

Title	Computing Methods for the Weight Distributions of Linear Block Codes and the Weight Distributions of the Extended Binary Primitive BCH Codes of Lengths 64 and 128
Author(s)	出崎, 善久
Citation	大阪大学, 1997, 博士論文
Version Type	VoR
URL	<a href="https://doi.org/10.11501/3129358">https://doi.org/10.11501/3129358</a>
rights	
Note	

*Osaka University Knowledge Archive : OUKA*

<https://ir.library.osaka-u.ac.jp/>

Osaka University

氏 名	出 崎 善 久
博士の専攻分野の名称	博 士 (工 学)
学 位 記 番 号	第 1 3 3 4 4 号
学 位 授 与 年 月 日	平 成 9 年 6 月 30 日
学 位 授 与 の 要 件	学位規則第 4 条第 2 項該当
学 位 論 文 名	Computing Methods for the Weight Distributions of Linear Block Codes and the Weight Distributions of the Extended Binary Primitive BCH Codes of Lengths 64 and 128 (線形ブロック符号の重み分布計算法, 及び符号長64, 128の2元原始拡大 BCH 符号の重み分布)
論 文 審 査 委 員	(主査) 教 授 都 倉 信 樹 (副査) 教 授 宮 原 秀 夫    教 授 柏 原 敏 伸    助 教 授 藤 原 融

## 論 文 内 容 の 要 旨

デジタル通信の発展に伴い、高速で信頼度の高い通信の要求が高まってきた。誤り検出/訂正符号はそれを実現するために必要不可欠である。特に、2元線形符号は実用上重要な符号のクラスである。2元線形符号の重み分布は、その符号の誤り特性を評価する上で重要である。例えば、2元線形符号を2元対称通信路で用いた場合の誤り見逃し確率は重み分布から容易に求めることができる。しかし、重み分布の公式は一部の符号のクラスについてしか知られておらず、計算量の小さい重み分布計算法も知られていなかった。

本論文では、まず線形符号に対する高速な重み分布計算法を提案する。この計算法は、符号のトレリスダイアグラム（以下、単にトレリスと言う）を用いる方法、及び符号のビット位置置換に対する不変性を利用した方法の2つからなる。提案した計算法を用いて、符号長64, 128の全ての2元原始拡大 BCH 符号の重み分布を求めた。また、この計算法を用いても重み分布計算が困難な短縮リード・ソロモン符号から得られる2元符号について、小さい重みの符号語数についての公式を導出し、誤り見逃し確率の上界、下界を導いた。

2章では、符号のトレリスを用いた重み分布計算法について述べている。この計算法では、トレリスの道をたどりそのラベル系列の重みを数えて重み分布を求める。線形符号の場合、トレリスの構造には規則性があり、それを利用することにより計算量を大幅に軽減できることを示した。この計算法の計算量は用いるトレリスのセクション分割に依存する。与えられたトレリスに対する計算量は容易に求めることができるので、いくつかのセクション分割の内から計算量の小さいものを選ぶことができる。例として、(128, 36) 2元原始拡大 BCH 符号を取り上げ、セクション分割の異なるいくつかのトレリスについて計算量の評価を行なった。

3章では、符号のビット位置置換に対する不変性を利用した方法について述べている。この方法では、重み分布を求めたい線形符号に対して、その線形部分符号の剰余類を同値類分割する。ある剰余類がビット位置置換によって別の剰余類に移る場合、それらの剰余類は同じ同値類に属する。分割で得られた各同値類についてその要素数と代表元の重み分布かわかれば、元の符号の重み分布を求めることができる。そのため、同値類に含まれる要素数や同値類数を効率的に求めることが重要になる。巡回群やアフィン群の場合に、それらに対する公式を導いている。

4章では、上で提案した方法を用いて、符号長64, 128の全ての2元原始拡大 BCH 符号の重み分布を求めた。求めた重み分布を用い、それらの符号を2元対称通信路上で誤り検出のみに用いた場合の誤り見逃し確率を計算した。その結果を用いて、通信路のビット誤り率に対する誤り見逃し確率の単調性を数値的に調べた。

