

半導体レーザの周波数雑音特性と物理乱数生成への応用

前原 進也

新潟大学大学院

自然科学研究科 材料生産開発科学複合生産システム専攻

あらまし

半導体レーザは、ダイオードレーザやレーザダイオードとも呼ばれ、他の種類のレーザと比較した場合、小型・軽量、低電流・低電圧動作、安価、長寿命、高発光効率、直接変調が可能などの優れた特徴を持っている。このため半導体レーザは、光ファイバ通信の光源、CD・DVDなどの記録読み出し光源、レーザプリンタ用光源、バーコードリーダー、レーザポインタなどに広く応用されている。

しかしながら、半導体レーザには、強度雑音や周波数雑音といった量子雑音、モードホッピング雑音やモード分配雑音といった縦モードに関するレーザ自体の持つ本質的な雑音がある。また、外的要因による雑音として、レーザ駆動電流源やレーザ温度の変動による雑音、レーザ活性層への戻り光により誘起する雑音がある。それゆえ、半導体レーザの応用分野を拡大していくためには、これらの雑音を十分に把握し、改善を施していかなければならない。

半導体レーザを精密光計測や高分解能分光などに応用する場合、周波数は、温度や電流の変化により、大きく影響を受けやすく、フリーランニング状態の半導体レーザの周波数安定度は、 $10^{-8} \sim 10^{-9}$ 程度である。したがって、周波数安定度として 10^{-13} 程度が要求されるレーザ干渉計を用いた地球重力場の精密計測のような応用を行う場合には、レーザ周波数の安定化が必要となる。

半導体レーザの周波数は、その共振器長、共振器屈折率に依存するが、これらは温度や電流によって制御可能である。レーザの温度を制御する場合には、ペルチェ素子を利用した方法が用いられるが、応答速度は遅く、制御帯域は 1Hz 程度であるため、長時間の安定化に適している。一方、レーザの電流を制御する場合には、外部周波数基準を用いた電氣的負帰還制御が行われるため、応答速度が速く、温度の場合よりも広い帯域で高い安定度を得ることが可能である。これまでのところ、原子または分子の吸収線やファブリペローエタロンを外部周波数基準とした電氣的負帰還制御による実験は多数報告されており、最近では、半導体レーザの周波数安定度として、 10^{-14} 程度が実現できている。

一方で、このような雑音は積極的に応用される場合もあり、量子雑音を用いた例としては、新しいタイプの高分解能分光法が藪崎らによって報告されている。この分光法では、ダイオードレーザ、光周波数弁別器（原子の吸収線）、光検出器、スペクトラムアナライザを用いたシンプルなシステムで分光実験が行われており、レーザ光が原子の吸収線を介してゆっくりと掃引されるとき、透過光強度が大きな揺らぎを示すことが指摘されている。

この他の雑音の応用として、最近では、物理乱数を高速に生成するという研究が盛んに行われている。一般に乱数とは、等確率性と無規則性の 2 つの性質を併せ持つランダムな数の列のことであり、その生成方法により、疑似乱数と物理乱数に分類されている。乱数の応用としては、暗号鍵の生成、ゲーム、モンテカルロシミュレーションなどがあるが、これらの応用には、主に疑似乱数が使用されている。疑似乱数は 1 つの初期値と決定論的

アルゴリズムにより計算機上で生成できるので、安価で高速な乱数を容易に再現可能であるが、周期性が存在するため、高速計算が可能な時代の暗号化に使用するには不十分であると考えられる。これに対して、物理乱数は、ランダムな物理現象である雑音をセンサで検出してデジタル数値化することで生成できるため、再現性はなく周期性も存在しない。したがって、情報の安全性が十分に確保できると考えられる。物理乱数の生成のために利用される物理過程の例としては、放射性同位元素の崩壊、抵抗で発生する熱雑音、ツェナーダイオードのショット雑音などがある。しかしながら、これらを利用した物理乱数の生成速度は、最大で数 10～数 100Mb/s 程度であり、一般に疑似乱数の生成速度に比べて遅い。そこで、近年では半導体レーザの位相雑音測定や戻り光によって発生させたカオス波形を利用することで物理乱数を生成する研究が報告されており、その生成速度は最大で 300Gb/s にも及んでいる。

一方、本研究では、半導体レーザの発振スペクトルが瞬間的にはより狭いスペクトルとしてランダムに動き回っているのではないかと考えて、そのスペクトルを周波数弁別器を介して透過光強度信号に変換すれば、スペクトルのランダムな動きに応じた振幅揺らぎの信号が得られるとして実験を行い、3Gb/s の速度で物理乱数を生成することができた。

このように、本研究では、半導体レーザの雑音特性に着目して研究を行っており、本論文では、半導体レーザの周波数安定化に関する実験と半導体レーザの周波数雑音を用いた物理乱数の新しい生成法に関する実験について報告する。また、半導体レーザの周波数安定化を施した状態で、物理乱数を生成するという実験についても述べる。

目次

第1章 序論

第2章 半導体レーザの特性

- 2.1 レーザ
- 2.2 半導体レーザ
- 2.3 レート方程式
- 2.4 量子雑音
 - 2.4.1 強度雑音
 - 2.4.2 周波数雑音
- 2.5 スペクトル線幅
- 2.6 縦モードに関する雑音
 - 2.6.1 モード分配雑音
 - 2.6.2 モードホッピング雑音
- 2.7 戻り光雑音
- 2.8 レーザ光とコヒーレンス

第3章 周波数弁別器

- 3.1 Rb 原子の吸収線
 - 3.1.1 エネルギー準位
 - 3.1.2 スペクトルの広がり
- 3.2 飽和吸収分光

第4章 暗号と乱数

- 4.1 古典暗号
 - 4.1.1 単一換字式暗号
 - 4.1.2 多表式換字暗号
- 4.2 現代暗号
 - 4.2.1 共通鍵暗号
 - 4.2.2 公開鍵暗号
- 4.3 量子暗号
- 4.4 乱数
 - 4.4.1 疑似乱数
 - 4.4.2 物理乱数

第 5 章 直接変調方式によるレーザ周波数安定化

- 5.1 直接変調方式による安定化の原理
- 5.2 実験内容
- 5.3 実験結果
- 5.4 考察

第 6 章 外部変調方式によるレーザ周波数安定化

- 6.1 磁界変調方式による安定化の原理
 - 6.1.1 Faraday Normal 方式
 - 6.1.2 Faraday PEAK 方式
- 6.2 実験内容
- 6.3 実験結果
- 6.4 考察

第 7 章 物理乱数の生成

- 7.1 周波数雑音を用いた物理乱数生成の原理
- 7.2 物理乱数生成システム
- 7.3 実験結果と考察

第 8 章 周波数安定化時の物理乱数

- 8.1 実験方法
- 8.2 実験結果と考察

第 9 章 結論

第1章 序論

半導体レーザは、半導体中の電子の光学遷移による光子の誘導放出を利用した光波の発振器および増幅器の総称である。半導体レーザは、光励起や電子ビーム励起でも発振するが、pn 接合した半導体に電流を注入することによっても発振するため、ダイオードレーザやレーザダイオードとも呼ばれ、他の種類のレーザと比較した場合、

- ①小型・軽量：デバイス自体の大きさは 1mm^3 程度以下である
- ②低電流・低電圧動作：数 V の低い電圧で mA 領域の電流を注入するだけで駆動できる
- ③低価格：小型で層状の基本構造であるため、大量生産に適している
- ④長寿命：10 万時間程度と推定されている
- ⑤高発光効率：効率は数%から数十%ときわめて高い
- ⑥直接変調：電流に信号を重畳することで光の強度、周波数、位相を変調できる

などの優れた特徴を持っている^{(1), (2)}。このため半導体レーザは、光ファイバ通信の光源、CD・DVD などの記録読み出し光源、レーザプリンタ用光源、バーコードリーダー、レーザポインタなどに広く応用されている。

しかしながら、半導体レーザには、強度雑音や周波数雑音といった量子雑音^{(3), (4)}、モードホッピング雑音やモード分配雑音といった縦モードに関するレーザ自体の持つ本質的な雑音がある⁽⁵⁾。また、外的要因による雑音として、レーザ駆動電流源やレーザ温度の変動による雑音⁽⁶⁾、レーザ活性層への戻り光により誘起する雑音がある⁽⁷⁾。これらの雑音は、半導体レーザの光出力、光周波数、発振スペクトル幅に影響を及ぼす要因となる。それゆえ、半導体レーザの応用分野を拡大していくためには、これらの雑音を十分に把握し、改善を施していかなければならない^{(8), (9)}。

半導体レーザを精密光計測や高分解能分光などに应用する場合、高いスペクトル純度と周波数の安定性が重要となり、それらは測定感度や分解能に大きく影響する⁽¹⁰⁾。スペクトル純度については、市販の半導体レーザでも、縦・横単一モード発振が再現性よく得られ、スペクトル線幅が数 MHz 程度と理論値に近い特性が得られている。これに対してレーザ周波数は、周囲温度や電流のわずかな変化により、大きく影響を受けやすく、フリーランニング状態の半導体レーザの周波数安定度は、 $10^{-8} \sim 10^{-9}$ 程度である。したがって、周波数安定度として 10^{-13} 程度が要求されるレーザ干渉計を用いた地球重力場の精密計測のような応用を行う場合には、レーザ周波数の安定化が必要となる^{(11), (12)}。

半導体レーザの周波数は、その共振器長、共振器屈折率に依存するが、これらは温度や電流によって制御可能である。光周波数の変化量はレーザにより異なるが、例えば、温度に対しては -30GHz/K 、電流に対しては -5GHz/mA 程度となる⁽¹³⁾。レーザの温度を制御する場合には、ペルチェ素子を利用した方法が用いられるが、応答速度は遅く、制御帯域は 1Hz 程度であるため、長時間の安定化に適している。一方、レーザの電流を制御する場合には、外部周波数基準を用いた電氣的負帰還制御が行われるため、応答速度が速く、温

度制御の場合よりも広い帯域で高い安定度を得ることが可能である。これまでのところ、原子または分子の吸収線やファブリ・ペロー・エタロンを外部周波数基準とした電氣的負帰還制御によるレーザ周波数安定化実験が多数報告されている⁽¹⁴⁻³⁶⁾。

温度や電流による制御のほかに、ピエゾ素子を用いて外部共振器長を変えることにより周波数を制御する研究も報告されている⁽³⁷⁻³⁹⁾。この光帰還では、波長可変範囲の拡大や発振スペクトル幅の狭窄化が可能となり、500nm の範囲に及ぶ波長可変⁽⁴⁰⁾や数 Hz までの発振スペクトル線幅の狭窄化が実現されている⁽⁴¹⁾。

一方で、このような雑音は積極的に応用される場合もあり、量子雑音を用いた例としては、新しいタイプの高分解能分光法が藪崎らによって報告されている^{(42), (43)}。この分光法では、半導体レーザ、光周波数弁別器（原子の吸収線）、光検出器、スペクトラムアナライザを用いたシンプルなシステムで分光実験が行われており、レーザ光が原子の吸収線を介してゆっくりと掃引されるとき、透過光強度が大きな揺らぎを示すことが指摘されている。

この他の雑音の応用として、最近では、物理乱数⁽⁴⁴⁾を高速に生成するという研究が盛んに行われている⁽⁴⁵⁻⁶²⁾。一般に乱数とは、等確率性と無規則性の2つの性質を併せ持つランダムな数の列のことであり、その生成方法により、疑似乱数⁽⁶³⁾と物理乱数に分類されている。乱数の応用としては、暗号鍵の生成（ワンタイム・パッド暗号⁽⁶⁴⁾における使い捨て乱数）、ゲーム、モンテカルロシミュレーションなどがあるが、これらの応用には、主に疑似乱数が使用されている。

疑似乱数は1つの初期値と決定論的アルゴリズムにより計算機上で生成でき、安価で高速な乱数を容易に再現可能であり、線形合同法やM系列、メルセンヌ・ツイスタ法などがある。しかしながら、疑似乱数は、初期値やアルゴリズムを知られてしまうと、未来に出力される乱数列を容易に算出され再現されてしまう。また、生成した乱数列には周期性が存在するため、十分に長い乱数列を解析することで、アルゴリズムを推測されてしまうという脆弱性を持つ。このため、例えば、ランダムな鍵（文字列）を暗号文に使用するワンタイム・パッド暗号が必要とされる場合には、情報の安全性を保証するのは困難となる。

これに対して、物理乱数は、ランダムな物理現象である雑音をセンサで検出してデジタル数値化することで生成できるため、再現性はなく周期性も存在しない。したがって、十分な安全性が確保できると考えられる。物理乱数の生成のために利用される物理過程の例としては、放射性同位元素の崩壊、抵抗で発生する熱雑音、ツェナーダイオードのショット雑音などがある。しかしながら、これらを利用した物理乱数の生成速度は、一般に疑似乱数の生成速度に比べて遅い。そこで近年では、物理乱数の生成には、光もしくは光電子システムが使用されつつある。以下に、最近報告された物理乱数の生成法とその生成速度について示す。

①フォトンカウンティング検出器⁽⁶²⁾：68 Mb/s

②レーザの位相雑音^{(51), (52)}：500 Mb/s⁽⁵²⁾

③自然放出⁽⁵³⁾ : 12.5 Gb/s

④SLED⁽⁵⁶⁾ : 20 Gb/s

⑤半導体レーザカオス⁽⁴⁷⁻⁵⁰⁾ : 300 Gb/s⁽⁴⁹⁾

一方、本研究においても、半導体レーザの光出力変動を単に光検出することで物理乱数を生成⁽⁴⁶⁾するという実験を行ってきたが、現在では、より高速な物理乱数の生成速度を得るために、半導体レーザの周波数雑音に注目して物理乱数の生成^{(54), (55), (57-61)}を行っている。

半導体レーザの周波数雑音スペクトルは、自然放出による白色雑音や緩和振動周波数 (数 GHz) で共振状のピークを示し高域遮断するキャリア変動雑音、その他の外部雑音 (雰囲気温度や電流源) の影響などを含んでいる^{(3), (4), (9)}。全体としてみると、数 GHz までにわたってほぼ一様な雑音帯域が存在している。半導体レーザカオスに基づいた物理乱数は決定論的な性質のために、本質的にはランダムではないが、量子雑音は自然放出のランダムな性質に起因しているため⁽⁵²⁾、半導体レーザの周波数雑音は物理乱数の雑音源として適している。そこで本研究では、半導体レーザの発振スペクトルが瞬間的にはより狭いスペクトルとしてランダムに動き回っているのではないかと考えて、そのスペクトルを周波数弁別器を介して透過光強度信号に変換すれば、スペクトルのランダムな動きに応じた振幅揺らぎの信号が得られるとして実験を開始した。我々の物理乱数生成システムは、このような半導体レーザの持つ周波数雑音特性を利用し、かつ、取得データの並列処理を行うことで、生成速度を向上させることが可能な特長を持っている。現段階では、3 Gb/s の速度で物理乱数を生成することができている⁽⁶¹⁾。我々の知る限りでは、このような方法を用いた物理乱数の生成に関する報告はまだない。

このように、本論文では、半導体レーザの周波数安定化に関する実験と半導体レーザの周波数雑音を用いた物理乱数の新しい生成法に関する原理的提案について報告する。また、半導体レーザの周波数安定化を施した状態で、物理乱数を生成するという実験についても述べる。

以下、第 2 章では半導体レーザの雑音特性について考える。第 3 章では、周波数弁別器として用いられる Rb 原子の吸収線について述べる。第 4 章では、暗号と乱数の関係について述べる。第 5 章では、半導体レーザの周波数に直接変調を加え、飽和吸収分光法を用いた発振周波数安定化について述べる。第 6 章では、周波数基準に磁界変調を加えて発振周波数安定化を行う方法について述べる。これらの周波数安定化に対して、第 7 章では、半導体レーザの周波数雑音を積極的に利用して物理乱数を生成するという新しい応用について述べる。続いて、第 8 章では、半導体レーザの周波数安定化を行った状態で、物理乱数を生成し、フリーランニング状態で生成した物理乱数との評価を比較する。そして、第 9 章で本研究についてまとめる。

第2章 半導体レーザーの特性

2.1 レーザ⁽⁶⁵⁾

レーザー (LASER) は、Light Amplification by Stimulated Emission of Radiation (誘導放射による光の増幅) の頭文字から作った用語で、初期の段階では、可視光とその周辺の周波数領域のもののみを意味したが、その後あらゆる波長のものの総称となった。1958 年、タウンズとシャウローによって可能性が予測され、1960 年にメイマンがルビー・レーザーの発振に成功した。

Fig.2-1 のような準位構造の原子 (分子・イオンの場合もある) は、励起状態 b にあるときには振動数が

$$\nu_{ab} = \frac{(E_b - E_a)}{h} \quad (2.1)$$

の光を放射して基底状態 a に遷移する。この遷移は原子の周囲に光が存在しなくても起こるが (自然放出)、原子の振動数 ν_{ab} の光を入射すれば、この光に誘発されて原子は振動数 ν_{ab} の光を放射する (誘導放出)。誘導放出された光と入射光は、進行方向および位相が同じであるという特徴がある。強い誘導放出を起こさせる装置がレーザーである。

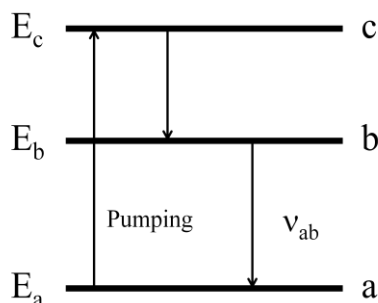


Fig.2-1 3 準位レーザーのエネルギー準位図

振動数 ν_{ab} の光は励起状態 b にある原子から振動数 ν_{ab} の光を誘導放出させるが、基底状態にある原子によって吸収されるので、振動数 ν_{ab} の強い光を作るためには、励起状態 b にある原子数を基底状態にある原子数より多くしなければならない。そのためには電子ビームをあてたり、別な振動数の強い光をあてることによって、基底状態にある原子をまず励起状態 c に遷移させる (ポンピング)。励起状態 c に励起された原子が、周囲にエネルギーを与えて励起状態 b にすぐ落ちる場合、 $a \rightarrow c \rightarrow b$ という過程によって、基底状態にある原子よりも励起状態 b にある原子の数を多くすることができる。このような反転分布の状態をつくるのがレーザー発振に必要な条件である。

反転分布が実現されている媒質を2枚の鏡（反射板）の間に置き、鏡の間隔は誘導放出される光の波長の整数倍になるように調整し、誘導放出された光が鏡で反射されて定在波をつくるようにしておく。ポンピングをつづけると、光は鏡の間を進行する間に誘導放出によって増幅され、これが鏡の反射によってさらに増加しつづけると発振現象を起こす。これをレーザ発振という。

レーザから発振される光は、非常によい指向性をもち、強度が強く、単色で位相が空間的にも時間的にもそろっているという特性をもっている。

2.2 半導体レーザ⁽⁶⁶⁾

1962年のほぼ同じころ、GE、IBM、MITの各研究所で、液体窒素温度（77K）に冷却したpn接合ガリウム・ヒ素（GaAs）に電流を流して、波長 $0.85\mu\text{m}$ の最初のパルス発振の半導体レーザが開発された。1970年にはアルフェロフ、林巖雄、パニッシュらによって、ダブルヘテロ接合構造の半導体レーザが開発され、室温連続動作に成功した。現在では半導体レーザといえば、このダブルヘテロ接合構造のレーザをさす。

ダブルヘテロ構造とは、異なる化合物半導体層（GaAsやAlGaAsなどのように2つ以上の元素からなる半導体層）を3層重ね合わせたもので、真ん中がバンドギャップの狭い発光層（GaAs）で活性層（ $0.1\mu\text{m}$ 程度）と呼ばれる。その上下を活性層よりもバンドギャップの少し広いp型AlGaAsとn型AlGaAsの半導体層（クラッド層）で抱き合わせた構造になっている。ファブリ・ペロー共振器は半導体結晶のへき開面を利用している。これでも半導体は高屈折率であるため、端面で35%程度の反射率を得ることができる。

