デジタル指紋符号の組合せ理論的新構成法に関する研究

著者	藤原 良叔
発行年	2018
URL	http://hdl.handle.net/2241/00158869

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　２２　日現在

機関番号：　１２１０２
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2017
課題番号：　２６４００１８６

研究課題名（和文）デジタル指紋符号の組合せ理論的新構成法に関する研究

研究課題名（英文）A Study on Combinatorial Construction of Digital Fingerprint Code

研究代表者
藤原　良叔（Fuji-Hara, Ryoh）

筑波大学・システム情報系（名誉教授）・名誉教授

研究者番号：３０１６５４４３

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：デジタル・コンテンツと呼ばれるデータに関して，一番大きな問題はそれらコンテンツの違法コピーを如何に防ぐかである．今研究されている方法に，利用者にはわからないように，識別コードを埋め込む方法がある．　このための符号を構成するために，新しい概念を導入し，構成した．
完全ハッシュ族(PHS)はデジタル指紋に使われる．強さ3，行数3のPHSの無限系列を構成した．そして強さ3，長さ3の分離可能符号について，サイズの上界を最適化理論に基づき導き，その上界に達成できる符号をPHSや組合せ的デザインにより構成した．またブロドキャスト暗号化の鍵不正配分を防ぐための方法についての最適符号も構成した．

研究成果の概要（英文）：Regarding data called digital content, the biggest problem is how to prevent illegal copying of those contents. There is a method to embed an identification code into the method being studied, so that the user does not know In order to construct the code for this purpose, a new concept was introduced and constructed.
We constructed the perfect hash families (PHS) which are used for digital fingerprints . They are infinite series of strength 3 and row number 3. For separable codes of strength 3 and length 3, upper bounds of size were derived based on the optimization theory, codes achievable in the upper bound were constructed by PHS and combinatorial design. We also constructed the optimum code for the method to prevent unauthorized key distribution of Broadcast encryption.

研究分野：　組合せ理論とその情報科学への応用

キーワード：　デジタル指紋符号　完全ハッシュ族　組合せ的デザイン　射影幾何　グループ検査

1. 研究開始当初の背景

(1) デジタル・コンテンツと呼ばれるデジタル音楽，書籍，映像，コンンピュータ・ソフトウェア等が普及しつつある．そんな中で，一番大きな問題はそれらコンテンツの違法コピーを如何に防ぐかである．今研究されている方法に，デジタル・コンテンツの中に，利用者にはわからないように，識別コードを埋め込む方法である．目的はたとえ複数人が結託したとしても，違法コピーされたものと判断できる，あるいは結託者達を追跡できるようにすることである．それらの目的を達成する符号を構成するのは難しい課題であるが，世界各地で研究が盛んである．この符号を構成するため，既存研究とは異なる，新しい概念を導入し，構成手法を新しく作り直すことを目的とする．

(2) デジタル・コンテンツへの識別コードの埋め込みは，0,1 値を，あるいは音量，色合い等のレベル値（整数値と解釈してよい）の情報に小さな値，0,±1，±2 を足しあわせ，利用者にはほとんど判別できない様な形でデータの埋め込みを行う．もちろん埋め込み場所はユーザには秘密である．そしてユーザごとに異なる値を埋め込む．コンテンツが２値で７ビットの場合を考えてみる．例えば，いま(0,0,1,0,1,0,0)という識別コードを埋め込むと，0 の所は変わらず，１の所はビットが反転する．利用者は当然どの場所に１があるかは知らない．もし一人のユーザが単独で違法コピーを作成したなら，その作成者は簡単に特定されてしまう．そこで当然，複数人が結託して，ユーザが特定されないようなコピーを作成しようと考えるであろう．いま二人のユーザ A,B がそれぞれコンテンツ

(1,0,1,1,0,1,0) と (1,0,0,1,1,0,0)