既知の計算法で重み分布計算が困難な場合には、重み分布の一部から誤り見逃し確率の上界、下界を導出して評価する場合がある。5章では、短縮リード・ソロモン符号から得られる2元符号の小さい重みをもつ符号語数について考察している。生成多項式  $(X-\alpha)$  の場合に重み2の符号語数が原始元  $\alpha$  に依存しないことを示し公式を導いた。また、生成多項式  $(X-1)(X-\alpha)$  の場合に、重み4, 6の符号語数の上界を求めた。これらの結果を用いて、各生成多項式を用いた場合の誤り見逃し確率の上界、下界を与える式を導出し、それらがビット誤り率が比較的小さい場合にほぼ一致することが確認された。

## 論文審査の結果の要旨

本論文では、線形符号の効率的な重み分布計算法を提案し、それを用いて重要な符号のクラスである符号長64, 128の拡大 BCH 符号の重み分布を求めている。この計算方法では、線形符号のトレリス構造、及びビット位置置換に関する性質を利用して計算量を大幅に軽減している。2章では、符号のトレリスダイアグラムを用いた重み分布計算法を提案している。線形符号の場合、そのトレリスダイアグラムは規則的な構造をもつことが知られている。提案されている計算法では、その構造的特性を利用して計算量を大幅に軽減することに成功している。また、この方法の計算量を解析しその評価が容易であることも示されている。計算量はトレリスダイアグラムのセクション分割に依存するが、事前に計算量を評価することにより計算量が小さくなるトレリスダイアグラムを選択することができる。

3章では、符号のビット位置置換に関する性質を利用した重み分布計算法を提案している。線形符号はその線形部分符号の剰余類の直和となっており、各剰余類の重み分布を求めることができれば元の符号の重み分布を求めることができる。各剰余類間でのビット位置置換に関する不変性がわかっているならば、不変な剰余類についての重み分布計算が1回ですむので、計算量の大幅な軽減ができる。剰余類の不変性に関する研究としては例えば、リード・マラー符号の剰余類のアフィン置換に対する不変性の研究が知られている。本論文では、リード・マラー符号と拡大巡回符号の共通部分の剰余類のアフィン置換に対する性質を解析している。拡大 BCH 符号を適当にビット位置置換して得られる符号はリード・マラー符号を含んでいるので、ここで得られた結果を適用することができる。

4章では、上で提案した2つの方法を用いて符号長64, 128の2元原始拡大 BCH 符号の重み分布を求め、誤り見逃し確率の評価を行なっている。それらのうちには符号語数が  $2^{64}$  の符号も含まれており、提案した計算法の有効性を示す例となっている。BCH 符号は実用上重要な符号であり、それを用いた様々な誤り制御システムが検討されている。誤り見逃し確率は、実際のシステムで用いる符号を選ぶ基準の一つとなるが、ビット誤り率の値は正確に評価できないことも多く、システムの特性に応じた適当なビット誤り率の範囲での誤り見逃し確率の最大値が重要な尺度となる。本論文では拡大 BCH 符号のビット誤り率に対する誤り見逃し確率の単調性、最大値を評価し、いくつかの符号について単調でないことも明らかにしており、理論面でも実用面でも価値ある結果を得ている。2, 3章で提案した方法も含め、既知の計算法では重み分布計算が困難な場合は、重み分布の一部から誤り見逃し確率の上界、下界を求めて評価することができる。5章では、短縮リード・ソロモン符号から得られる2元符号の小さい重みをもつ符号語数を評価し、2元対称通信路で誤り検出のみを行なった場合の誤り見逃し確率の上界、下界を与える式を導出している。リード・ソロモン符号は VLSI のシグネチャ検査や、一般の通信路における接続符号化で実際に用いられており実用上極めて重要な符号である。いくつかの具体例についてビット誤り率が比較的小さいところで上界、下界がほぼ一致することを示している。

以上のように、本論文では線形符号の効率的な重み分布計算法を提案して、実用上重要ないくつかの符号について実際に重み分布を求めており、博士(工学)論文として価値あるものと認める。