この半導体チップに電流を順方向に流すと、p型とn型の接合部（活性層）には伝導帯電子と価電子帯正孔が多量に注入され、反転分布が形成される。Fig.2-2に示したように、高いエネルギー状態の伝導帯電子は低いエネルギー状態の価電子帯に遷移して正孔と再結合すると半導体中より光が放出される。活性層はクラッド層より、数%程度屈折率の高い材料で形成されているため、活性層内に光が閉じ込められる。さらに、注入電流を高め、励起を強くすると、誘導放出の割合が増し（増幅利得が増加）、利得が共振器の損失を超えるとレーザ発振が起こる。

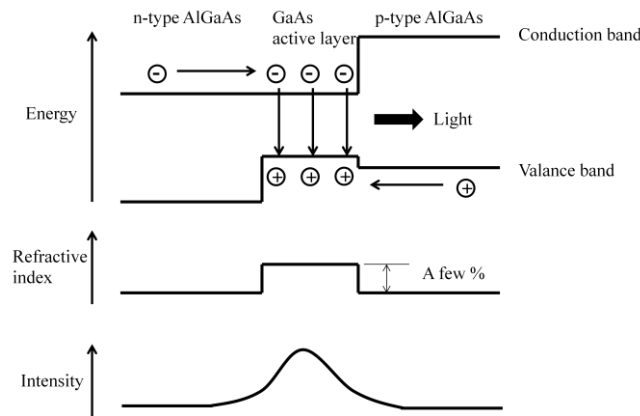


Fig.2-2 ダブルヘテロ構造のエネルギー状態、屈折率、光強度

2.3 レート方程式^(6,7)

半導体レーザの出力光パワーと電流注入ポンピングなどの関係を記述するのにレート方程式がよく用いられる。伝導帯および価電子帯における電子数密度を N_c [個数/ m^3] および N_v [個数/ m^3] とする。簡単のために、両エネルギー帯の幅の効果は考慮しないで、それぞれに 1 準位だけある 2 準位系とみなすことにする。この半導体中を伝搬する光子数密度 S [個数/ m^3] の時間的変化割合 $\partial S / \partial t$ の増加分は、以下のように表される。

$$\frac{\partial S}{\partial t} = (N_c - N_v)BS \quad (2.2)$$

ここで、 B [m^3/s] は誘導遷移確率である。また、光子の寿命時間 τ_p の共振器内にあるので、 $\partial S / \partial t$ の減少分は

$$\frac{\partial S}{\partial t} = -\frac{S}{\tau_p} \quad (2.3)$$

と書ける。式(2.2)、(2.3)から

$$\frac{\partial S}{\partial t} = (N_c - N_v)BS - \frac{S}{\tau_p} \quad (2.4)$$

が得られる。右辺第 1 項は誘導放出による光子数の増加の割合、第 2 項は共振器中での減少の割合を示す。 B [m^3/s] の物理的意味は、単位体積あたり、1 秒間に光子 1 個が入射し、1 個の電子を誘導遷移し、1 個の光子を放出する割合である。

一方、この誘導放出により、電子数密度 N_c が変化する。 N_c が時間的に変化する割合は、次式で与えられる。

$$\frac{\partial N_c}{\partial t} = -(N_c - N_v)BS - \frac{N_c}{s} + \quad (2.5)$$

右辺第 1 項は誘導放出または誘導吸収効果を、第 2 項は自然放出効果を表している。ポンプ項は単位時間あたりに注入された電子数密度であって、注入電流 I [A]、注入される体積を V_a [m³] とすれば

$$= \frac{I}{eV_a} \left[\left(\frac{\text{個数}}{\text{m}^3} \right) \cdot \left(\frac{1}{\text{s}} \right) \right] \quad (2.6)$$

となる。

式(2.4)、(2.5)は誘導放出による相互作用によって生じる光子数と電子数の時間的変化割合を示すレート方程式である。このレート方程式の物理的意味を Fig.2-3 に示す。

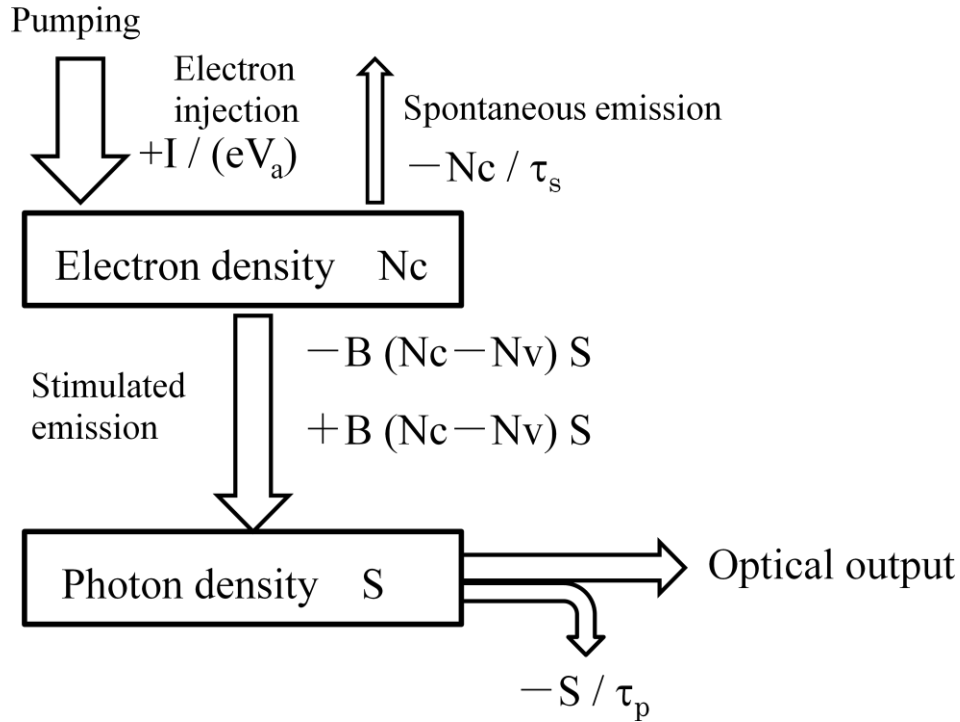


Fig.2-3 レート方程式の物理的意味の説明図

以上は、伝導帯および価電子帯にそれぞれ 1 つの準位しかないとみなして、2 準位系としての近似的な扱いであるが、実際には、両エネルギー帯は連続した多準位で構成されているので、すべての準位についての利得の和をとってレート方程式を解かなければ、実際の現象を記述したことにはならない。しかし、この近似的な取り扱いで、半導体レーザーの特性の大筋を把握することができる。

2.4 量子雑音 (5), (68)

量子雑音とは、自然放出に起因する雑音で、振幅が揺らぐ AM 雑音と、発振周波数が揺らぐ FM 雑音がある。Fig.2-4 に自然放出と AM 雑音、FM 雑音との関係を示す。自由空間中では、自然放出光の振幅、発光周波数、位相はランダムであり、そのため自然放出光が AM 雑音と FM 雑音の根本的な原因となる。FM 雑音は、自然放出からの直接的な影響の他に、AM 雑音からも次のような影響を受ける。光の振幅が揺らぐ AM 雑音によって、発光再結合に寄与するキャリア密度が変動を受け、キャリア雑音が発生する。この結果、自由キャリアプラズマ効果などによって半導体の屈折率が揺らぎ、共振波長が変動して、発振周波数が揺らぐ FM 雑音が生じる。また、AM 雑音が原因となって生じたキャリア雑音は、電流雑音も引き起こす。電流雑音によって、活性層で発生するジュール熱が変動するので、屈折率が変化し、FM 雑音につながる。一方、AM 雑音もそれ自身が引き起こしたキャリア雑音によって、発光再結合レートが揺らぐため、変化を受ける。このように量子雑音は、根本原因は自然放出であるが、相互に関係している。

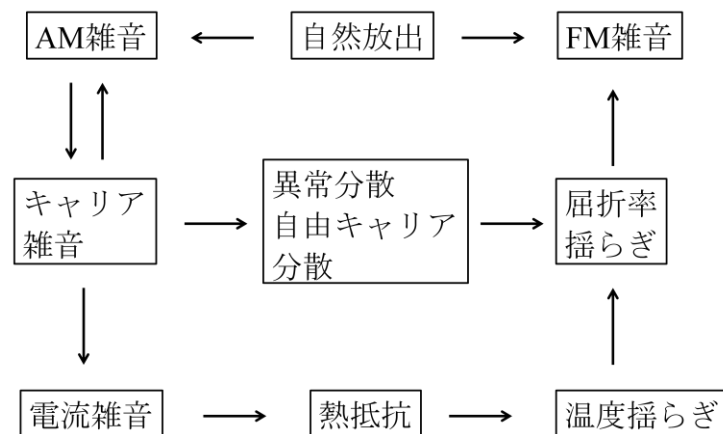


Fig.2-4 量子雑音

2.4.1 強度雑音 (AM 雑音)

半導体レーザからの出力強度を $S(t)$ とする。 $S(t)$ は直流的な成分 S_0 の他に揺らぎ成分を有しており、この揺らぎが強度雑音となる。強度雑音は次式の RIN (相対雑音強度) で評価される。

$$\text{RIN} = \frac{\langle S^2 \rangle}{S_0^2} \quad (\text{Hz}^{-1}) \quad (2.7)$$

ここで、 $\langle S^2 \rangle$ は揺らぎ相関の角周波数成分であり、次式のように $S(t)$ の自己相関の周波数成分として定義される。

$$\langle S^2 \rangle = \int_0 S(t_0) S(t_0 + \tau) e^{j\omega\tau} d\tau \quad (2.8)$$

また、出力 $S(t)$ を時間 t_0 を基準にフーリエ展開し、

$$S(t) = S_0 + \int_{-\infty}^{\infty} S_{\omega} e^{j\omega(t-t_0)} d\omega \quad (2.9)$$

と書くと、式(2.8)は

$$\langle S^2 \rangle = \int_{-\infty}^{\infty} S_{\omega} S_{\omega}^* d\omega \quad (2.10)$$

とも書かれる。

強度雑音の測定は、レーザからの出射光をそのまま光検出器（例えば、アバランシェフォトダイオード）で受光し、直流成分と交流成分に分け、交流成分をスペクトラムアナライザで測定する。光検出器からの出力電流が光強度 $S(t)$ に比例しており、スペクトラムアナライザの分解能を Δf (Hz) とすると、スペクトラムアナライザの画面上に描かれる出力は、 $\langle S^2 \rangle \Delta f$ となるので、その出力を Δf で割ったものが揺らぎ相関の周波数成分である。

2.4.2 周波数雑音（FM 雑音）

半導体レーザの周波数雑音は、自然放出光および屈折率ゆらぎによる光位相の変動が原因となっており、周波数雑音電力スペクトル密度で評価される。レーザ光の電界、位相および電子密度に関するレート方程式に自然放出によるゆらぎの項を表すランジュバン力をつけ加えることにより、周波数雑音電力スペクトル密度 $Q_{FM}(f)$ は次式のように求められる。

$$Q_{FM}(f) = \frac{(\delta f)_{ST}}{1 + \frac{2f_R^2}{(f_R^2 - f^2)^2 + (\frac{\gamma}{2})^2 f^2}} \quad (Hz) \quad (2.11)$$

ここで、 δf は電子密度変化に伴う屈折率変化により導入されるスペクトル線幅増大係数、 f_R はレーザの過渡的動作で観測される緩和振動周波数、 γ はその緩和振動のダンピング定数である。 $(\delta f)_{ST}$ はシャウロー・タウンズの式と呼ばれ、自然放出光が発振モード中にランダムな位相関係で混入することによる光周波数のゆらぎを表し、

$$(f)_{ST} = \frac{h}{8} \frac{n_{sp}}{p} \left(\frac{c}{n_r L} \right)^2 \quad (\text{Hz}) \quad (2.12)$$

で与えられる。ここで、 h は光子のエネルギー、 c は真空中の光速、 P はレーザ共振器内の光電力、 n_r はレーザ媒質の屈折率、 L はレーザ共振器長、 p は光子寿命である。 n_{sp} は自然放出と誘導放出の発生比で与えられる自然放出光因子 ($n_{sp} = 1.5 \sim 2.5$) である。周波数雑音スペクトルは緩和振動周波数 f_R で共鳴状のピークを持つ特性となること、光電力 P が大きいほど周波数雑音レベルは小さいことがわかる。

2.5 スペクトル線幅⁽¹⁾

半導体レーザが単一モード定常発振している場合でも、光周波数は完全に単一の定数ではなく揺らいでいる。したがって光波の周波数スペクトルも鋭いピーク状ではあるがデルタ関数ではなく、有限のスペクトル線幅をもっており、これは周波数雑音と密接な関係にある。半導体レーザでは、他の多くの種類のレーザと異なり、活性領域に高密度のキャリアが存在してその密度揺らぎが屈折率揺らぎを誘起し発振スペクトルに影響を及ぼす。このため半導体レーザのために修正されたシャウロー・タウンズの式を用いることで、発振スペクトル線幅 $\delta\omega$ は以下のように記述される。

$$\delta\omega = (n_{sp} / 2\tau_{ph} V_a S) [1 + \alpha^2] \quad (2.13)$$

ここで、 n_{sp} は自然放出光係数、 τ_{ph} は光子寿命、 V_a は活性領域の体積である。また、 α は線幅増大係数やアルファパラメータと呼ばれ、上式は、半導体レーザ中の自然放出ゆらぎの効果が屈折率ゆらぎにより α^2 倍に拡大されたものが線幅に加わることを示している。 α は通常 1 より大きいから屈折率ゆらぎが線幅を支配することになる。線幅 $\delta\omega$ は光子密度 S に反比例すなわち出力パワーに反比例して狭くなるが、多くの半導体レーザの定格出力時の $\delta\omega$ は数 MHz オーダである。しかし、内部損失 α_{int} を小さく、共振器長 L と端面反射率 R_f 、 R_b を大きくすれば光子寿命 τ_{ph} を長くできる。また、QW 構造を用いれば DH 構造より α を低減できる。さらにしきい値キャリア密度を高めれば、 n_{sp} と α を小さくできる。このような方法により、サブ MHz の線幅の QW レーザが実現されている。

2.6 縦モードに関する雑音⁽⁵⁾

2.6.1 モード分配雑音

モード分配雑音は、利得導波型の多モードレーザや、パルス変調によって多モード発振しているレーザにおいて、個々の縦モードを選択したときに観測される雑音である。光出

力全体の雑音は、単一縦モードレーザの雑音と同じであるが、個々の縦モードの雑音は非常に大きくなる。したがって、モード分配雑音は、モード選択性のあるシステム（例えば、光ファイバ通信システムでは、光ファイバの分散のためにモード選択性が生じる）で特に問題となる。また、この雑音は、低周波ほど大きい。モード分配雑音は、多モード発振時にトータルの光出力がランダムに各モードに分配されるために生じるので、モード分配雑音を抑制するには、半導体レーザを単一縦モード化すればよい。

2.6.2 モードホッピング雑音

モードホッピング雑音は、単一モードで発振しているレーザにおいて、温度、電流などの駆動条件によって、縦モードが他のモードにホップし、このとき複数のモードが競合して生じる雑音である。モードがホップする際に、2本以上のモードが交互にランダムな発振を繰り返し、各々の光出力がわずかに異なるために雑音が大きくなる。2本のモードが競合するときは、50MHz程度以下の低周波雑音であるが、3本以上のモードで競合するときは、高周波まで雑音が大きい。また、モードホッピング雑音が生じるときは、モード分配雑音も大きい。

モードホッピング雑音の原因は、自然放出光の揺らぎと、光利得の発振モードへの集中である。この雑音を避けるためには、単一縦モード化と多モード化の2種類の方法がある。

単一縦モード化については、過飽和吸収体を利用した双安定レーザや動的単一縦モードレーザを用いる方法がある。双安定レーザは、電流－光出力特性に大きなヒステリシスがあるため、モード間の競合が起きにくいという特長がある。しかし、双安定レーザは、変調時に大きな消光比を保ちながら安定な縦モード動作を得ることが難しいので、動的単一モードレーザの範疇には入らない。

モード選択性のないシステム（例えば、コンパクトディスク）では、多モード化も、モードホッピング雑音を低減する上で有効な手段である。多モード化により、雑音レベルは単一縦モードの安定した状態より大きくなるが、温度変化に対して安定となり、雑音レベルの最大値が低減される。多モード化の方法としては、高周波重畳、セルフパルセーション、利得導波構造の採用などがある。高周波重畳とは、直流バイアスに600MHz以上の電流パルスを重畳する方法で、電流の最小値が発振しきい値以下になるようにする。こうすることで、光出力はパルス状になり、過渡的に広い範囲で利得が損失を上回るので、多モード発振する。一方、過飽和吸収体を用いれば、素子自体でパルス状発振を行うセルフパルセーションを実現することができ、この時も多モード発振となる。また、屈折率導波構造と利得導波構造の中間の構造で、安定にパルス状発振が実現できる領域があることも報告されている。多モード化した場合、レーザ光のコヒーレンスが低くなるので、後述するように戻り光に対しても安定となり、光ディスクへの応用では有力な方法である。

2.7 戻り光雑音 (5)、(68)、(69)

戻り光雑音は、半導体レーザから出射した光が外部にある光学系によって反射されレーザ自身へ戻るために発生する雑音である。戻り光雑音の発生メカニズムとしては、「コヒーレント崩壊」現象による説明が有名である。これは戻り光の混入によりレーザ内の電子密度が不規則に変動して過剰雑音になるというモデルであり、出射光に対する戻り光の率が 10^{-4} 以上で発生する。しかし、実験的には戻り光率が 10^{-6} 以下でも雑音が発生しており、このモデルだけでは十分な説明が出来ない。

戻り光により「カオス状態」になるとするモデルも提案されている。カオス本来の意味は「混沌」であるが、研究の進展によりカオス現象にもいくつかの規則が示されている。しかし、カオス状態になるためにも戻り光率が 10^{-3} 以上は必要である。

戻り光率が 10^{-6} 以下でも生ずる過剰雑音の説明としては、反射点とレーザとで形成する外部共振器モードと発振モードのモード競合を原因とするモデルが存在する。先に述べたモードホッピング現象はモード競合が強くなった場合の現象であるが、モードホッピングに至らず、発振モードが安定に見える状態でも、モード間の相互作用のために雑音が増加している。Fig.2-5 のような配置を考えた時、外部共振器モードが生じはじめる戻り光率 Γ_c は、

$$\Gamma_c \cong 22R_2 \left[\frac{n_r L}{l(1-R_2)} \right]^2 / \quad (2.14)$$

となる。ここで、 L はレーザ共振器の長さ、 l はレーザと反射点との距離、 R_2 はレーザ共振器出射端側の電力反射率、 n_r は活性領域での屈折率、 η はレーザ端面に達した戻り光が活性領域へ結合する比率である。

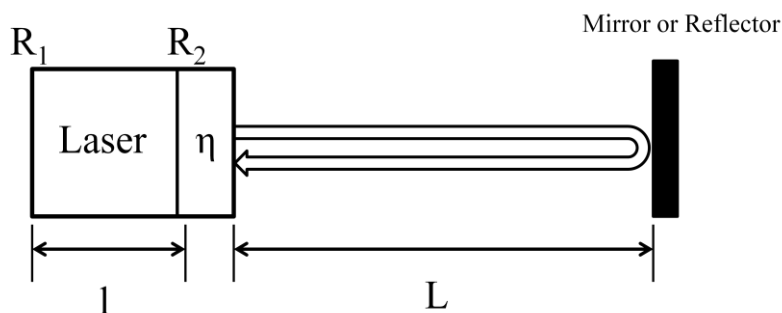


Fig.2-5 光フィードバックの概略図

2.8 レーザ光とコヒーレンス (67)、(70)、(71)

