネル配線(2層ビア多重化)

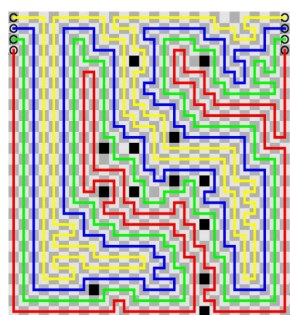


a) 総配線長最小

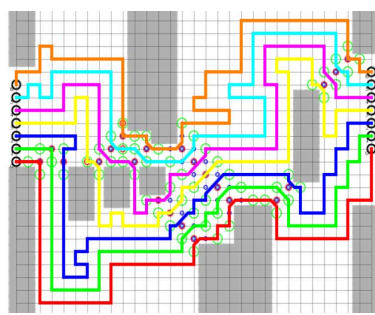
b) 最大最小

c) 等長

端子集合対間配線(1層)

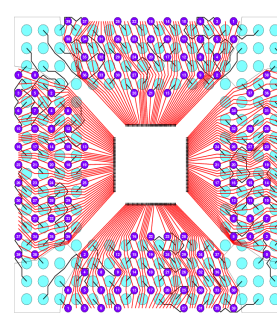


a) HV



b) HVX

プリント基板配線(1層指定長)【論文1,2】



パッケージ配線(2層BGA引出線付)【論文3】

3 関連する業績、プロジェクトなど

論文：

- 1.Kiosk Shinoda, Yukihide Kohira, Atsushi Takahashi. Single-Layer Trunk Routing Using Minimal 45-Degree Lines. *IEICE Trans. Fundamentals*, Vol.E94-A, No.12, pp.2510-2518, 2011.
- 2.Yukihide Kohira, Atsushi Takahashi. CAFE router: A Fast Connectivity Aware Multiple Nets Routing Algorithm for Routing Grid with Obstacles. *IEICE Trans. Fundamentals*, Vol.E93-A, No.12, pp.2380-2388, 2010.
- 3.Yoichi Tomioka, Yoshiaki Kurata, Yukihide Kohira, Atsushi Takahashi. MILP-based Efficient Routing Method with Restricted Route Structure for 2-Layer Ball Grid Array Packages. *IEICE Trans. Fundamentals*, Vol.E92-A, No.12, pp.2998-3006, 2009.
- 4.Yukihide Kohira, Shuhei Tani, Atsushi Takahashi. Minimization of Delay Insertion in Clock Period Improvement in General-Synchronous Framework. *IEICE Trans. Fundamentals*, Vol.E92-A, No.4, pp.1106-1114, 2009.
- 5.Yosuke Takahashi, Yukihide Kohira, Atsushi Takahashi. A Fast Clock Scheduling for Peak Power Reduction in LSI. *IEICE Trans. Fundamentals*, Vol.E91-A, No.12, pp.3803-3811, 2008.
- 6.Atsushi Takahashi. Practical Fast Clock-Schedule Design Algorithms. *IEICE Trans. Fundamentals*, Vol.E89-A, No.4, pp.1005-1011, 2006.

著書：情報基礎数学 昭晃堂(2007), 情報とアルゴリズム 森北出版(2005)

受賞：東工大挑戦的研究賞(2005), LSI IPデザイン・アワード IP賞(2001), 電子情報通信学会学術奨励賞(1998), 回路とシステム軽井沢ワークショップ奨励賞(1992)



准教授 原 祐子

研究分野： 組み込みシステム、ハードウェア・ソフトウェア協調設計
キーワード： 高信頼システム、CAD、システム・オン・チップ
ホームページ： <http://www.cad.ce.titech.ac.jp/>

1 研究内容と目指すもの

- (1) 高信頼組み込みシステムのハードウェア・ソフトウェア協調設計手法
- (2) 新たな計算パラダイムに向けた高位合成・論理合成手法
- (3) 他分野のアプリケーション・アーキテクチャ設計へのCAD技術応用

2 関連する最近の研究テーマ

高信頼組み込みシステムのハードウェア・ソフトウェア協調設計手法

自動車・航空機・衛星などのセーフティクリティカルな組み込みシステムは言うまでもなく、携帯電話や家電製品などの組み込みシステムにとっても、信頼性（長い期間、正しく動くこと）は非常に重要な問題である。半導体（シリコンデバイス）の微細化や低電力技術の発展、さらに、ポストシリコンデバイス（図1）の開発・発展に伴い、信頼性の問題はますます深刻化している。これまでは、どこか1カ所故障してもスベアの部品が肩代わりする多重化や、トランジスタが正しく動作する条件（低い周波数・高い電圧）で動かすなど、安全側に倒した設計をしていた。しかし、回路規模が大きくなれば製造コストは上がり、保守的な条件で設計・使用すれば消費エネルギーの増加や性能ロスが起こるため、微細化・低電化が進んだシリコンデバイスやポストシリコンデバイスのメリットである「低消費エネルギー」の恩恵にあずかれない。