を持っているとする．この二つを比べると，第 3,5,6 ビットが異なり，他は同じである．このことから，A,B は識別コードは少なくとも第 3,5,6 ビットには埋め込まれていると推測する．すなわち，自分たちのコンテンツ以外で，考えられるコンテンツは

(1,0,0,1,0,0,0),(1,0,0,1,0,1,0),(1,0,0,1,1,1,0),
(1,0,1,1,0,0,0),(1,0,1,1,1,0,0),(1,0,1,1,1,1,0),

の６種類となり，その内どれかを作れば，それは違法コピーと判断されず，かつ作成者がわからないのではないかと考える．このとき結託者達の持っているコンテンツ X={A,B}を親(parents)といい，親および上の６個のコンテンツの集合を 子孫集合(descendant set)といい，desc(X)と書く．

(3) この子孫集合を使って，いくつかの違法コピーに耐性を持った符号が提議されている．C を識別コードを埋め込まれたコンテンツ全体とし，X,Y を異なる親の集合（共通部分があってもよい）とするとき，たとえば

① 任意の X, Y , X≠Y, |X|,|Y| ≤ t に対し，もし X≠Y なら desc(X)≠desc(Y) ，（t-separable code）
② 任意の X , |X|=t, に対し， desc(X)∩C = X , （t-frameproof code）
③ 任意の X, Y , X≠Y, |X|,|Y| ≤ t に対し，もし X∩Y=∅ なら desc(X)∩desc(Y)=∅, (t-secure frame-proof code)

等の符号が定義されている．これら子孫集合をもとに定義されている符号は デジタル指紋符号(Fingerprinting codes) と呼ばれている． このように，違法コピーかどうかの判定を目的とした「電子すかし」とは異なる概念である．また今までの「誤り訂正符号」とも全く異なり，集合論的に提議されているため，これまでのような代数的な手法が利用しにくい．しかし構成のための強力な手法が無いため，今までのところ，誤り訂正符号の中から，デジタル指紋符号の条件を満たす符号を見つける研究が殆どである．

２．研究の目的

(1) そこで我々は，符号の定義の基盤になっている子孫集合を集合ではなく，同値なひとつのベクトルとして表現するアイデアを考えた[1]．そしてそれらのベクトル同士の演算が出来るように，新しい可換環を定義した．２値の場合を考えよう．上の例の子孫集合を直積で表現すると

{1}×{0}×{0,1}×{1}×{0,1}×{0,1}×{0}

となり，{0,1}となっている３桁には全ての組合せが現れる．
これを次のようなベクトルにする．

dv(X)=(1,0,α,1,α,α,0)

{0,1}に対応する桁には不定元 α を代入する． このベクトルを子孫ベクト(descendant vector) と呼び，dv(X) と書く． そして A={ 0, 1, α, α+1 } の４つの元の上に加法 + と乗法 * の演算を持つ可換環を新たに定義した[1]．実際には子孫ベクトルは親が与えられたとき，その中の(0,1)ベクトルから演算によって求まる．

(2)このベクトルを使うと集合論的な関係が代数的な性質と対応できる．たとえば

1. x ∈ desc(X) ←→ dv(X)+x が 1 を含む．
2. x ∈ desc(X) → dv(X)*x = x
3. 任意の X, Y に対して desc(X)∩desc(Y)=∅ ←→ dv(X)+dv(Y) が 1 を含む
4. desc(X) ⊂ desc(Y) ←→ dv(X)*dv(Y)=dv(X) かつ dv(X)+dv(Y) は 1 を含まない
5. dv(X ∪ Y) = dv(X)*dv(Y) + alf(dv(X) + dv(Y))， alf は α をつける特殊関数．

といったように，集合関係が A 上の子孫ベクトルの演算で判定できる[1].