2 つに分けた波がよく干渉することをコヒーレントであるといい、ほとんどまたは全然干渉しないことをインコヒーレントであるという。時間的コヒーレンスは、波の周波数の単一性 (あるいは単色性) や、波束の連続性を表すもので、Fig.2-6 にその説明を示す。Fig.2-6(a)

の完全にコヒーレントな光は単一周波数の連続波を指し、周波数スペクトルで表すと 1 本の線スペクトルとなる。これに対して、いろいろな波長を含むか、短い波束の波がランダムに重なり合っている Fig.2-6(d) のような波はインコヒーレント光である。実際には、Fig.2-6(a) のような完全なコヒーレント光を得るのは難しく、Fig.2-6(b) のようにある時間内では単一周波数ではあるが波束の長さが有限な場合や、わずかな振幅ゆらぎや位相ゆらぎのある Fig.2-6(c) のような波が実際上のコヒーレント光といえる。

Fig.2-6(c) のような場合において、一定周波数の放射持続時間を Δt 、周波数スペクトル幅を Δf とすると、フーリエ変換の性質から、

$$\Delta t \cdot \Delta f \cong 1 \quad (2.15)$$

なる関係が成り立つ。このとき、時間的コヒーレンスの度合いを表す実的な量として用いられるコヒーレンス長 L_c は、およそ次式で与えられる。

$$L_c = c\Delta t = \frac{c}{\Delta f} \quad (2.16)$$

式(2.16)を用いると、ある光源の Δf がわかれば、およそのコヒーレンス長 L_c を評価できる。

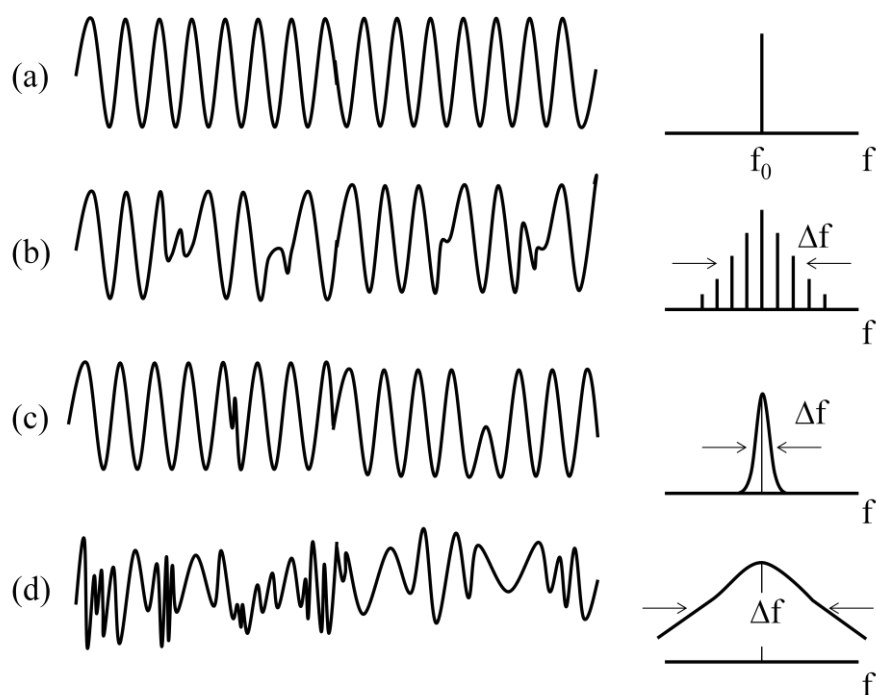
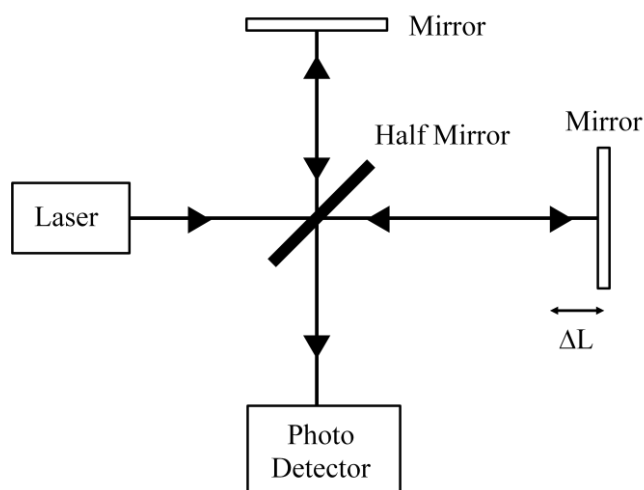


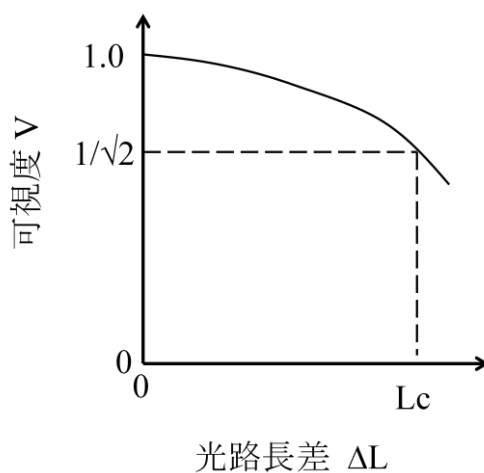
Fig.2-6 コヒーレンスの異なる光波の時間波形と周波数スペクトル

L_c は可干渉距離であり、Fig.2-7(a) に示すマイケルソン干渉計を用いて測定することができる。例えば、2 つの干渉アームの光路差 ΔL が 0 となるように 2 つのミラーの位置を設定

する。次に、一方のミラーを固定し、他方のミラーを移動させて ΔL を変え、光検出器で干渉光の可視度 V を測定する。Fig.2-7(b)に示すように、 ΔL を増すにつれて V は低下し、一般に $V = \sqrt{1/2}$ となる光路差 ΔL を光源のコヒーレンス長 L_c とする。



(a) マイクエルソン干渉計



(b) 可視度

Fig.2-7 コヒーレンス長の測定

また、空間的コヒーレンスの度合いは、光源から放射される光ビームの指向性および集光性に関する。コヒーレンスの高いレーザビームは優れた指向性を持っている。実際には、回折によって光ビームはほぼ (波長) / (ビーム径) の広がり角を持つ。これに対して、白熱電球のようなインコヒーレント光源では、ビームは発光面全体から四方に放射され、周波数、位相、振幅の異なる光波が同時に放射されるので、その波面は複雑にゆがんでいる。

第3章 周波数弁別器

この章では、半導体レーザの発振周波数安定化を行う際に必要となる外部周波数基準について述べる。周波数基準として良く用いられるものにファブリ・ペロー干渉計や原子・分子の吸収線がある。前者は、共振周波数の選択範囲が広いという利点を持ち、短時間領域の安定化のための周波数基準として用いられている。しかしながら、周波数の絶対値が不確実であり、周囲の温度変動によって共振周波数が変化してしまうという欠点もある。一方後者では、原子などのエネルギー準位は物理的に決まっているため経年変化しないものと考えられるので長期的に安定な周波数基準と成り得る。周波数基準は、光周波数の揺らぎを光強度のゆらぎへと変換する素子であるため、周波数弁別器とも呼ばれる。本研究では、この原理を利用して物理乱数を生成する際にも用いられている。

3.1 Rb 原子の吸収線

3.1.1 エネルギー準位

ルビジウム(元素記号 Rb)は原子番号 37、原子量 85.5 のアルカリ金属の一つである。自然界には質量数が 85 と 87 の同位体がそれぞれ 72%、28%の割合で存在し ^{85}Rb 、 ^{87}Rb と表される。

原子の最外殻電子が基底状態から励起状態に遷移する際に、二つのエネルギー差に相当する波長の光を吸収する。Rb 原子の場合は最外殻電子を 5s 軌道に持ち、この最外殻電子が 5p 軌道に遷移することにより強い吸収が起こる。さらに 5s 軌道と 5p 軌道はそれぞれ異なるエネルギー準位に分離しているため、吸収される波長の光がいくつも存在する。このため、吸収スペクトルは一本だけでなく何本も存在する。

電子は原子核の周りを回っていて、軌道は軌道角運動量 L で表される。5s 軌道は $L = 0$ 、5p 軌道は $L = 1$ である。また、電子は核の周りの回転による角運動量の他にそれ自身の軸の周りの角運動量を持っており、これを電子スピン S と呼ぶ。 L と S との合成角運動量 J は 5s 軌道では $J = 1/2$ 、5p 軌道では $J = 1/2, 3/2$ となり、5p 軌道は二本のエネルギー準位に分離する。従って Rb 原子には、 $5s_{1/2}$ から $5p_{1/2}$ へと、 $5s_{1/2}$ から $5p_{3/2}$ への二つの遷移が存在するため 2 種類の異なった吸収線が現れ、それぞれ D_1 線 ($\lambda = 794.76\text{nm}$)、 D_2 線 ($\lambda = 780.02\text{nm}$) と呼ばれている。さらに原子核もまたそれ自身の軸の周りの角運動量を持っており、これを核スピンという。この核スピンによる付加角運動量 I は同位元素によって異なる値を持ち、 ^{85}Rb 原子は $I = 5/2$ 、 ^{87}Rb 原子は $I = 3/2$ である。よって、それぞれの同位体での全角運動量 $F = J + I$ の値が異なる状態にわずかなエネルギー差ができるため、エネルギー準位が $5s_{1/2}$ で 2 本、 $5p_{3/2}$ で 4 本、 $5p_{1/2}$ で 2 本に分離する。この核スピンを考慮に入れた構造は超微細構造と呼ばれている。これらの分離の様子を Fig.3-1(a)、(b)に示す。

また、異なる準位間の遷移は、選択規則によって制限を受ける。 ΔL 、 ΔJ 、 ΔF はそれぞれの遷移に対する変化量であり、これ以外の遷移は禁止される。この選択規則は次のよう

になっている。

[選択規則]

$L: \Delta L = +1, -1$

$J: \Delta J = 0, +1, -1$ (ただし、 $J=0 \rightarrow J=0$ への遷移は禁止)

$F: \Delta F = 0, +1, -1$ (ただし、 $F=0 \rightarrow F=0$ への遷移は禁止)

この選択規則により、Rb 原子の吸収スペクトルは D_1 線が質量数 85 で 4 本、質量数 87 で 4 本の合計 8 本が現れ、 D_2 線では質量数 85 で 6 本、質量数 87 で 6 本の合計 12 本が現れる。

Fig.3-2 に Rb- D_2 線の吸収スペクトルの相対位置と相対強度を示す。

このようにして得られた理論的なスペクトルは線スペクトルであるが、実際に観測されるスペクトルは広がりを持っている。この広がりについては 3.1.2 で述べる。

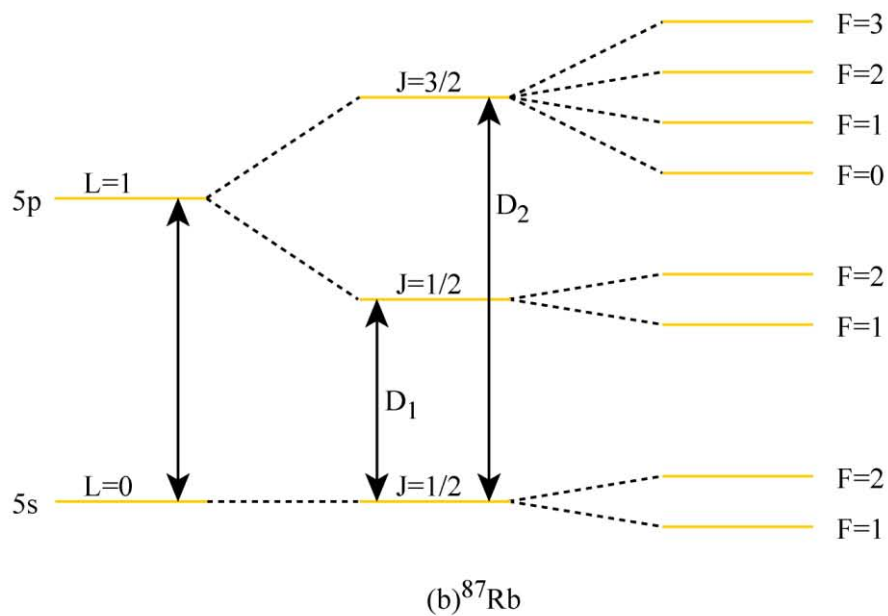
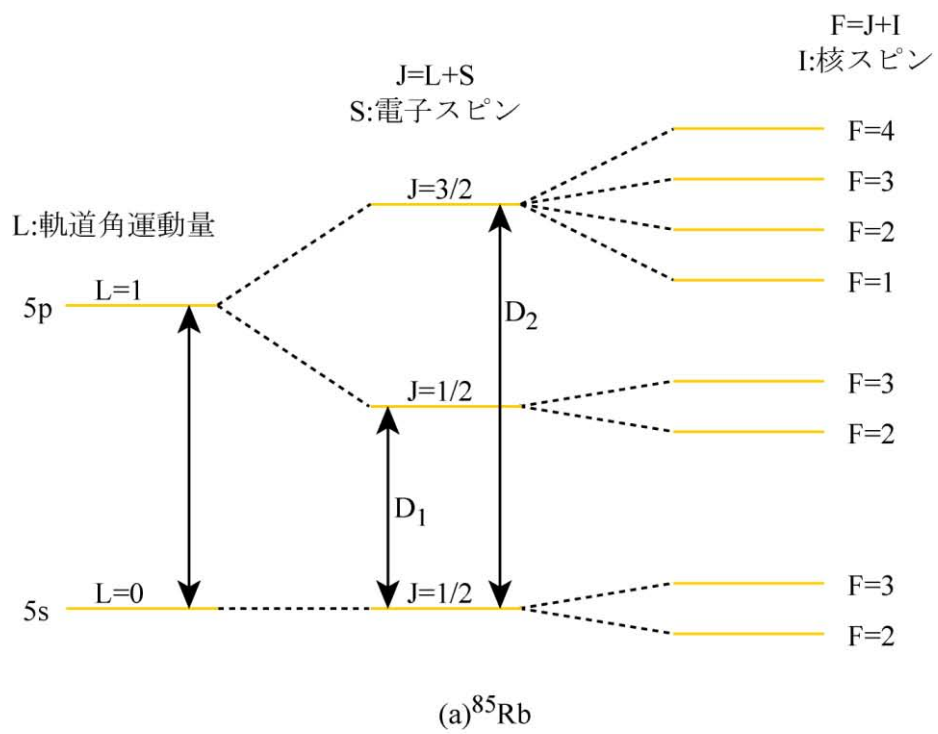
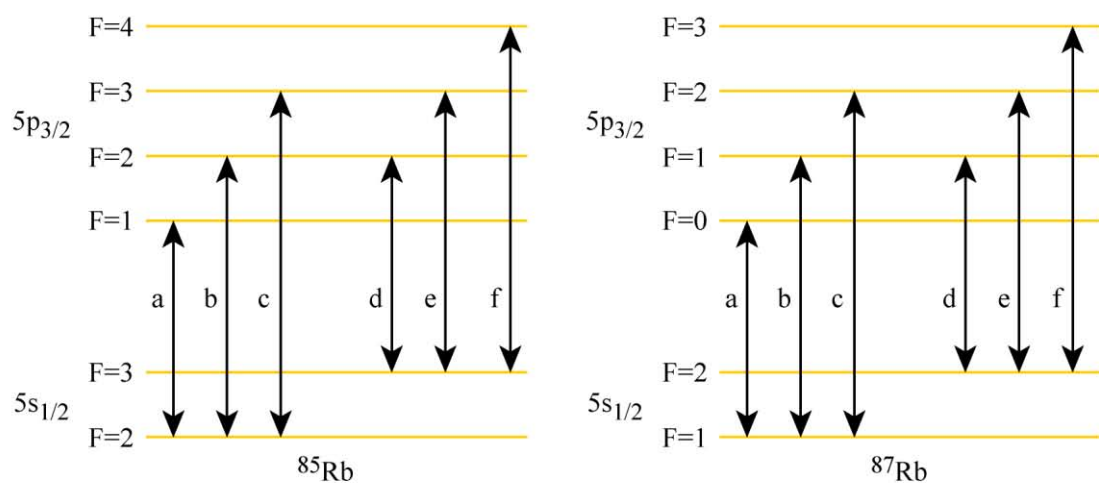


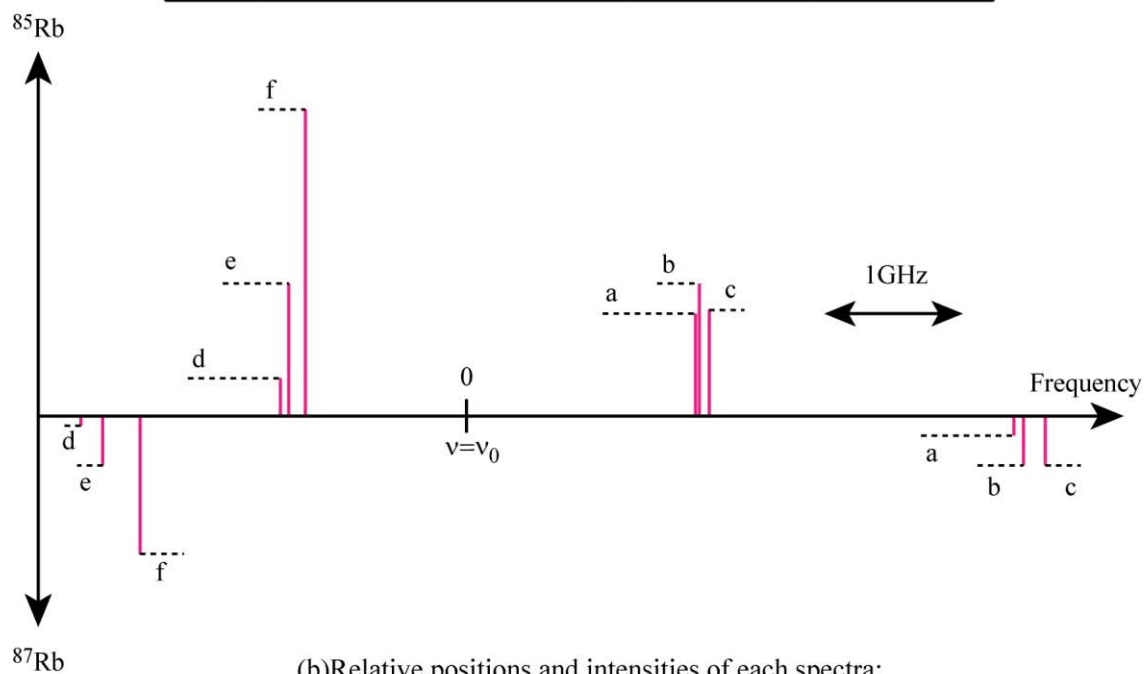
Fig.3-1 Hyperfine structures of Rb absorption lines.

図3-1 Rb原子の超微細構造



(a)Energy levels and transitions:エネルギー準位と遷移

遷移	^{85}Rb		^{87}Rb	
	$\nu-\nu_0$ [GHz]	相対強度	$\nu-\nu_0$ [GHz]	相対強度
a	1.66	33.4	3.97	6.40
b	1.69	43.2	4.04	16.1
c	1.76	34.6	4.20	16.1
d	-1.35	12.3	-2.80	3.20
e	-1.29	43.2	-2.64	16.1
f	-1.17	100.0	-2.37	45.0



(b)Relative positions and intensities of each spectra:
相対位置と相対強度

Fig.3-2 Relative positions and Relative intensities of Rb- D_2 absorption lines.