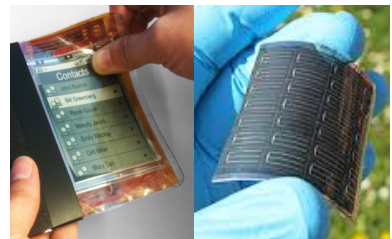


図1: ポストシリコンデバイス

本研究室では、製造コスト・性能・エネルギーの点で無駄なく、かつ、高い信頼性で組み込みシステムを設計する技術の研究に取り組んでいる（図2、論文[4]）。ハードウェアとソフトウェアの両面、さらには両者を融合した視点から、デバイスの多様な故障や不確かさの問題に包括的に当たることで、アプリケーションやアーキテクチャに応じた最良の解を導き出す。最終的には、ポストシリコンデバイスを用いて、回路の一部が故障しても自立して故障に対処する、次世代組み込みシステム（スマートセンサなど）の確立を目指す（図3）。

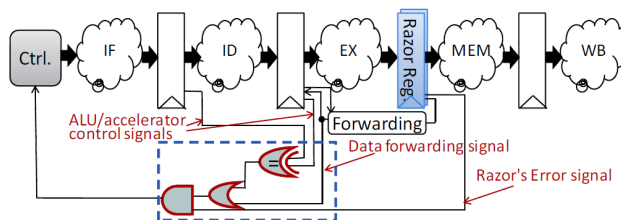


図2: 少ない性能・面積オーバーヘッドでタイミング違反を検出・修正するアーキテクチャ



図3: スマートセンサの例

新たな計算パラダイムに向けた高位合成・論理合成手法

組み込みシステムの大規模・複雑化に伴い、ハードウェア記述（Hardware Description Language: HDL）を用いる従来のハードウェア（RTL）設計技術は、設計生産性の点で非効率的になってきた。現在では、C/C++などの動作記述で設計し、RTL記述を自動生成する高位合成（High-Level Synthesis: HLS）という手法に徐々にシフトしている（図4、論文[1]）。

一方、従来は「計算結果は常に正しく行われる」ようにLSI設計が行われてきたが、近年、多少の誤差が許容できる場合には、確率的、あるいは、近似的な計算を採用することで、LSI設計を簡易化する方法が試みられている（前者をStochastic Computing（図5）、後者をApproximate Computing（図6）と呼ぶ）。

本研究室では、Stochastic ComputingやApproximate Computingに基づくLSI回路を、高位合成や論理合成によってより効率良く、最適な構成を体系的に決定する手法を確立することを目指す。これにより、回路面積、計算時間、エネルギー消費量の大幅な改善が実現する。