(3) このAの可換環は{0,1}に限れば2値の有限体と同値となっている．コンテンツは2値の有限体のベクトルとして扱えるため，そのベクトル達を有限射影幾何の点に対応することができる．これらの性質を使って，有限射影幾何を使って幾何的，代数的手法で各種のデジタル指紋符号を構成することを目的とする．

<引用文献>

[1] R. Fuji-Hara, Descendant Sets and Fingerprinting codes of Binary Case,submitted, The 11th International Conference on Finite Fields and their Applications, 2013年7月研究発表

[2] 藤原　良，備忘録：子孫集合と符号(ver 2.5)

３．研究の方法

我々のオリジナルの子孫ベクトル及び独自の可換環の理論を使って，デジタル指紋符号の構成を，今までとは全く異なる方法で行う．まずは最も基本の 2-separable code の構成する．そのために位数が2のn次元有限射影幾何 PG(n,2)の上で，*i*-line が存在しない最大部分空間を見つける研究をする．つぎに多値の場合の separable code の構成法を研究．特殊な条件を持ったLDPCや PHS と呼ばれる組合せ的構造が存在すれば，多値型 separable code が構成できることは証明した[2]．組合せ理論上の問題として条件付きLDPCやPHSの構成を行なう．

4. 研究成果

（1）デジタル・コンテンツと呼ばれるデジタル音楽，書籍，映像，コンピュータ・ソフトウェア等が普及しつつある．そんな中で,一番 大きな問題はそれらコンテンツの違法コピーを如何に防ぐかである．今研究されている方法に，デジタル・コンテンツの中に，利用者 にはわからないように，識別コードを埋め込む方法である．目的はたとえ複数人が結託したとしても，違法コピーされたものと判断で きる,あるいは結託者達を追跡できるようにすることである．この符号を構成するため，既存研究とは異なる，新しい概念を導入し， 構成手法を新しく作り直すことを試みている．

（2）位数2のn-1次元有限射影幾何PG(n-1,2)の上で，次元が d の i-line が存在しない部分空間（i-line free d-flat と呼ぶことにする)の 存在が証明できれば，2^{d+1}+1 個の語からなる 2-separable code が構成できることがわかっている．この方法が現在の所の唯一 の separable code のシステマティックな構成法である．d=n-2 の場合，i-line free の超平面は存在しないことを証明した．Hamming code の双対符号は Hadamard design と呼ばれる一種の組合せ的デザインの性質を持っていることが知られている，またこの符号は i-line free で部分空間にもなっている．この符号からいくつか(k 個)の座標を削除しても i-line free の性質は保っている．そのため，いまのところわかっている最大の i-line free d-flat は $n=2^m-2-k$ のときに次元が $d=2^{m-2}$ ，$0 \leqq k \leqq m-2$ である．この 系列よりも，できるだけ n に近い i-line free d-flat を見つける研究を行なった．

（3）完全ハッシュ族(PHS perfect hash family)はデジタル指紋だけでなく,他の情報科学の分野でもよく使われている．藤原（発表論文[1]）は有限幾何を用いて，強さ3,行数3の完全ハッシュ族の無限系列を構成した．

Cheng・Jiang・Li・繆・Tang（発表論文[2]）は強さ3，長さ3の分離可能符号について，サイズの上界を最適化理論に基づき導き，その上界に達成できる符号を完全ハッシュ族や Steiner triple system により構成した．

しかし，分離可能符号に基づいた不正ユーザー追跡アルゴリズムは，ユーザー数が分離可能符号の符号語数の上界を超える場合，或は不正ユーザー数がある限界を超える場合では，不正ユーザーを正しく追跡することができなくなる．この問題を解決するために，Jiang・Cheng・繆（発表論文[3]）や Cheng・Fu・Jiang・Lo・繆（発表論文[5]）は各々強分離可能符号やマルチメディア IPP 符号とよばれる符号を導入し，関連する不正ユーザー追跡アルゴリズムを開発した。極値グラフ理論を用いて，マルチメディア IPP 符号のサイズにおける上界を導いた．上界に到達する最適な強分離可能符号やマルチメディア IPP 符号を作行列や有限幾何などにより構成した．