図3-2 Rb- D_2 吸収線の相対位置と相対強度

3.1.2 スペクトルの広がり

ここでは吸収のスペクトルの幅 Δ を与える要因、さらにそのスペクトルの広がりの特徴について述べる。スペクトルの均一な広がり、各々の粒子が外部から統計的に共通な摂動を受けて遷移の上側や下側のエネルギー順位の平均寿命が有限となるために生じるもので、すべての粒子が互いに識別できない様な同じ形の一様に広がったスペクトルを有している場合に観測される。このときのスペクトルの幅はこの寿命時間の長さによって決まる値を持つ。また、共鳴周波数 ν_0 も擾乱により変化する可能性があるが、もし全原子がほぼ同一の擾乱を受けていれば、これらの値は全電子の対して同一で、各電子は等しいスペクトルを持ち互いに区別できない。このような区別できないスペクトルの重ね合わせによって得られる全体のスペクトルは均一広がりを有するといい、そのスペクトルの幅を均一幅という。

均一幅を与える要因の一つとして原子間の衝突がある。これによる幅を衝突幅 Δ_D といい、気体の場合にはその圧力に比例する。衝突がないとしても電子は有限な寿命時間の後にはそのエネルギー準位から他へ遷移する。この時間はその遷移に伴う自然放出の発生確率に逆比例する。これを自然寿命と呼ぶ。これによって決まる均一幅を自然幅 Δ_N と呼び、これは均一幅を与える最も根本的な要因である。

一方、各原子がそれぞれ少しずつ異なる擾乱を受けていると式の Δ_0 の値は少しずつ異なってくる。これらの重ね合わせとして得られるスペクトルは均一広がりの場合とは違った形状となり、これを不均一広がりという。両者の比較を Fig.3-3 に示す。不均一な広がりを与える要因としては、結晶のゆがみのために電子の受ける外力が場所によって異なることによるもの、気体中の原子の熱運動によるドップラー効果によるもの、などがある。ここではドップラー効果による吸収スペクトルの不均一広がりについて考える。原子が熱運動によって真空中を飛び回っているとすると、ここで、光の進行方向の原子の速度成分を v とすれば、入射する電磁波の周波数 ν はこの原子から見るとドップラー効果のためにずれており、

$$\nu' = \nu \left(1 - \frac{v}{c}\right) = \nu - \frac{v}{\lambda} \quad (3.1)$$

となる。 λ は電磁波の波長である。従って原子中の電子は式によると $\nu = \nu_0$ ではなく $\nu' = \nu_0$ なる電磁波に対して共鳴する。つまり、

$$\nu = \nu_0 + \frac{v}{\lambda} \quad (3.2)$$

となる。この式は電磁波から見ると各電子の共鳴周波数が原子の速度成分 v の値によって決まる、異なった値を持つことを意味している。このことにより、少しずつ周波数のずれた吸収スペクトルが多数集まって、全体として 1 本の広がったスペクトル線を作る。各原

子の速度成分は全て同一ではなくマクスウェル分布に従うことはよく知られている。すなわち速度成分が v と $v+dv$ の間にある原子の数は、

$$N(v)dv = \frac{N_0}{\sqrt{\pi}u} e^{-\frac{v^2}{u^2}} dv \quad (3.3)$$

である。ここで N_0 は全原子数、 u は最確速度であり気体の温度 T 、原子の質量 M 、ボルツマン定数、 $k_B=1.38 \times 10^{-23} \text{J/K}$ によって、

$$u = \sqrt{\frac{2k_B T}{M}} \quad (3.4)$$

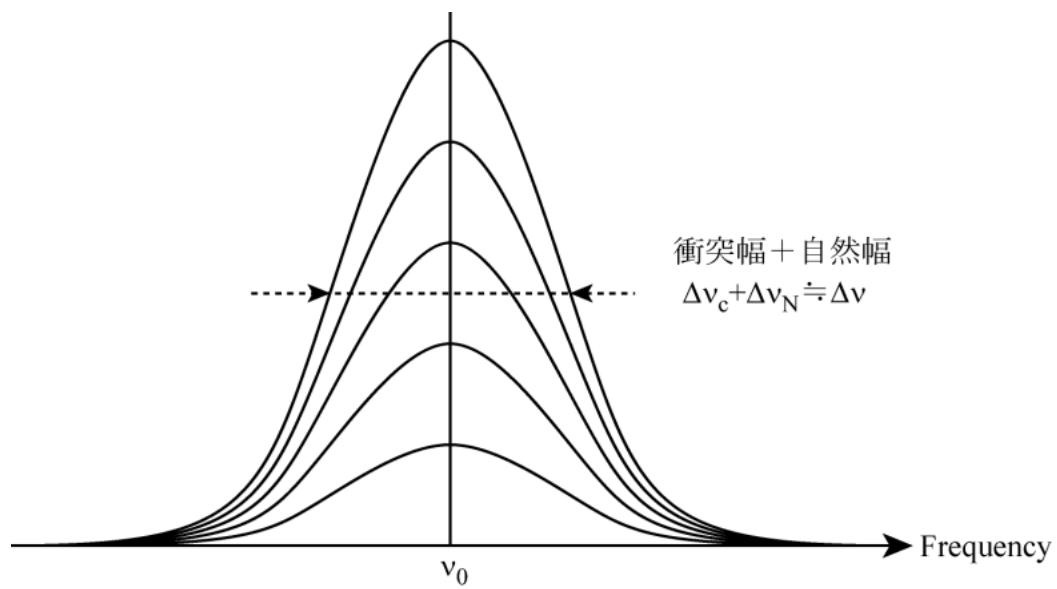
と表される。式(3.2)より $v = (v_0 - \nu)\lambda$ を式(3.3)に代入するとドップラー効果による不均一幅を持つスペクトルとして

$$g(\nu) = \frac{\lambda}{\sqrt{\pi}u} \exp \left[- \left(\frac{\nu - \nu_0}{u/\lambda} \right)^2 \right] \quad (3.5)$$

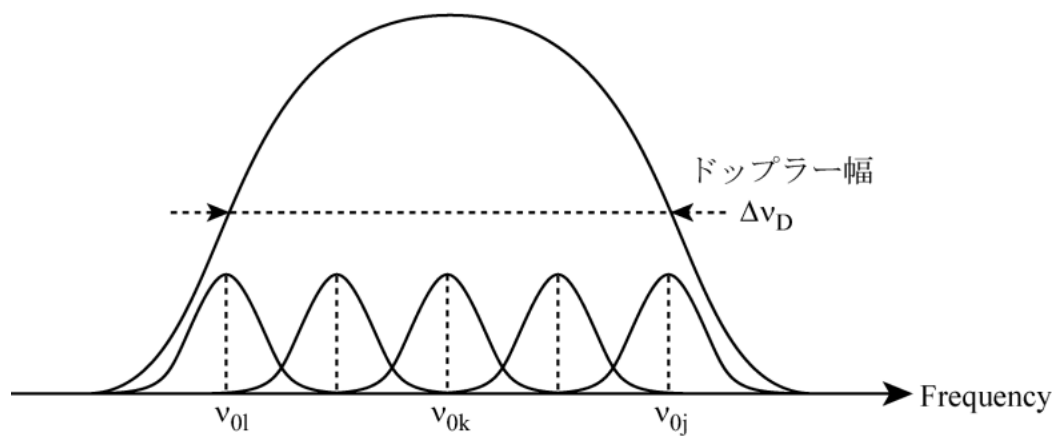
で与えられるガウス形(Gaussian)を得る。その半値全幅 $\Delta \nu_D$ は、

$$\Delta \nu_D = \sqrt{\ln 2} \left(\frac{u}{\lambda} \right) \quad (3.6)$$

であり、この不均一広がりをドップラー幅と呼ぶ。不均一広がりを示すスペクトルを構成する全電子の内、同じ速度成分 v を持つ電子の副集団からなるスペクトルは均一広がりを持っているから、実際には全体としてのスペクトルの幅は均一幅とドップラー幅のどちらよりも大きくなる。Fig.3-3 に均一広がりと不均一広がりの図を示す。



(a) Homogeneous broadening



(b) Inhomogeneous broadening

Fig.3-3 Homogeneous broadening and inhomogeneous broadening.

図3-3 均一広がりと不均一広がり

Fig.3-4 に示される波形が実際に観測される Rb 原子の D₂ 吸収線である。実際に予測される吸収スペクトルはドップラー幅(約 500MHz)の影響を受け、12 本の線スペクトルが 4 本の広がったスペクトルになってしまう。

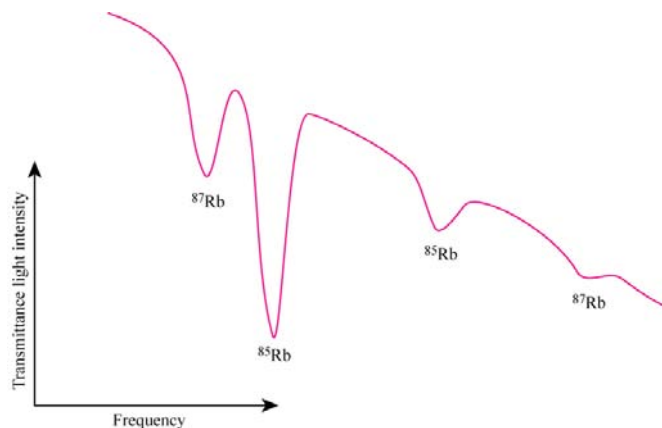


Fig.3-4 Observed profiles of the Rb-D₂ absorption lines.
図3-4 Rb-D₂吸収線の観測波形

衝突幅 Δ_c 、自然幅 Δ_N 、ドップラー幅 Δ_D の具体的な数値は次の通りである。

[衝突幅]

衝突幅 Δ_c の半値全幅は、

$$\Delta\nu_c = 2Pa^2 \sqrt{\frac{8\pi}{Mk_B T}} \quad (3.7)$$

M : 原子質量

k_B : ボルツマン定数

T : 気体の絶対温度

P : 圧力

a : 相互作用の及ぶ原子間距離

で与えられる。実験室内の条件で計算した値 Δ_c では約 0.2Hz となり、無視できるほど小さい。

[自然幅]

自然幅 Δ_N の半値全幅は励起準位の寿命を τ とすると、不確定性関係から、

$$\Delta\nu_N = \frac{1}{2\pi\tau} \quad (3.8)$$

となる。また、Rb 原子の吸収線の各遷移に対する寿命は、

$$\begin{aligned} 5s_{1/2} \rightarrow 5p_{1/2} (\text{D}_1 \text{ 線}) \cdots \tau_1 &= 28.1 \text{ ns} \\ 5s_{1/2} \rightarrow 5p_{3/2} (\text{D}_2 \text{ 線}) \cdots \tau_2 &= 26.7 \text{ ns} \end{aligned}$$

であり、これらを式(3.8)に代入すると、

$$\begin{aligned} \Delta\nu_{N1} &= 5.66 \text{ MHz} \\ \Delta\nu_{N2} &= 5.96 \text{ MHz} \end{aligned}$$

となり、自然幅は両者とも約 6MHz となる。

[ドップラー幅]

上述の通り熱運動による共振周波数 ν_0 のシフトは個々の原子の速度分布に依存する。熱平衡状態における気体中の原子の速度分布は、マクスウェル・ボルツマン分布に従っており、スペクトル形状はガウス型となる。ドップラー幅 $\Delta\nu_D$ の半値全幅は、

$$\Delta\nu_D = \frac{2\nu_0}{c} \sqrt{\frac{2(\ln 2)k_B T}{M}} \quad (3.9)$$

ν_0 : 静止している原子の共鳴周波数
 c : 光速

で与えられる。共鳴周波数は超微細構造の数だけ存在する。ここでは、簡単のために D_1 線で $\Delta\nu_{D1}=377.2\text{THz}$ 、 D_2 線で $\Delta\nu_{D2}=384.3\text{THz}$ とする。通常 300K では、

$$\begin{aligned} \Delta\nu_{D1} &= 506 \text{ MHz} \\ \Delta\nu_{D2} &= 515 \text{ MHz} \end{aligned}$$

となる。

3.2 飽和吸収分光法

本節では、高精度な周波数基準を得ることができる飽和吸収分光法について述べる。3.1.2で述べたように吸収スペクトルの広がり要因には自然幅と呼ばれる均一幅とドップラー幅と呼ばれる不均一幅があることを示した。したがって、ドップラー広がり無くすことができれば自然幅程度の広がりを持つスペクトルを観測でき、半導体レーザーの高精度な周波数基準となる。そこでドップラー広がり影響を受けない飽和吸収分光法が考えられる。飽和吸収分光法において、光吸収の飽和という現象が重要になる。これは、ある一定の周波数で入射光の強度 P を大きくした場合、はじめは光の吸収量の増加分 ΔP が入射光強度 P に比例するが、遷移する準位間の原子数分布の差が小さくなるにつれて ΔP が P に比例しなくなり、ついに一定値に行き着く現象である。飽和吸収は均一広がり範囲内でのみ起こるため、原子が熱運動していても不均一広がりには行き渡らない。飽和吸収観測用の光学系を Fig.3-7 に示す。

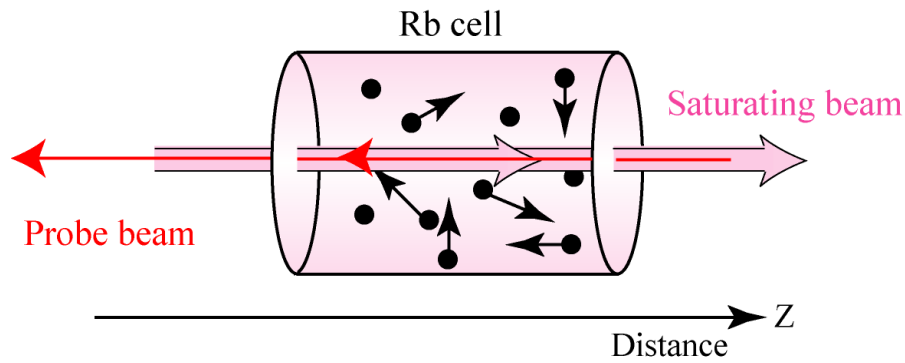


Fig.3-7 Fundamental optical setup for the saturated absorption spectroscopy.

飽和吸収を起こさせる光を飽和光(Saturating beam)、観測用の光をプローブ光(Probe beam)と呼ぶ。周波数を掃引しながらプローブ光を受光した結果、飽和光による飽和吸収波形とプローブ光による線形吸収波形との合成波形が得られる。

原子によるドップラー効果を考えるため、熱運動している原子のレーザー光に平行な速度成分を V_z とする。まず Fig.3-8(a)に示すような2準位系について考える。レーザー光の周波数が ω の場合、飽和光とプローブ光により励起される原子はそれぞれ次式を満たす速度成分を持つものに限られる。

$$\begin{array}{ll} \text{飽和光} & V_z = (\omega - \omega_0) / k \end{array} \quad (3.14)$$

$$\begin{array}{ll} \text{プローブ光} & V_z' = -(\omega - \omega_0) / k = -V_z \end{array} \quad (3.15)$$

ここで、 $k = \omega / c$ 、 ω_0 は原子の自然共鳴周波数である。

レーザ光の周波数が $\omega < \omega_0$ のとき、飽和光は負の速度成分をもつ原子群を、プローブ光は正の速度成分をもつ原子群をそれぞれ励起する。これらの吸収は互いに影響を及ぼさない。 ω が ω_0 に近づくにつれて共鳴する原子数も増加するため吸収量も増加する。

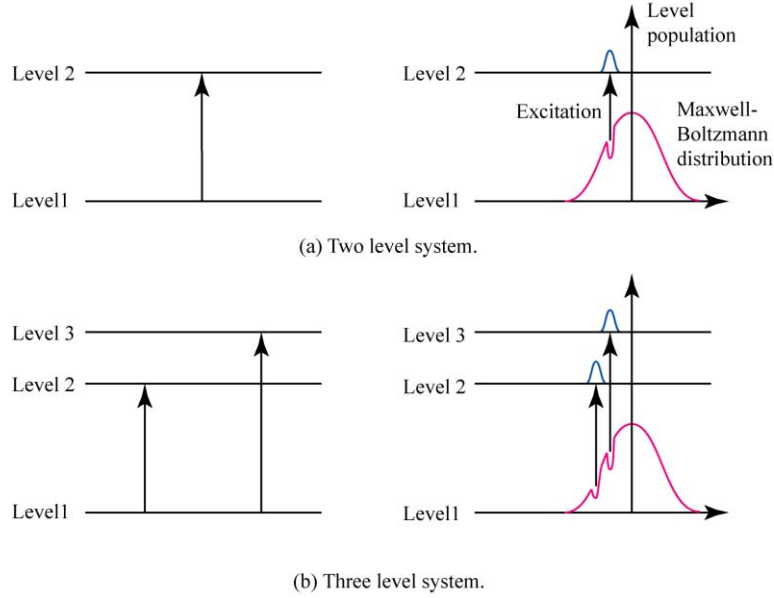


Fig.3-8 Energy level and velocity distribution of atoms.
図3-8 原子の速度分布とエネルギーレベル

$\omega = \omega_0$ となると、飽和光、プローブ光共にドップラー効果による影響を受けない速度成分 $V_z = 0$ の原子群を励起する。このとき飽和光はこの原子群に対して飽和を起こしているので、プローブ光による吸収量は減少する。

$\omega > \omega_0$ になると、飽和光は正の速度成分をもつ原子群を、プローブ光は負の速度成分をもつ原子群をそれぞれ励起し、これらの場合も互いに影響を及ぼさない。

以上のことから、レーザ光を周波数掃引しながらプローブ光の透過光強度を観測すると、ドップラー広がりを中心付近に飽和吸収信号の一つである反転ラムディップと呼ばれる鋭い信号が得られる。この様子を Fig.3-9(a)に示す。反転ラムディップの半値全幅は近似的に自然幅の 2 倍である。これは、飽和光とプローブ光による吸収が共に自然幅程度の半値全幅を持つためである。

次に Fig.3-8(b)に示すような 3 準位系について考える。準位 0 から準位 1 に遷移するときの自然共鳴周波数を ω_1 、準位 2 に遷移するときの自然共鳴周波数を ω_2 ($\omega_1 < \omega_2$) とする。このとき遷移する原子の速度成分もドップラー効果により次式を満たすものに限られる。

$$\text{飽和光} \quad V_{z1} = (\omega - \omega_1) / k \quad (3.16)$$

$$V_{z2} = (\omega - \omega_2) / k \quad (3.17)$$

$$\text{プローブ光} \quad V_{z1}' = -(\omega - \omega_1) / k \quad (3.18)$$

$$V_{z2}' = -(\omega - \omega_2) / k \quad (3.19)$$

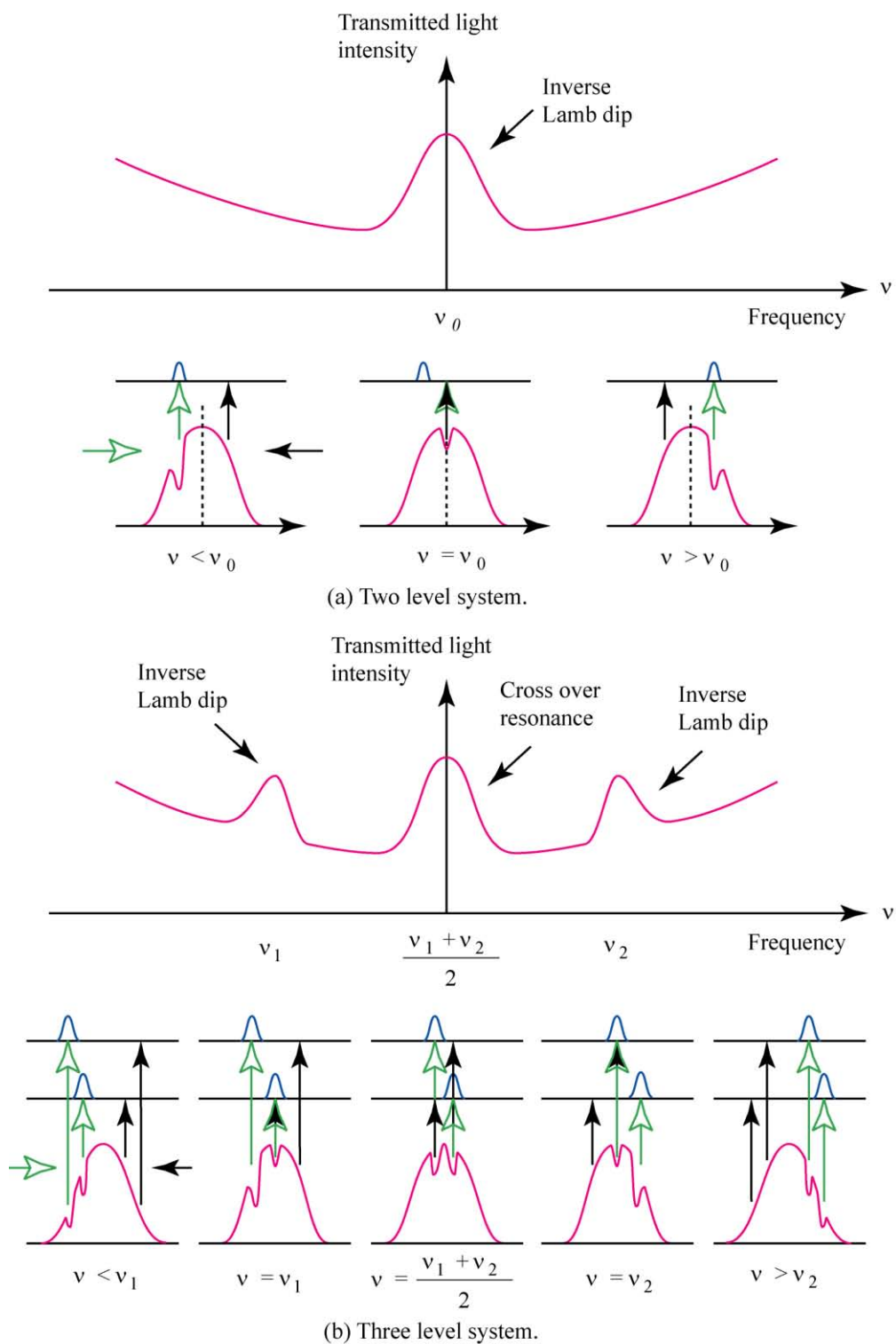


Fig.3-9 The saturated absorption signals.