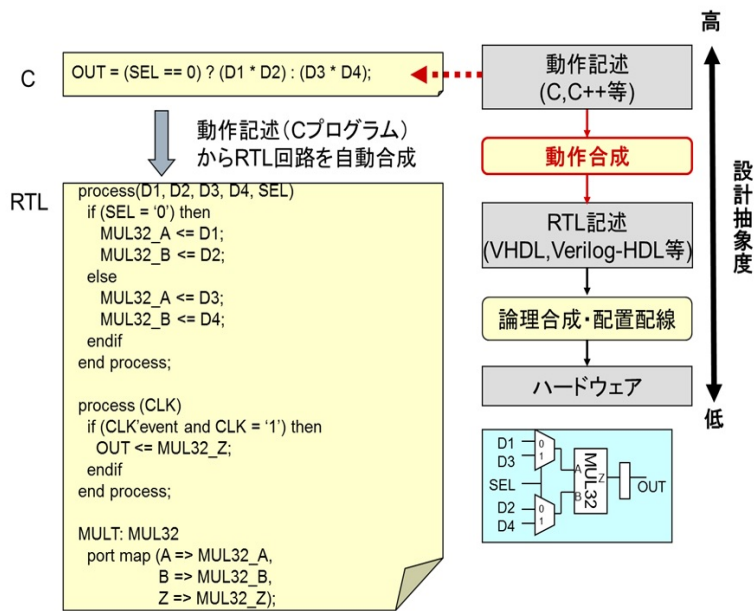


図4: CとHDLで同じ回路(2つの乗算演算)を設計した際の記述量の差

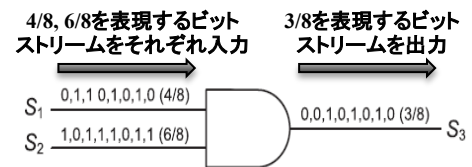
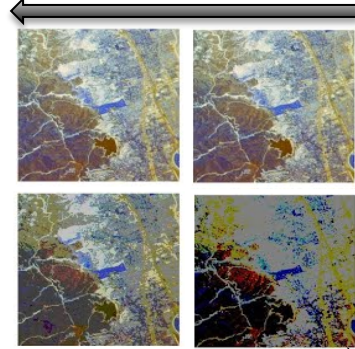


図5: Stochastic Computingの例 (1ビットANDゲートで8ビット乗算器を代替)

← 計算精度: 高 (計算時間: 長)



計算精度: 低 (計算時間: 短) →

図6: Approximate Computingを画像処理に適用した例

他分野のアプリケーション・アーキテクチャ設計へのCAD技術応用

HLSや論理合成を含む、組込みシステムを設計するための支援ソフトウェアをCAD (Computer Aided Design) と言う。CAD技術には、様々・複数の制約(製造コスト・性能・エネルギー・信頼性など)の下で、最適な設計を行うために、広い設計空間を効率的に探索するアルゴリズムがふんだんに盛り込まれている。

本研究室では、従来のCAD技術を新たなアーキテクチャ設計・アプリケーション最適化(パイオチップ設計(図7, 論文[2])など)、新たなCAD技術の問題解決(メニーコアのタスクマッピング(図8, 論文[3])など)に応用する研究・勉強を進めている。組込みシステム設計に限らず、我々の日常に存在する複雑な問題を、CAD技術の応用によってスマートに解決する。

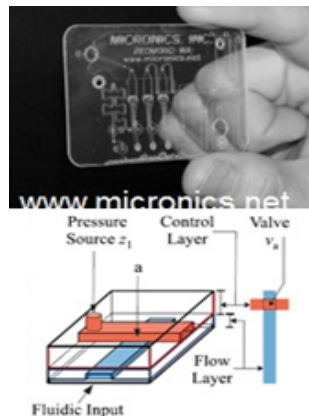


図7: バイオチップ設計(論文[2])

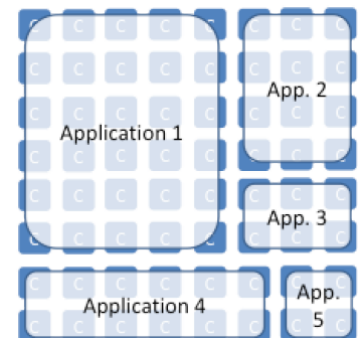


図8: メニーコアのタスクマッピング(論文[3])

3 関連する業績、プロジェクトなど

論文:

[1] Y. Hara-Azumi, T. Matsuba, H. Tomiyama, S. Honda and H. Takada, "Impact of Resource Sharing and Register Retiming on Area and Performance of FPGA-based Designs," IPSJ Transactions on System LSI Design Methodology, vol.7, pp.37-45, Feb. 2014.

[2] T. A. Dinh, S. Yamashita, T.-Y. Ho, and Y. Hara-Azumi, "Clique-Based Architectural Synthesis of Flow-Based Microfluidic Biochips," IEICE Transactions on Fundamentals of Electronics (Special Section on "VLSI Design and CAD Algorithms"), vol.E96-A, no.12, pp.2668-2679, Dec. 2013.

[3] J. Kaida, Y. Hara-Azumi, T. Hieda, I. Taniguchi, H. Tomiyama, and Koji Inoue, "Static Mapping of Multiple Data-Parallel Applications on Embedded Many-core SoCs," IEICE Transactions on Information and Systems, vol.E96-D, no.10, pp.2268-2271, Oct. 2013.

[4] T. Ahmed, J. Yao, Y. Hara-Azumi, S. Yamashita, and Y. Nakashima, "Selective Check of Data-Path for Effective Fault Tolerance," IEICE Transactions on Information and Systems (Special Section on "Reconfigurable Systems"), vol.E96-D, no.8, pp.1592-1601, Aug. 2013.

受賞: 情報処理学会山下記念研究賞 (2011), 情報処理学会優秀学生賞 (2008, 2012, 2013)

プロジェクト: JST PRESTO さきがけ「階層融合型機能的冗長化による次世代低電力デバイス向け高信頼化設計」, 2013.08~2017.03.