Shangguan・Wang・Ge・繆（発表論文[6]）が組合せ論的・確率論的手法を利用し，frameproof 符号のサイズに関する tight な上界と下界を導いた．

５．主な発表論文等

〔雑誌論文〕（計7件）

[1] R. Fuji-Hara, Perfect hash, families of strength three with three rows from varieties on finite projective geometries, Designs, Codes and Cryptography 査読有 77, 351-356 (2015) DOI:10.1007/s10623-0052-z

[2] Cheng・Jiang・Li・Miao・Tang, Bounds and constructions for 3-separable codes of length 3, Designs, Codes and Cryptography 査読有, 81 317-335 (2016), DOI:10.1007/s10623-0052-z

[3] J. Jiang, M. Cheng and Y. Miao , Strongly separable codes, Designs, Codes and Cryptography, 査読有, 79 303-318 (2016), DOI:10.1007/s10623-015-0050-1

[4] H. Cai, Z. Zhou, X. Tang and Y. Miao , Zero-difference balanced functions with new parameters and their appli- cations, IEEE Transactions on Information Theory , 査読有, 63 4376-4378 (2017) DOI: 10.1109/TIT.2017.2675441

[5] M. Cheng, H.-L. Fu, J. Jiang, Y.-S. Lo and Y. Miao, Codes with the identifiable parent property for multimedia fingerprinting, Designs, Codes and Cryptography,査読有, 83, 71-82 (2017) DOI:10.1007/s10623-016-0203-x

[6] C. Shangguan, X. Wang, G. Ge, Y. Miao , New bounds 2-separable codes of length 2 (for frameproof codes), IEEE Transac- tions on Information Theory , 査読有, 63 7247-7252 (2017) DOI:10.1109/TIT.2017.2745619

[7] Y. Gu, Y. Miao, Bounds on trace- ability schemes , IEEE Transactions on Information Theory,査読有, vol. 64, pp. 3450-3460.(2018) DOI:10.1109/TIT.2017.2766659

〔学会発表〕(計 7 件)

① R. Fuji-Hara , Perfect Hash Families with Strength Three with Three Rows, Algebraic Combinatorics and Applications(招待講演) Michigan Technological University, Houghton, Michigan, USA, 2015 年 08 月 26 日~ 08 月 30 日
② Y. Miao , Xiangshan Business Hotel, Beijing, People's Republic of China , Workshop on Coding Theory and Cryptography(招待講演) 2016 年 07 月 02 日~07 月 08 日
③ Y. Miao Identification of non-zero coordinates in a sparse vector 現代分析とその応用研究集会(招待講演)(国際学会) 清華大学(中華人民共和国) 2016 年 08 月 03 日~08 月 03 日
④ Y. Miao , Separable codes and related tracing algorithms for multimedia fingerprinting , Workshop on Graph Theory and Combinatorics of Yangtze Delta(国際学会) 南京師範大学(中華人民共和国) 2016 年 04 月 15 日~ 04 月 17 日
⑤ 藤原 良, 超大容量通信・メモリー時代の符号を考える , 研究集会「実験計画法と符号および関連する組合せ構造」(招待講演) , 秋保リゾート ホテルクレセント(宮城県仙台市) 2016 年 11 月 28 日~ 11 月 30 日
⑥ Y. Miao , 電子指紋の組合せ理論, 日本数学会 2017 年度年会(招待講演) 首都大学東京 2017 年 03 月 24 日~ 03 月 27 日
⑦ 藤原 良, 深層学習の中の組合せ的デザイン問題,研究集会:実験計画法と符号および関連する組合せ構造(招待講演)(招待講演) 2017

６．研究組織

(1)研究代表者
藤原 良叔 (FUJI-HARA, Ryoh)
筑波大学・システム情報系・名誉教授
研究者番号： 30165443

(2)研究分担者
繆 瑩 (MIAO, Ying)
筑波大学・システム情報系・教授
研究者番号：10302382