图3-9 饱和吸收分光信号

3 準位系の場合も 2 準位系と同様に、レーザ発振周波数 ν が ν_1 及び ν_2 に一致したときに反転ラムディップが観測される。さらに、レーザの周波数が共鳴周波数の中間値 $(\nu_1 + \nu_2)/2$ のとき、飽和光の V_{z1} とプローブ光 V_{z2} 飽和光の V_{z1}' とプローブ光 V_{z2}' が等しくなるためプローブ光による吸収量は減少する。したがって、レーザ光の周波数を掃引しながらプローブ光の透過光強度を観測すると、2 つの反転ラムディップの間にこれと同程度の広がりを持つ鋭い信号が得られる。これはクロスオーバー共鳴と呼ばれる飽和吸収分光信号である。この 3 準位系の飽和吸収分光信号の様子を Fig.3-9(b)に示す。D₂ 線の超微細構造から反転ラムディップとクロスオーバー共鳴の総数を計算すると 24 本になる。しかし、これらは非常に狭い間隔で並んでいるため 1 つずつ観測することはできない。そのため実際に観測される飽和吸収分光信号は、いくつかの反転ラムディップとクロスオーバー共鳴が重なりあったものになっている。

このようにして得られた飽和吸収分光信号は通常吸収の吸収幅に比べて十分狭い。この周波数に対して安定化を行えば半導体レーザの安定度は向上する。Fig.3-10 に実際に観測された Rb 原子の D₂ 線の飽和吸収分光による吸収波形を示す。実験で得られた反転ラムディップの幅は約 100MHz 程度である。

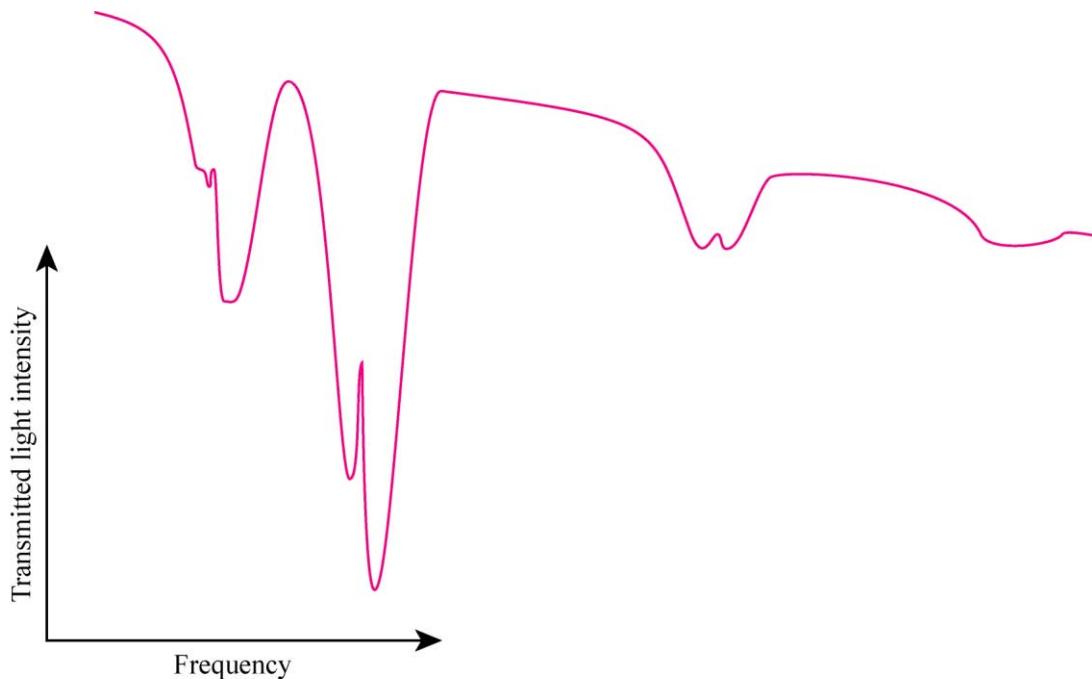


Fig.3-10 Observed profiles of the Rb-D2 absorption line using the saturated absorption spectroscopy.

第4章 暗号と乱数

暗号には、コード (Code) とサイファー (Cipher) がある。前者は、あるまとまりのある語や句を他のもので置き換えるのに対し、後者は、通信の文字を一对一に置き換える。しかしながら、暗号学者によって主に研究されてきたのは、サイファーであり、暗号というとサイファーだけを指す場合が多い。したがって、本章では、以下、サイファーのことを暗号と呼ぶことにする⁽⁷⁴⁾。

古典式暗号は、換字式暗号、転置式暗号、分置式暗号の3つに分類することができるが、ここでは、換字式暗号について述べていくことにする。

4.1 古典暗号⁽⁶⁴⁾

4.1.1 単一換字式暗号

換字式暗号の古いものとしては、シーザー暗号がよく知られている。シーザー暗号は、ローマのジュリアス・シーザーが使ったといわれているもので、平文の各文字を辞書順に3文字だけシフトして暗号文をつくる暗号であり、カエサル暗号とも呼ばれる。

Fig.4-1 にカエサルの用いた平アルファベット (もとのメッセージを書くときに使われるアルファベット) と暗号アルファベット (平アルファベットの代わりに使われるアルファベット) を示す。Fig.4-1 からわかるように、暗号アルファベットは平アルファベットから3文字分だけずれている。ここで、ずらす文字数を1文字から25文字まで変えてやれば、25種類の暗号が作れるのは明らかである。実際、平アルファベットをどう並び替えてもよいことにすれば、作れる暗号の種類は大幅に増やすことが可能である。

平アルファベット	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
暗号アルファベット	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
平文	v e n i , v i d i , v i c i (来た、見た、勝った)																									
暗号文	Y H Q L , Y L G L , Y L F L																									

Fig.4-1 カエサル暗号

具体的な個々の暗号は、“アルゴリズム”と“鍵”によって指定される。アルゴリズムとは、大まかな暗号化の方針のことで、鍵はその詳細を決めるものである。今の場合、アルゴリズムは平アルファベットを暗号アルファベットで置き換えることに相当する。暗号アルファベットは平アルファベットをどう並び替えたものでもよい。どれか1つの暗号アルファベットを指定するためには、鍵を選ばなくてはならない。アルゴリズムと鍵の関係を Fig.4-2 に示す。

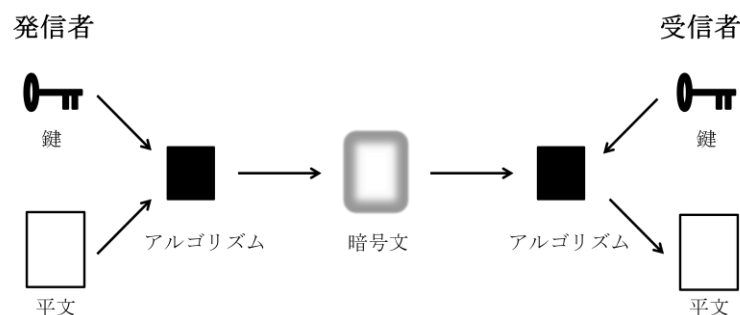


Fig.4-2 アルゴリズムと鍵の関係

暗号システムが安全であるためには、鍵の秘密が守られなければならない。それに加えて、鍵の候補が多くなければならない。例えば、カエサル暗号は、鍵の候補がわずか 25 通りしかないため、暗号としてはあまり強力ではない。これに対して、ごく一般的な換字式暗号のアルゴリズムでは、暗号アルファベットは平アルファベットをどう並び替えたものでもよいから、鍵の候補は、 4×10^{26} 通りを上回る。そのような暗号システムの一例を Fig.4-3 に示す。このタイプの暗号の強みは、使うための手続きはごく簡単であるにもかかわらず、鍵の候補を「総当たり式」にチェックするのは事実上不可能であるため、高い安全性が保証されることである。

平アルファベット	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
暗号アルファベット	J	L	P	A	W	I	Q	B	C	T	R	Z	Y	D	S	K	E	G	F	X	H	U	O	N	V	M
平文	e	t		t	u	,		b	r	u	t	e	?	(ブルータスよ、おまえもか)												
暗号文	W	X		X	H	,		L	G	H	X	W	?													

Fig.4-3 一般的な換字式アルゴリズムの例

また、鍵の候補が多少減ってもよいという場合には、もっと簡単に鍵を作る方法もある。暗号アルファベットを作るときに、平アルファベットをランダムに並び替えるのではなく、“鍵語（キーワード）”または“鍵句（キーフレーズ）”を使う方法である。例えば、キーフレーズとして“JULISCAER”を使う場合には、この文字列を暗号アルファベットの先頭に置く。暗号アルファベットの残りの部分は、キーフレーズの後ろに正しいアルファベットの残りの文字を続けてゆけばよい。今の場合、暗号アルファベットは次のようになる。

平アルファベット	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
暗号アルファベット	J	U	L	I	S	C	A	E	R	T	V	W	X	Y	Z	B	D	F	G	H	K	M	N	O	P	Q

この方法の長所は、キーワードやキーフレーズを記憶するのが簡単であるという点である。

4.1.2 多表式換字暗号

多表式の暗号は、単一換字式暗号が安全でなくなってきた 15 世紀後半から 16 世紀後半にかけて考え出された暗号で、ヴィジュネル暗号はその中で恐らく最も有名なものであり、フランスの外交官ブレーズ・ド・ヴィジュネルによる多表式の換字式暗号のことである。

ヴィジュネル暗号が強力なのは、1 個ではなく、26 個の暗号アルファベットを使うためである。実際に暗号化を行うには、はじめに“ヴィジュネル方陣”を作る必要がある。これを表 1 に示す。

表 1 ヴィジュネル方陣

平文	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

最上段は平アルファベットで、その下に 26 種類の暗号アルファベットが続く。平文の各文字は、26 種類の暗号アルファベットのどれを使って暗号化してもよい。例えば、2 の行の暗号アルファベットを使えば、平文の a は暗号化されて C になるが、12 の行の暗号アルファベットを使えば、平文の a は暗号化されて M になる。暗号アルファベットを 1 つだけ使ってメッセージ全体を暗号化したとすると、それは単なるカエサル暗号にすぎないが、ヴィジュネル暗号では、平文中の 1 つ 1 つの文字に対して、ヴィジュネル方陣の異なる行（つまり異なる暗号アルファベット）が使用される。

メッセージのスクランブルをはずすには、それぞれの文字がヴィジュネル方陣のどの行を用いて暗号化されたかを知らなければならない。したがって、正当な受信者は送信者とのあいだで、行の切り替え方法をあらかじめ取り決めておく必要がある。そのためにはキーワードを使用すればよい。キーワードの使い方の具体例をみるために、“divert troops to east ridge（軍勢を東の尾根に向けよ）”というメッセージを、“WHITE”というキーワードを使って暗号化することにする。はじめに、平文の上にキーワードを繰り返して書き、平文のすべての文字にキーワードのどれかの文字が対応するようにしておく。したがって、暗号文は次のように作成される。最初の文字 d を暗号化するには、その上の文字が W であるためこれがヴィジュネル方陣の行を指定する。W ではじまる 22 の行が、平文の文字 d を換字する暗号アルファベットである。ゆえに、平文の文字 d は、暗号文では Z で表されることになる。

キーワード	W H I T E W H I T E W H I T E W H I T E W H I
平文	d i v e r t t r o o p s t o e a s t r i d g e
暗号文	Z P D X V P A Z H S L Z B H I W Z B K M Z N M

平文の 2 番目の文字 i を暗号化するときも、このプロセスを繰り返せばよい。

今の場合、キーワードには 5 つの文字が含まれているので、送信者はヴィジュネル方陣中の 5 つの行を使うことになるが、より長いキーワード、もしくはキーフレーズを用いれば暗号化に使用される行が増えるので、暗号をより複雑にすることができる。ヴィジュネル暗号の決定的な強みは、頻度分析では解読できないことである。それに加えて、辞書に載っている単語はもちろん、単語をつなげたものでも、勝手に作った言葉でも鍵になりうるため、鍵の候補が莫大な数に増やすことができる点である。

4.2 現代暗号

4.2.1 共通鍵暗号⁽⁶⁴⁾

共通鍵暗号は、暗号化と復号に同一の（共通の）鍵を用いる暗号である。第 1 次大戦の終わり近く、米国陸軍の暗号研究を率いていたジョセフ・モーボーン少佐は、かつてない

安全性の高さを達成するために、ヴィジュネル暗号にランダム鍵を組み込むことを提唱した。ランダム鍵は、意味のある言葉の並びではなく、でたらめな文字列である。モーソンの提唱した暗号システムでは、はぎ取り式の分厚いメモ帳のようなものを用意し、メモ帳の各ページにはランダムな文字列が書かれており、これが鍵となる。鍵には2つとして同じものはない。このメモ帳を2部用意し、1部は送信者用、もう1部は受信者用とする。送信者はメモ帳の第1ページに書かれた鍵を使って、ヴィジュネル暗号でメッセージを暗号化する。Fig.4-4に示したのは、メモ帳の3つのページ（実際には、それぞれのページには何百もの文字が書かれている）と、そのうちの1ページ目を用いて暗号化されたメッセージである。受信者は、送信者と同じ鍵を用いてヴィジュネル暗号のプロセスを逆転させれば、暗号文を容易に復号することができる。メッセージがうまく送受信され、復号が無事にすんだら、鍵の役目を果たした紙は捨ててしまう。したがって、同じ鍵は二度と使われることはない。次のメッセージを暗号化するときには、メモ帳の次のページにあるランダムな文字列を鍵として用い、使用後はそれも捨てる。どの鍵も一回しか使われないので、この暗号システムは“ワンタイム・パッド（一回限りのメモ帳）暗号”と呼ばれている。

	シート1	シート2	シート3
	<div> P L M O E Z Q K J Z L R T E A V C R C B Y N N R B </div>	<div> O I W V H P I Q Z E T S E B L C Y R U P D U V N M </div>	<div> J A B P R M F E C F L G U X D D A G M R Z K W Y I </div>
鍵	P L M O E Z Q K J Z L R T E A V C R C B Y		
平文	a t t a c k t h e v a l l e y a t d a w n		
暗号文	P E F O G J J R N U L C E I Y V V U C X L		

Fig.4-4 ワンタイム・パッド暗号（“attack the valley at dawn”というメッセージを暗号化）

ワンタイム・パッド暗号の安全性は、ひとえに鍵がランダムであるという点にかかっている。ランダムな鍵は暗号文にランダムさをもたらし、暗号文がランダムならば、暗号解読者に手掛かりを与えるパターンや構造を生じさせない。実際、ワンタイム・パッド暗号で暗号化されたメッセージが解読不能であるということは数学的に証明可能である。言い換えると、ワンタイム・パッド暗号は、ヴィジュネル暗号がそうであったように単に解読不能だとみなされているのではなく、絶対に安全であると言える。しかしながら、ワンタ

イム・パッド暗号は理論上は完璧であるが、実用上は以下の2つの点が問題となる。

- (1) ランダムな鍵を膨大に生成する技術
- (2) ランダムな鍵の配送手段

(1) については、ランダムな鍵を作る方法としては、完全にランダムな振る舞いをする
ことがわかっている自然界の物理プロセスを利用することで解決できる。また、(2) の鍵
配送問題については、次節で述べることにする。

4.2.2 公開鍵暗号 (74-76)

先に述べた共通鍵暗号は、暗号化用の鍵と復号用の鍵が同じでなければならなかった。
そして、この暗号を通信路に用いようとすると、送る側と受け取る側で同じ鍵を持つ必要
があるが、この鍵をどうやって安全に送信し、共有するかということが問題となる。送
信の途中でこの鍵が誰かの手に渡れば同じ鍵を用いて暗号化したデータはすぐに解読され
てしまう。この暗号鍵そのものに暗号をかけて送る手が考えられるが、共通鍵暗号を使う
限り、そのための元になる鍵をどうやって安全に送るかという問題に陥り、解決策にはな
らない。一方、公開鍵暗号では、暗号化と復号に2種類の異なる鍵が利用される。したが
って、一方をみんなに公開し、もう一方を自分で秘密に保管するということが可能である。
公開した方の鍵は不特定多数の人に渡しても、秘密に保管した鍵を類推することは数学的
に不可能な仕組みになっている。ただし、公開鍵暗号は共通鍵暗号に比べて処理速度が遅
いという問題がある。そこで、文書などの大量データの暗号化には共通鍵暗号を用い、そ
の共通鍵暗号の鍵を安全に配送するのに公開鍵暗号が使われている。これにより、鍵配送
の安全性、容易性と、大量データの暗号処理の効率性を両立できるようにしている。公開
鍵暗号としては、米国で開発された RSA 暗号が有名である。RSA は、1977 年に米国のマサ
チューセッツ工科大学にいた R. Rivest、A. Shamir、L. Adelman の3人の頭文字に因んで名
付けられたものである。ここでは、RSA 暗号がどれくらい安全かをみていくことにする。

アリスがボブ宛てにメッセージを暗号化するには、ボブの公開鍵を調べなければならな
い。ボブは自分用の公開鍵を作るために2つの素数 p_B 、 q_B を選び、それらを掛け合わせて
 N_B を作る。ただし、ボブは、 p_B 、 q_B の復号鍵を秘密にしているとする。一方、 N_B は公開さ
れている。公開された N_B は“408508091”であるとする。アリスはこの N_B を一方向関数に入
れ、ボブ宛てのメッセージを暗号化する。暗号化されたメッセージを受け取ったボブは、
個人鍵 p_B 、 q_B の値を使ってメッセージを復号する。ここで、そのメッセージをイヴが途中
で傍受したとする。イヴがメッセージを解読するためには、公開されている N_B から p_B と
 q_B を素因数分解を用いて割り出さなければならない。

ところで、素因数分解というのは非常に時間のかかるプロセスであり、基本的には1つ
1つの素数で N_B が割り切れるかどうかを確かめていくことになる。今回の場合、最終的に

2000 番目の素数“18313”が割り出され、もう一方は“22307”となる。しかしながら、この例で用いた N_B では安全性が高いとは言えないので、ボブはもっと大きな素数を個人鍵として選ぶ必要がある。例えば、 10^{65} ぐらいの大きさの素数を選んだとする。すると、 N_B の値は $10^{65} \times 10^{65}$ 、つまり 10^{130} 程度になる。この2つの素数を掛け合わせて N_B を作ることは、コンピュータを使えば、1秒ほどでできるだろうが、そのプロセスを逆転させて p_B と q_B を割り出すには莫大な時間がかかってしまう。

このように、RSA 暗号などの現代暗号の安全性は、秘密鍵の存在によって保証されている。これらの暗号を解読することが難しいのは、盗聴者が秘密鍵を知らないからであり、もし盗聴者に秘密鍵が知られてしまえば、暗号は容易に解読されてしまう。また、量子コンピュータが実現されれば、ショアのアルゴリズムを用いて素因数分解が効率よく実行できるようになる。これにより、RSA 暗号は量子コンピュータを持った盗聴者に破られてしまうばかりでなく、暗号解読の過程で秘密鍵も知られてしまうので、秘密鍵と対応する公開鍵で暗号化されたすべての暗号文がその盗聴者によって解読されてしまう。量子コンピュータの実現は大変な困難が予想されているが、今後の暗号は素因数分解の難しさをその安全性の根拠とするだけでは不充分であると考えられる。

4.3 量子暗号 (76)、(77)

先に述べた公開鍵暗号の将来的な安全性の問題を解決する方法としては、光の量子的性質を用いた量子暗号（量子暗号通信）が注目されている。これは、ネットワークへの応用は難しいが、1対1通信では、ある程度の実用性をもっていると言われている。明子と凡太郎が量子暗号通信を行うには、二人の間に光子の量子状態が伝達できる量子通信路が必要となるが、これは光ファイバを用いることにより実現可能である。さらに、明子と凡太郎の間には通常の双方向の通信路（例えば、インターネット）も必要となる。この通信路は盗聴されてもよいのだが、明子と凡太郎はお互いに受け取った情報が間違いなく相手からのものであることを確認する必要がある。つまり、メッセージ認証が行われることが必要である。このとき、量子暗号により明子と凡太郎の間でランダムな系列を秘密に共有することができる。このようにして共有された秘密系列は、この量子暗号システムに対する攻撃が量子通信路で伝達される情報の盗聴・改ざんに限られるなら、原理的な安全性を持っている。そこで、この系列を秘密鍵として、明子と凡太郎の間で通常の通信路を介し、ワンタイム・パッド暗号により原理的に安全な守秘通信を行うことができる。ただし、明子と凡太郎の間で、通常の通信路におけるメッセージ認証が安全に行われることが前提となる。このためには、明子と凡太郎は、あらかじめ一定の秘密情報を安全に共有しておく必要がある。また、量子通信路から送信機の状態を観測するなど、伝達情報以外への攻撃がある場合には、必ずしも安全性は保証されない。このような物理的攻撃にも対処できるように量子暗号システムは十分注意深く構成する必要がある。









以上のような前提が満たされる場合、量子暗号で原理的な安全性が達成できるのは、量子通信路を盗聴すると、光子の量子状態が破壊されてしまい、盗聴されたことを検出できるためである。そこで、盗聴されたと思われる情報は捨てて、安全な情報だけを用いればよい。このためには、単一光子で通信をする必要があるが、このような技術は現在可能になってきている。

このような原理に基づく量子暗号方式はいくつか提案されているが、1984年にベネットとブラサードによって発表されたBB84と呼ばれる方式が最も有名である。この方式では、情報の伝達に光子の偏光状態が用いられている。ただし、偏光状態として水平と垂直（+で表す）、45度、135度（×で表す）の2通りの方法で情報を伝達する。+で送る場合は、水平、垂直の偏光がそれぞれ情報0、1を表し、×で送る場合は、45度、135度がそれぞれ情報0、1を表すとする。受信側では、あらかじめ+であるか×であるかのいずれかを想定し測定系を設定して偏光を測定する。このとき、送信側と受信側で+、×の設定が一致すれば、情報は高い確率で正しく受信できる。一方、これが一致しなければ、情報は伝達できない。つまり、誤り率が1/2となってしまう。しかも、元の偏光状態の設定がどうであったかを知ることも原理的には不可能である。

BB84を行うには、まず明子は0、1の乱数列を生成し、これを2ビットずつに区切る。その1ビット目は偏光の設定を+するか×とするかを決めたもので、2ビット目は秘密情報の元になるものである。いま、1ビット目が0なら偏光の設定は+、1なら×にすることにする。一方、凡太郎も0、1の乱数列を生成し、各ビットの0、1に応じて、測定系を+または×に設定する。したがって、明子と凡太郎の間での情報伝達は、それぞれの乱数に応じて表2のようになる。

次に、明子と凡太郎は通常の通信路を用いて、偏光の設定をどのようにしたかをお互いに教え合う。二人はその設定が一致したときに伝達された情報、つまり表2で?以外の場合の情報だけを残すことにし、これが明子と凡太郎の間で共有する秘密情報の元になる。量子通信路には誤りもあり、また盗聴されていれば、高い確率で誤りが生じる。そこで、誤り訂正符号を用いるとともに、明子と凡太郎の間で共有された情報の一部を開示して誤りがどの程度生じているかを確かめるなどの方法によって、共有情報から信頼のできる情報だけを抽出する。このようにして、明子と凡太郎は安全な情報を共有することができる。

表 2 BB84 方式

明子の乱数	偏光の設定	偏光状態	凡太郎の乱数	偏光の設定	測定結果	受信情報
00	+		0	+		0
			1	×	?	?
01	+		0	+		1
			1	×	?	?
10	×		0	+	?	?
			1	×		0
11	×		0	+	?	?
			1	×		1

各ビットは、光子 1 個で伝達されるので、盗聴者はそれを盗聴すると、凡太郎へ情報が伝達されなくなる。ただし、盗聴者は盗聴した情報を凡太郎に再送する場合も考えられる。しかし、盗聴者は明子の偏光の設定を知らないので、1/2 の確率で誤った設定を行ってしまう。この場合、盗聴した情報は 1/2 の確率で誤ることになるため、盗聴者から凡太郎に送られる情報は少なくとも 1/4 の確率で誤っている。量子通信路の誤りの確率は、それよりもずっと小さいので、明子と凡太郎は、盗聴されていることを検知でき、盗聴者の送ってきた情報をほぼ確実に除くことが可能となる。

このような量子暗号にはまだ問題も多く、究極の暗号とは言えないが、原理的な安全性が保証されており、今後は限定的にはあるが、実用化されると期待されている。

4.4 乱数

一般に乱数とは等確率性と無規則性の 2 つの性質をあわせもつ数列のことであり、生成方法により疑似乱数と物理乱数に分類される。

4.4.1 疑似乱数 ^(6 3)

疑似乱数は、コンピュータのアルゴリズムにより生成され、線形合同法や M 系列、メルセンヌ・ツイスタ法などがある。ここでは、古典的な疑似乱数生成法として知られる線形合同法について説明していくことにする。

定義 4.1

N 、 a 、 c を整数とし、数列 x_i ($i = 1, 2, 3, \dots$) を漸化式

$$x_{i+1} = ax_i + c \bmod N$$

で生成して $\{0,1,\dots,N-1\}$ に値を取る疑似乱数として用いることを、線形合同法という。初期値 x_1 はユーザが選ぶことができ、これを選ぶごとに異なる数列が得られる。 x_1 のことを疑似乱数の

シード（種）と言う。

線形合同法は、今まで最も広く使われてきた疑似乱数生成法であると言える。多くの C 言語のライブラリで、 $a = 1103515245$ 、 $c = 12345$ 、 $N = 2^{32}$ としたものが 90 年代まで標準的に実装されていた。例えば、このパラメータで、 $x_1 = 3$ とすると

$$\begin{aligned}x_2 &= 1103515245 \times 3 + 12345 \bmod 2^{32} \\&= 3310558080 \bmod 2^{32} \\&= 3310558080, \\x_3 &= 1103515245 \times 3310558080 + 12345 \bmod 2^{32} \\&= 3653251310737941945 \bmod 2^{32} \\&= 465823161, \\x_4 &= 679304702, \\x_5 &= 2692258143,\end{aligned}$$

という具合に数列が生成される。この数列は

- ・ 周期的であり、どの初期値を取っても周期は 2^{32}
- ・ 1 周期に、0 から $2^{32}-1$ までのすべての整数をちょうど 1 回ずつ取る

ということが数学的に証明できる。

このような方法で作られた数列は、初期値と漸化式がわかる限り誰にでも再現可能である。

4.4.2 物理乱数

物理乱数は、ランダムな物理現象を利用して生成される乱数である。よく知られた物理乱数生成法として、例えば、放射性崩壊を利用した方法⁽⁶⁴⁾がある。この生成法では、放射性物質の塊を実験機の上に置き、ガイガー・カウンタで放射線を検出する。放射線は立って続けに出ることもあれば、放出から放出までにだいぶ間があくこともある。その時間間隔は完全にランダムであって、予測不可能である。そこで、ガイガー・カウンタにディスプレイをつなぎ、ディスプレイ上には速いサイクルでアルファベットの文字が次々に表示されるようにしておき、放出が検出されると表示は一瞬停止するとする。そのとき画面ににあった文字を記録する。そして、ディスプレイは再びスタートするため、同様の記録を繰り返せば、ランダムな信号を手に入れることができる。しかしながら、この方法では物

理乱数の生成速度は遅い。別の物理乱数生成器としては、抵抗や半導体内部で発生する熱雑音を検出して、デジタル数値化する方法などもある。また、最近では、半導体レーザの位相雑音や戻り光雑音を用いた物理乱数生成器も多数報告⁽⁴⁷⁻⁵²⁾されており、本研究では、半導体レーザの周波数雑音を用いた物理乱数の生成が実現できている^{(54), (55), (57-61)}。

第5章 直接変調方式によるレーザ周波数安定化

半導体レーザの安定化においては、初期の頃はファブリペロー干渉計を用い、外部の参照周波数により安定化する方法がとられ、後に、直接原子や分子の吸収線を用いる方法が用いられるようになった。吸収線を用いる時、その吸収線がスペクトル幅の小さい線を持つこと、またそのスペクトル強度が強く尖鋭であることが高い安定度を得るための1つの条件となる。このような線形吸収を用いる方法以上に、更にスペクトル幅の狭い飽和吸収線⁽⁷⁸⁾、⁽⁷⁹⁾などのドップラーフリースペクトル線を用いる方法は、安定化実験には有利となる⁽⁸⁰⁾。

そこで本章では、Rb原子の飽和吸収分光法を用いた半導体レーザの発振周波数安定化について述べ、制御信号の改善による発振周波数安定度への影響について述べる。

5.1 直接変調方式による周波数安定化の原理⁽¹³⁾

半導体レーザの発振周波数は、周囲温度や電流の僅かな変化により大きく変化する。変化量は、レーザにより異なるが例えば、温度に対しては -30GHz/K 、電流に対しては -5GHz/mA 程度である。したがって、実際に半導体レーザを使用するときは、温度制御を施し、低雑音の電流源で駆動して周波数の安定化を行っている。それでも、今後の応用を拡大するためには、更なる周波数の安定度を向上させる必要がある。その場合には、Fig.5-1示すような安定化システムを用い、周波数基準の周波数に半導体レーザの発振周波数を安定化する。この回路の動作は以下のようなものである。

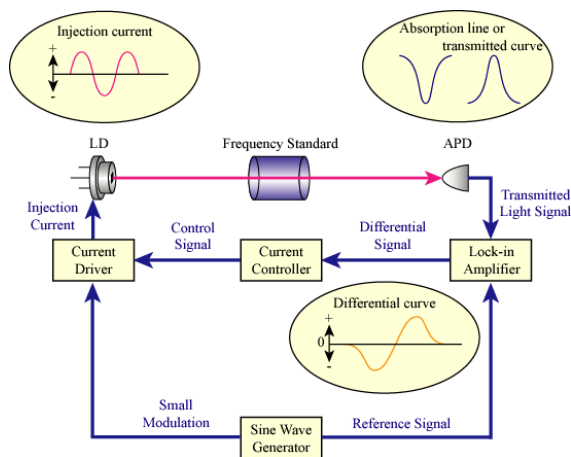


Fig.5-1 Stabilization flow chart.

半導体レーザには、あらかじめ数 kHz 程度の周波数の微少な交流電流を直流電流に重畳して加えて浅く周波数変調を行い、この光出力を周波数基準（例えば Rb セルやファブリペローエタロン等）を透過させると、その出力光は、Fig.5-2(a)のようになる。すなわち、この光出力には微少な周波数変調がくわえられているから、光の周波数が周波数基準より高い

場合には、光検出器出力は変調信号と同位相の信号が現れ、また周波数基準より低い場合には逆位相の信号があらわれ、周波数基準と一致しているときには同一周波数成分が無く 2 倍の周波数成分が出てくる。

そこで、この検波信号を、変調信号を基準としてロックインアンプで同期検波を行えばその平均出力は Fig.5-2 (b)のように、透過出力の微分信号が得られる。したがって、この微分信号すなわち誤差信号を半導体レーザに帰還することにより、半導体レーザの発振周波数を周波数基準となる P 点に合わせることができる。この P 点からの周波数のずれ Δ に対する誤差信号 ΔV を制御信号とすると、安定化点 P での接線の傾きは

$$G_d = \frac{\Delta V}{\Delta \nu}$$

[V/GHz]

と表され、これを周波数弁別利得と呼ぶ。

P 点での接線の傾きが大きいほど高精度な制御信号を得ることができる。つまり G_d は周波数の検出感度を決定づける量であり、 G_d の向上は直接、安定度の向上につながる。

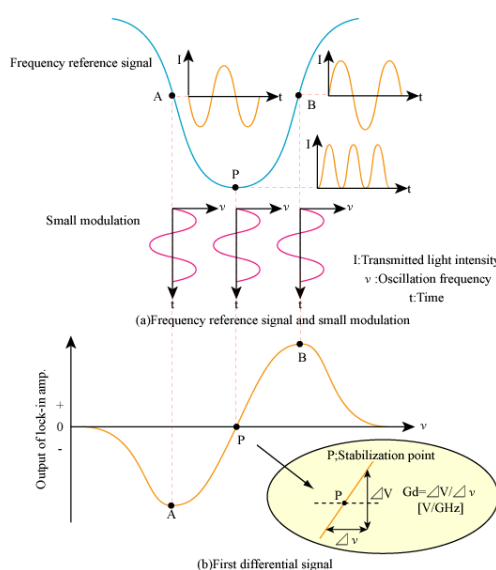


Fig.5-2 Simultaneous detection.

5.2 実験内容

以前の実験で、用いるセルを変えることで吸収量を増加させ、 G_d を増加させることができたが、セルを加熱することでもこのような効果が得られることが考えられる。これは、セルを加熱することでセル内部に吸着している固体原子を蒸発させ、セル内部の気体原子数を増やすことにより、光の吸収を起こす原子数を増加させることができるためである。すなわち、セルを加熱することによって吸収量が増加し精度の良い制御信号が得られると

予想できる。

そこで Rb セルをニクロム線で巻き、ニクロム線に電流を流すことでセルを加熱する。その状態で安定化を行い、セルを加熱した場合と常温の状態での安定度の比較を行った。

Fig.5-3 に実験に用いた光学系を Fig.5-4 に実験系を示す。半導体レーザ 1(LD1)、半導体レーザ 2(LD2)共に、注入電流には変調周波数(fm)2kHz の正弦波状の微小変調を加え、LD1、LD2 を発振させる。LD から照射された光はコリメートレンズ、光アイソレータを透過し、 $\lambda/2$ 板によって偏光方向が回転する。その後ハーフミラーによって分けられる。ハーフミラーによって分けられた一方の光は PBS によって各偏光方向に分けられる。PBS で分けられた光はプローブ光、飽和光としてそれぞれ Rb セルを透過し、飽和吸収分光光学系を形成している。プローブ光は各々のアバランシェホトダイオード(APD)で受光される。各 APD で得られた波形は飽和吸収分光法を用いた吸収波形となり、各 LD の安定化に用いられる。また、ハーフミラーによって分けられたもう一方のレーザ光はビート信号用に光軸を合わせて APD3 で受光される。Rb セルを加熱することによる周りへの影響を軽減するために LD と Rb セルは断熱素材で作られた箱で覆っている。

用いられているロックインアンプ(Lock-in Amplifier)には参照信号として、周波数(fr)が 2kHz の方形波が加えられている。そして、それぞれのロックインアンプの時定数(τ)は 0.01s にする。各々の LD から放出されたレーザ光を外部周波数基準である Rb セルに透過させ、APD で受光することにより、透過光強度波形を得る。この波形をロックインアンプで同期検波することにより一次微分波形、即ち誤差信号を得ることができる。この誤差信号から電流制御器(Current Controller)で制御信号を得て、電流ドライバ(Current Driver)から半導体レーザの注入電流にフィードバックする。このようにして、各々の LD の安定化を行う。また、LD1、LD2 共に 1/1000K 以下の温度制御が可能な温度コントローラ(Temperature Controller)により温度制御が施されている。また、LD1、LD2 からの 2 つのレーザ光の光軸を合わせて APD3 で受光してビート信号を検出し、周波数カウンタ(Frequency Counter)によって 2 つのレーザ光の周波数差をビート周波数として測定する。検出されたビート周波数をコンピュータ(Computer)に取り込み、アラン分散の平方根を計算することにより安定度の評価を行う。

このような光学系、実験系において常温の状態での安定化を行った場合と Rb セルにニクロム線を巻き、ニクロム線に電流を流し約 40℃まで加熱した状態で安定化を行った場合での安定度の比較を行った。

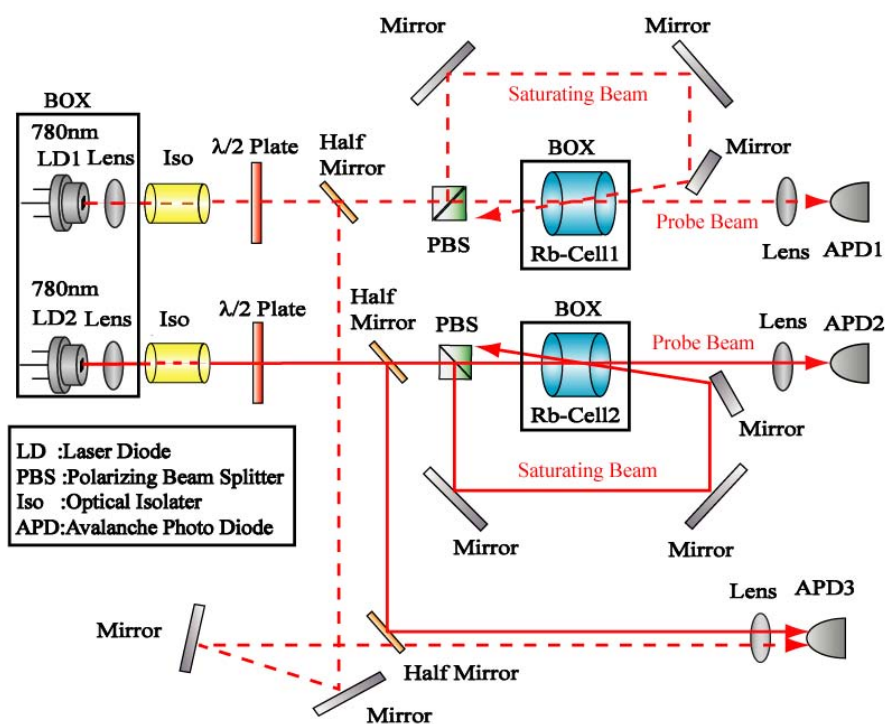


Fig.5-3 Optical setup.

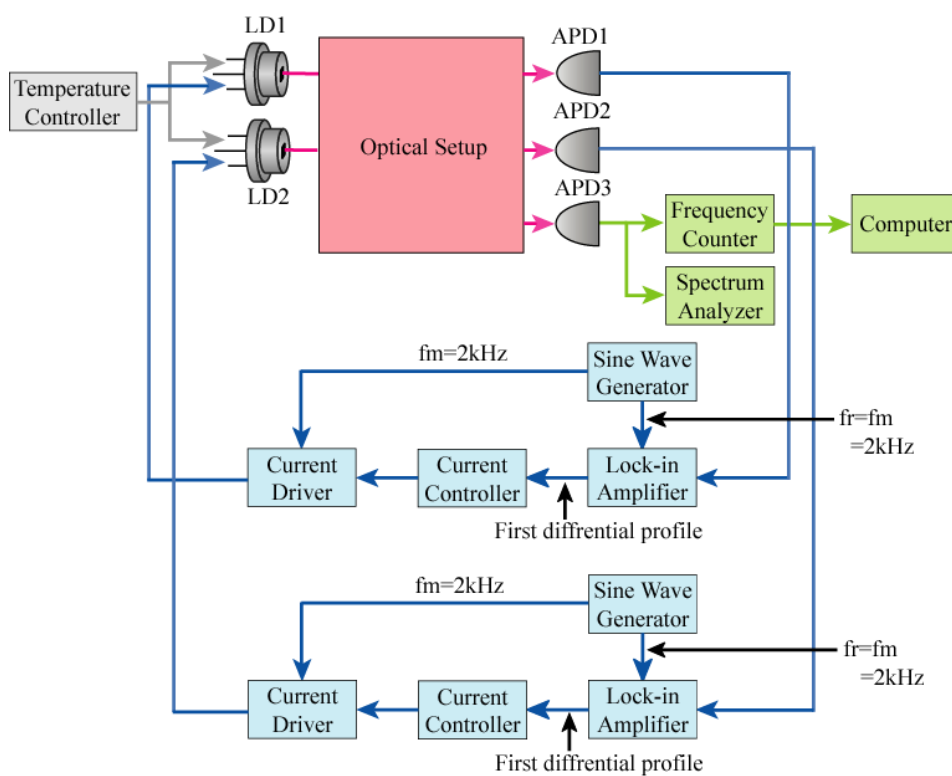


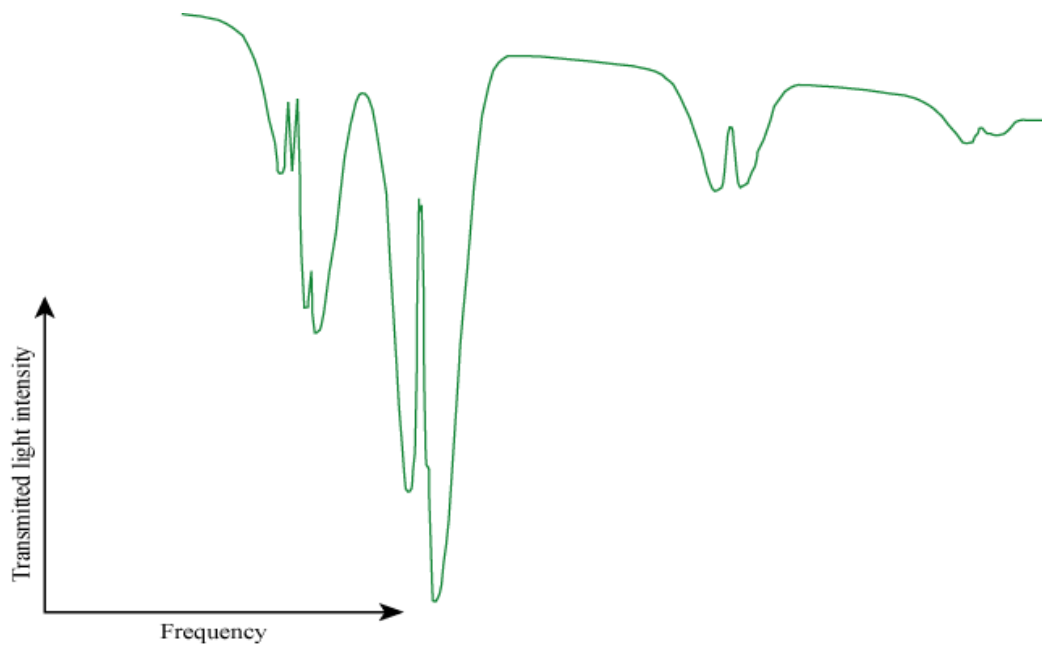
Fig.5-4 Experimental setup.

5.3 実験結果

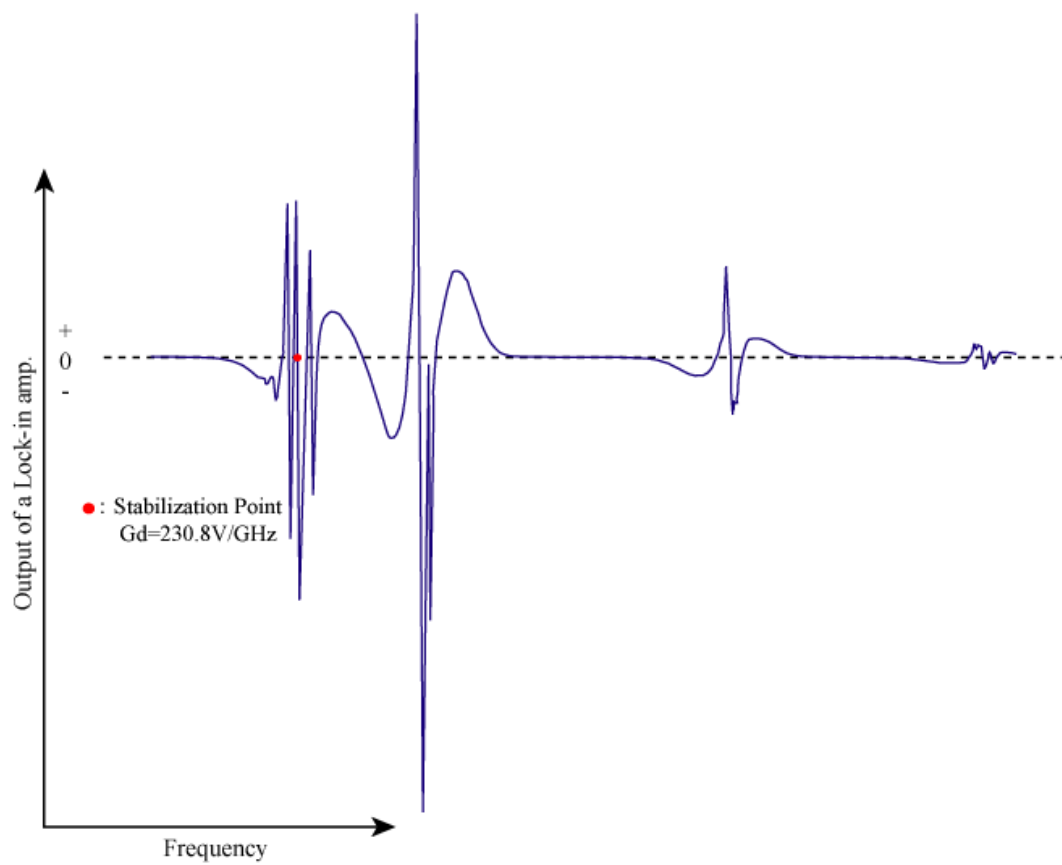
Fig.5-5 に Rb セルをニクロム線で加熱した状態で得られた LD1 での吸収線波形とそのロックインアンプ出力を示す。このときのセル付近の温度は 40.23°C であった。セル付近とは、セル内部の温度を測定することが出来ないため、セルにサーミスタを接着させて測定した値である。同様に Fig.5-6 にニクロム線で加熱した状態で得られた LD2 での吸収線波形とそのロックインアンプ波形を示す。このときのセル付近の温度は 42.10°C であった。各安定化点での G_d は LD1 で常温の状態が 213.0V/GHz 、Rb セルを加熱した場合が 230.8V/GHz であった。また、LD2 では常温の状態が 213.3V/GHz 、Rb セルを加熱した場合が 329.5V/GHz であった。LD1、LD2 共に Rb セルを加熱した方が G_d が増大した。

吸収量の違いがわかりやすいように Fig.5-7 に LD1 で得られた常温の状態と Rb セルを加熱した状態の吸収線波形を同一の縮尺で重ね合わせたものを示す。吸収量の小さい波形が常温 (22°C) の状態で得られた吸収線波形、吸収量の大きい波形が Rb セルを加熱した状態 (40°C) で得られた吸収線波形である。Rb セルを加熱した状態の方が常温の状態に比べ大きな吸収が起こっていることがわかる。

常温の状態と Rb セルを加熱した状態で安定化を行った場合の安定度の比較を Fig.5-8 に示す。●で示されているものが常温の状態での安定化を行った場合の安定度、◆で示されているものが Rb セルを加熱した状態での安定化を行った場合の安定度である。全体的に Rb セルを加熱した状態で安定化した方が安定度が向上した。しかしながら大幅な安定度の向上は見られなかった。

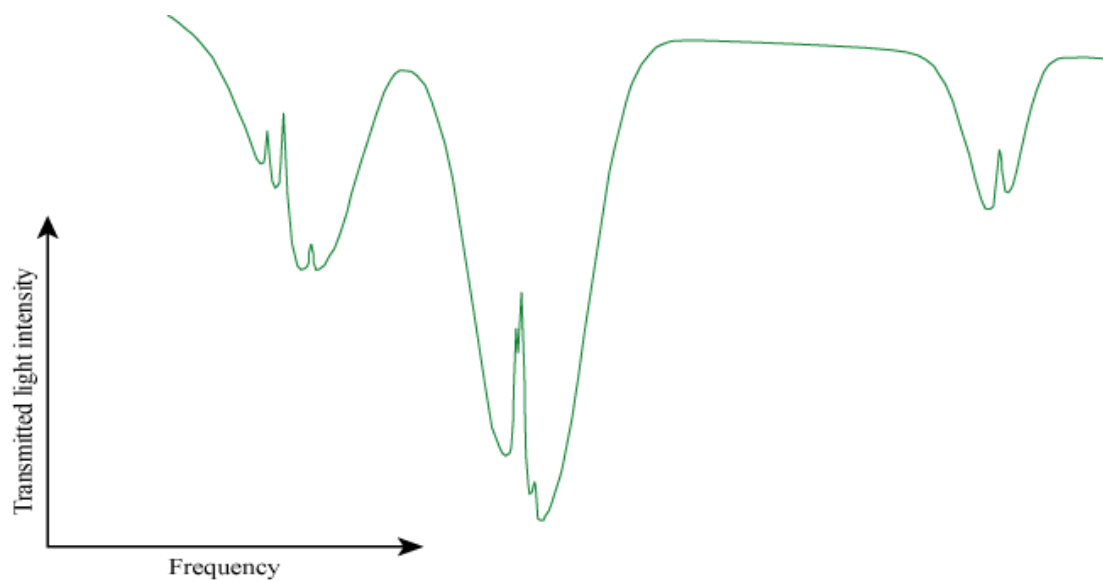


(a) Rb-D2 absorption line using the saturated absorption spectroscopy

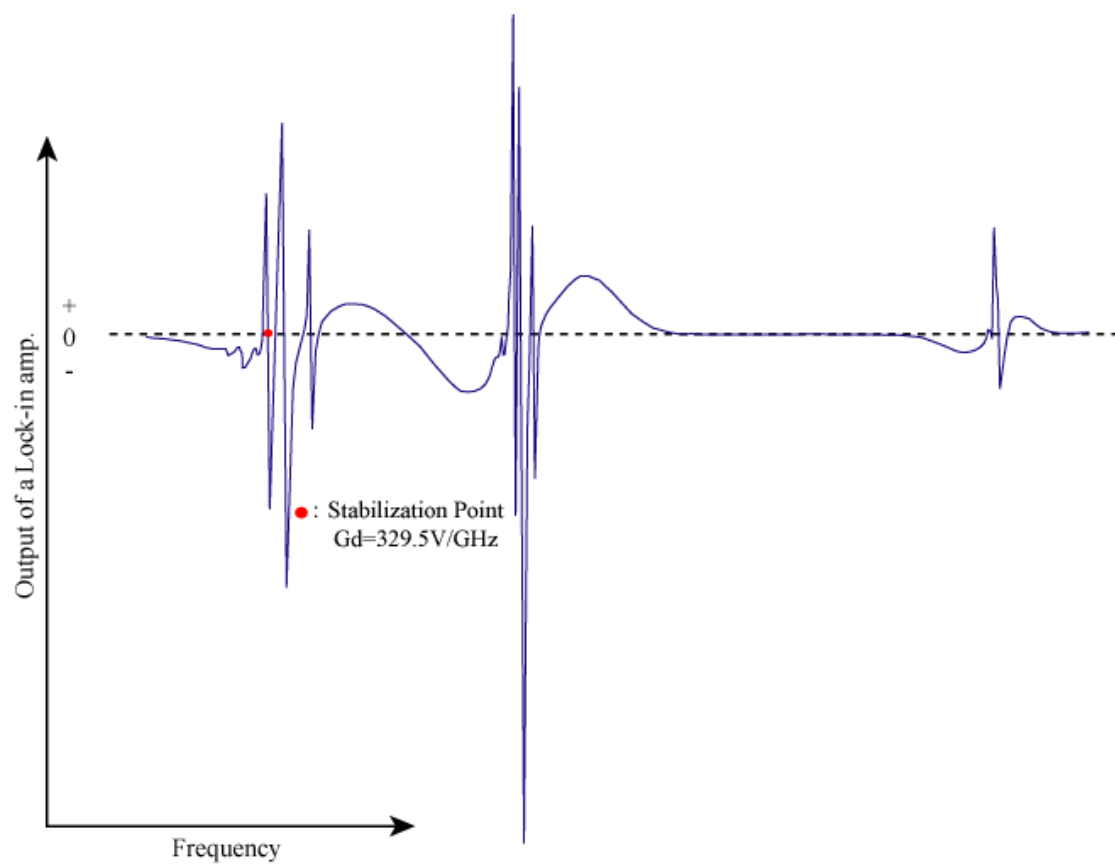


(b) Output of a Lock-in amp.

Fig.5-5 Observed profiles of the Rb absorption line at LD1 and its output of a Lock-in amp.



(a) Rb-D2 absorption line using the saturated absorption spectroscopy



(b) Output of a Lock-in amp.

Fig.5-6 Observed profiles of the Rb absorption line at LD2 and its output of a Lock-in amp.

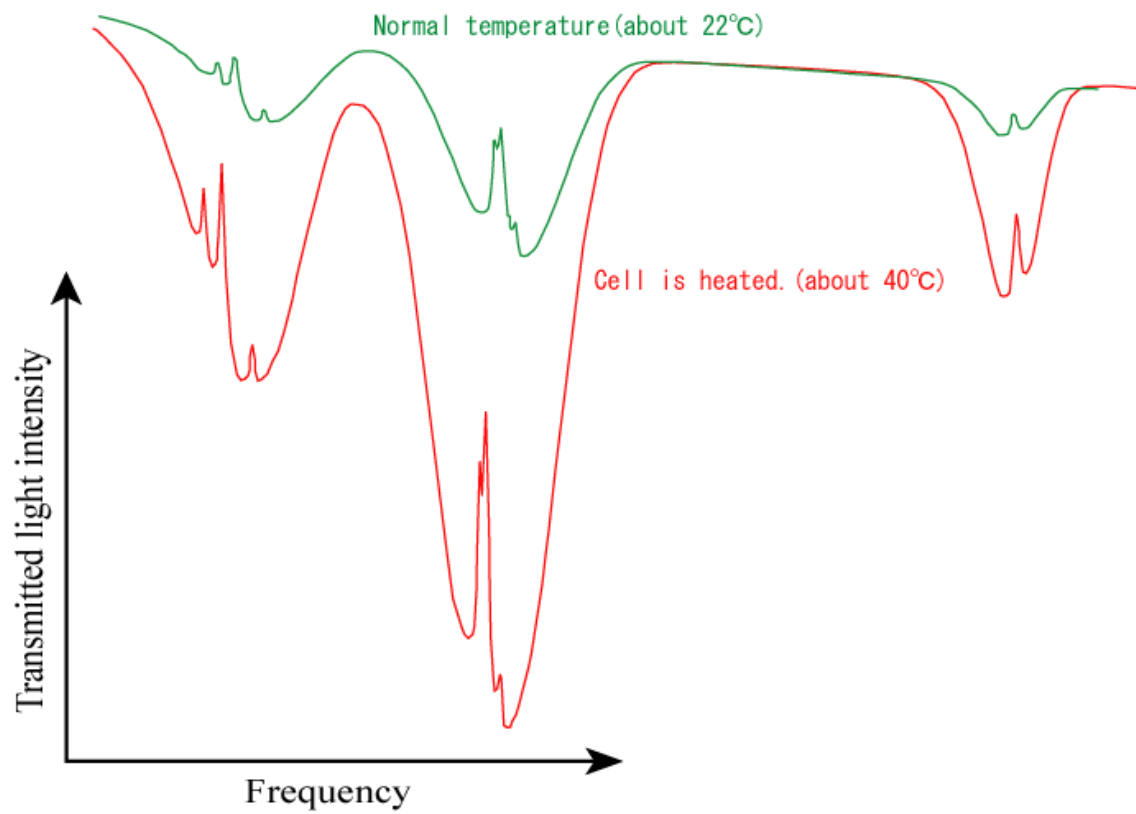


Fig.5-7 Comparison between observed profiles of the Rb absorption line at normal temperature and observed profiles of the Rb absorption line when heated cell.

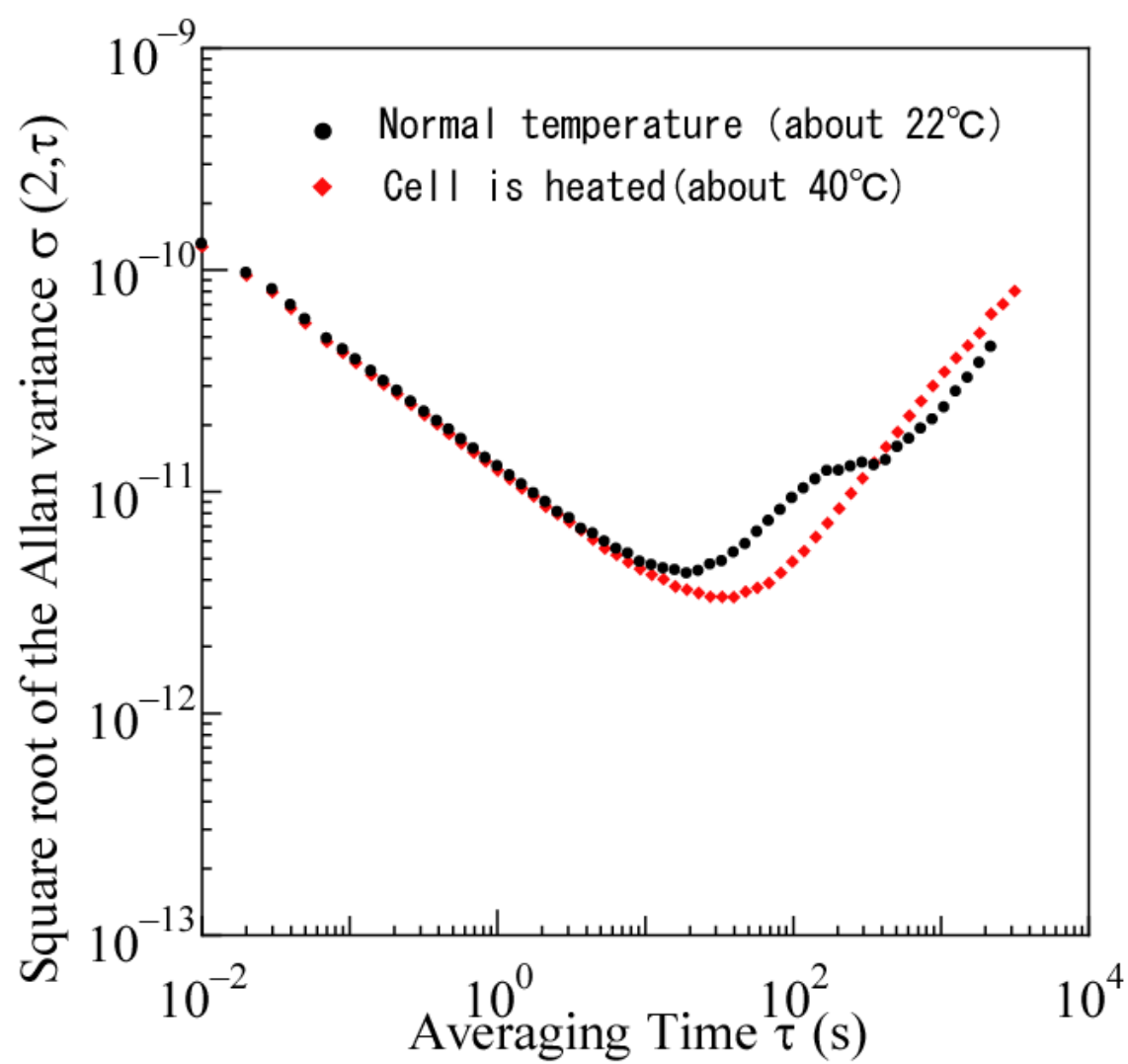


Fig.5-8 Experiment result

5.4 考察

Rb セルを常温の状態で行った場合に比べ Rb セルを加熱した状態で行った場合の方が吸収量が増加している。これは、Rb セルを加熱することによりセル内部に吸着している Rb 原子が蒸発しセル内部の気体原子数が増加、それにより光の吸収を起こす原子数が増加し結果的に吸収量が増加したと考えられる。それに伴い G_d の増大も見られる。また、Rb セルを常温の状態で行った場合に比べ、Rb セルを加熱した状態で行った方が安定度の向上が見られた。

しかしながら、これだけの吸収量の増大が見られていることを考えるともっと安定度の向上が見られてもいいのではないかと考えている。期待した通りに安定度の向上が見られなかった原因としては Rb セルを加熱することで雰囲気温度に影響し、LD や受光素子 APD などの熱的なノイズが増加した可能性が考えられる。また、Rb セルの加熱方法として、ニクロム線に電源から電流を流し続けただけであり温度が一定になるような制御を一切施していないため、温度変動によって安定化点が揺らいでいる可能性も考えられる。

第 6 章 外部変調方式によるレーザ周波数安定化

第 5 章で議論した直接変調方式による安定化では、半導体レーザの注入電流を微小変調することで、安定化しようとしている半導体レーザの周波数そのものに変調を加えているため、発振スペクトル幅を広げてしまうという欠点がある。

そこで、本章では吸収線の磁気光学効果であるファラデー効果を用いた磁界変調方式による安定化について述べる。この方式は、外部周波数基準に変調を加える方式で、この方式による安定化では、変調に伴う発振スペクトル幅の広がりとは問題とならない。

6.1 磁界変調方式による周波数安定化の原理

6.1.1 Faraday Normal 方式

ここでは、ファラデー効果によって安定化のための制御信号が得られる原理について述べる。レーザ光をそれぞれ磁界 H_1 、 H_2 ($H_1 < H_2$) が印加されている Rb セルを通過させると、ファラデー効果により偏光面が回転する。半導体レーザの発振周波数を Rb の吸収線付近で掃引しながら、偏光面の回転の効果を直線偏光板 (LP) を利用して光強度の変化に変換し観測される透過光強度信号が、それぞれ Fig.6-1(a) に示すような透過光強度信号になるとする。この透過光強度は Fig.6-1(b) のように A 点の周波数では磁界の増加にともない、偏光面と LP のなす角が減少し、透過光強度は増加する。B 点の周波数では磁界が変化しても偏光面が回転しないために透過光強度は変化しない。C 点の周波数では A 点とは逆の変化となる。そこで、Fig.6-1(c) のような大きさ $(H_1 + H_2)/2$ の直流磁界に、振幅 $(H_1 - H_2)/2$ の交流磁界を重ねし変調を加えると、それぞれ Fig.6-1(d) に示すような透過光強度の変化となり、この信号をロックインアンプにより変調周波数で同期検波したときの出力は A 点では正、B 点では零、C 点では負となるので、ロックインアンプ出力波形は Fig.6-1(e) のようになる。従って B 点の周波数を基準とすると、ロックインアンプ出力波形は B 点からのずれに対応した出力となるので、この出力を制御信号としてレーザの注入電流にフィードバックすれば、発振周波数の安定化を行うことができる。この方式ではレーザの注入電流にはまったく変調を加えていないため、発振スペクトルが広がるようなことはない。また、交流磁界の大きさを変えた場合の透過光強度信号とロックインアンプ出力波形を Fig.6-2 に示す。交流磁界の大きさにより G_d が変化することが予想される。この方式で安定化したものを Faraday Normal 方式と呼ぶことにする。

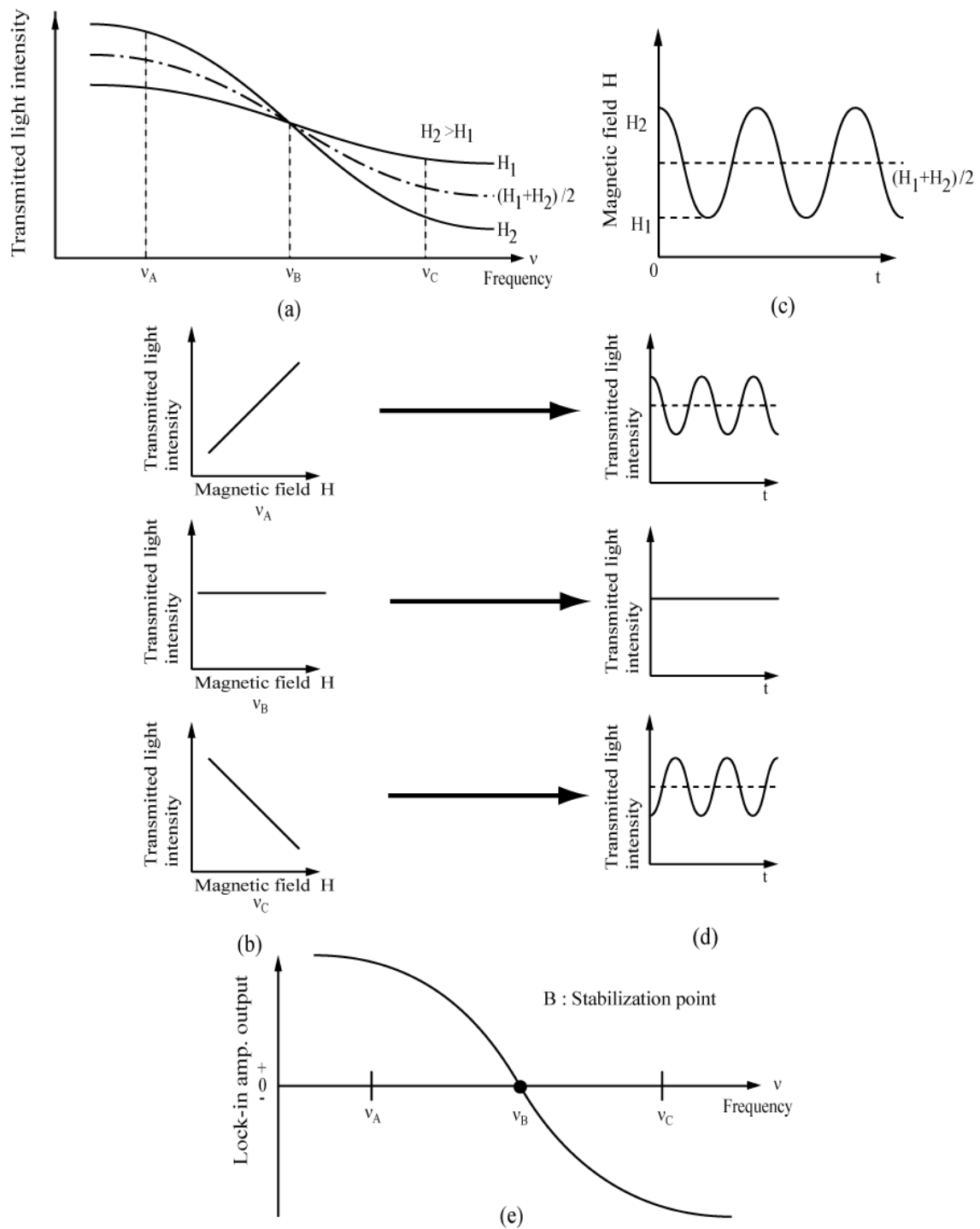
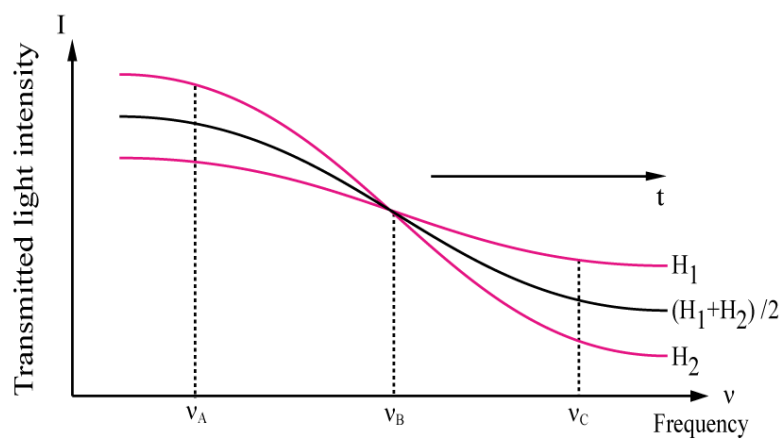
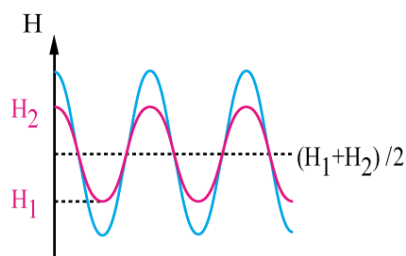


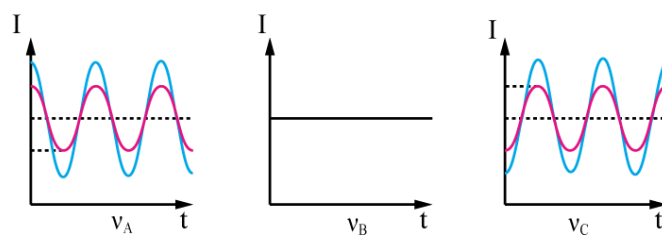
Fig.6-1 Principle of a magnetic modulation method by the Faraday effect(1).



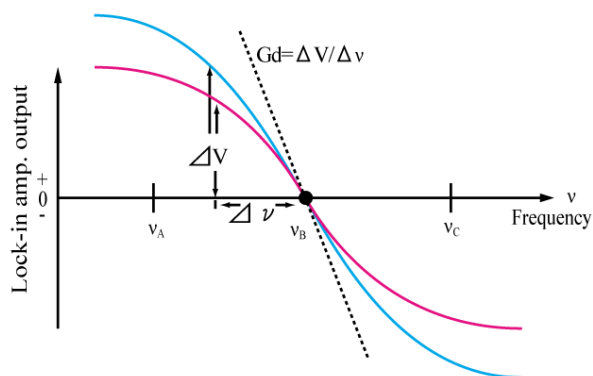
(a)



(b)



(c)



(d)

Fig.6-2 Principle of a magnetic modulation method by the Faraday effect(2).

6.1.2 Faraday PEAK 方式

PEAK 方式とは異なる 2 つの透過光強度信号を重ね合わせ、信号強度の強い方のみを回路で取り出しロックインアンプで同期検波することでロックインアンプ出力に飛びを生じさせる方法である (Fig.6-3)。このロックインアンプ出力の飛びによって作り出したゼロクロス点に安定化することで理論上無限大の周波数弁別利得 G_d を得ることができる。したがってこの周波数弁別利得を持った信号を用いれば安定度の向上が期待できる。

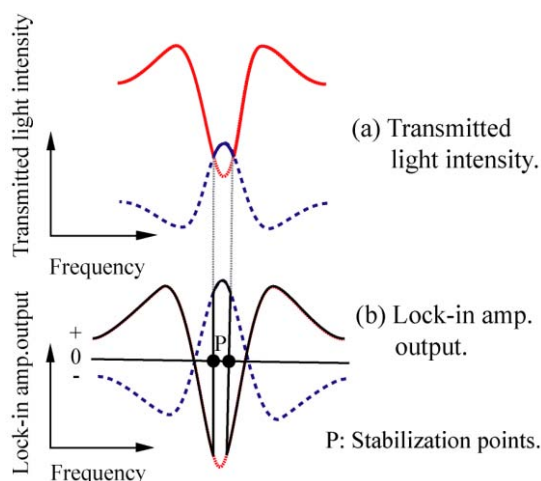


Fig.6-3 Principle of the Faraday PEAK method.

6.2 実験内容

本研究ではファラデー効果を利用して Rb セルに直流磁界と交流磁界を重ね合わせたものを印加することにより、安定化を行なっている。過去の実験においては、ノイズの低減、つまり半導体レーザの熱雑音低減を目標に掲げ、レーザマウントの温度制御を 1/100K の制御から 1/1000K へと改善することにより、Faraday Normal 方式において安定度を向上させた。そこで今回は制御信号の増加、つまり G_d の向上を目的として過去において Faraday Normal 方式と比べ G_d の向上ならびに安定度の向上が確認できた PEAK 方式を導入することにより周波数安定度向上を目指した。ファラデー効果を用いる場合、Rb セル前後の偏光板の設定により得られる透過光強度信号が変わってくる。PEAK 方式では、Rb セル後の偏光方向の設定が重要となる。

今回の実験では温度制御 LD1 電流 71mA、LD 1 温度表示 8.675k Ω 。LD2 電流 81mA、LD2 温度表示 7.191k Ω 、Rb セルに印加される磁界は LD1、LD2 の系ともにヘルムホルツコイルへの直流電流 3A により発生される直流磁界約 100 ガウスと 8V_{p-p} と 1.3kHz により発生される交流磁界を重ね合わせたものを印加している。

Fig.6-4 にファラデー効果を用いた PEAK 方式の光学系、実験系を示す。±1/1000K 程度までの制御が可能な温度コントローラを用いて温度制御された LD1 より発振したレーザ光はレンズによってコリメートされた後、光アイソレータ(ISO)を通り、LP1 で直線偏光とな

る。磁界変調を加えられた Rb セルを通過したレーザ光は、ファラデー効果により偏光面の回転角に変調を加えられ、ビームスプリッタ(BS)によって2つに分けられそれぞれ等価的に $+\pi/4[\text{rad}]$ と $-\pi/4[\text{rad}]$ に設定した LP2、LP3 を通過し APD1、APD2 で受光される。APD1、APD2 で得られる透過光強度信号は Fig.6-3(a) のような信号波形となる。LP をそれぞれ等価的に $+\pi/4[\text{rad}]$ と $-\pi/4[\text{rad}]$ にすることにより、APD2 で得られる信号は APD1 で得られる信号に対して反転した信号となり、PEAK 方式に適した信号となる。

APD1、2 で得られた2つの信号は識別回路 (PEAK Circuit) により出力の大きい方の信号だけが取り出され、ロックインアンプに入力される。この信号を変調周波数で同期検波することで得られる制御信号に PID 制御を施し、レーザの駆動電流にフィードバックすることで安定化が行われる。便宜上この安定化の方式を Faraday PEAK 方式と呼ぶことにする。

また、LD2 を用いて同じ系を組み上げる。BS1、BS4 によってそれぞれ分けられたレーザ光を干渉させて Lens5 で集光、APD3 で受光する事でビート信号として観測し、得られたデータをアラン分散の平方根値を算出することで評価している。

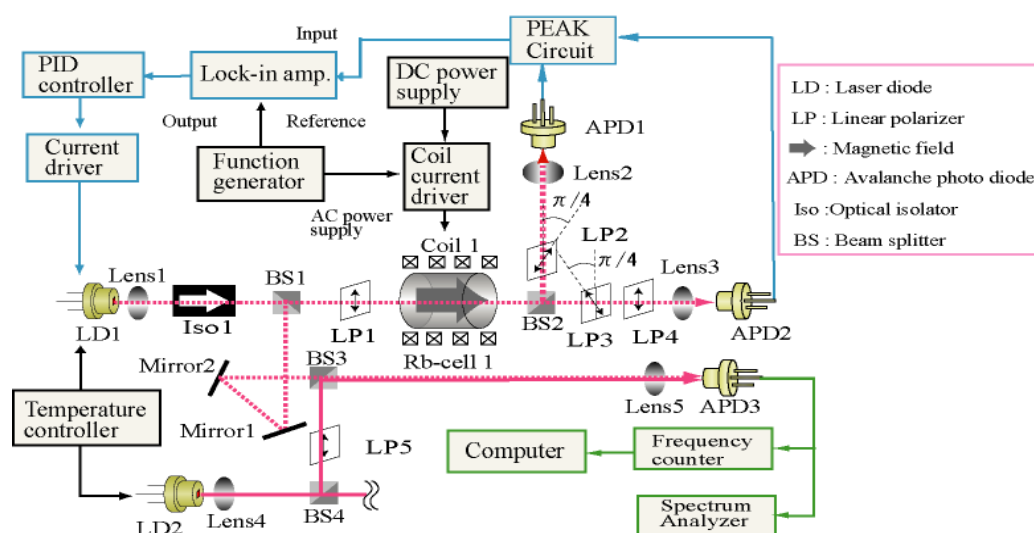


Fig.6-4 Optical and Experimental setup of the Faraday PEAK method.

6.3 実験結果

Fig.6-5 に今回の実験結果をアラン分散の平方根値で示す。Fig.6-5 おいて “●” はフリーランニング (LD マウント温度制御のみ)、“○” は Faraday Normal 方式 (Fig.6-4 において BS2 ならびに PEAK 回路を用いない方法)、“▼” は Faraday PEAK 方式の実験結果を表している。

今回、温度制御が向上した状態で Faraday PEAK 方式を用いたことによって、Faraday Normal 方式と比較して特に $\geq 0.3\text{s}$ において顕著な安定度向上が確認できた。しかし、過去

の実験から Faraday PEAK 方式を用いた際は、長期の安定度よりも短期の安定度が向上してきたという結果が示されている⁽²⁰⁾。よって、今回の実験データは再実験の必要があるものと考えている。

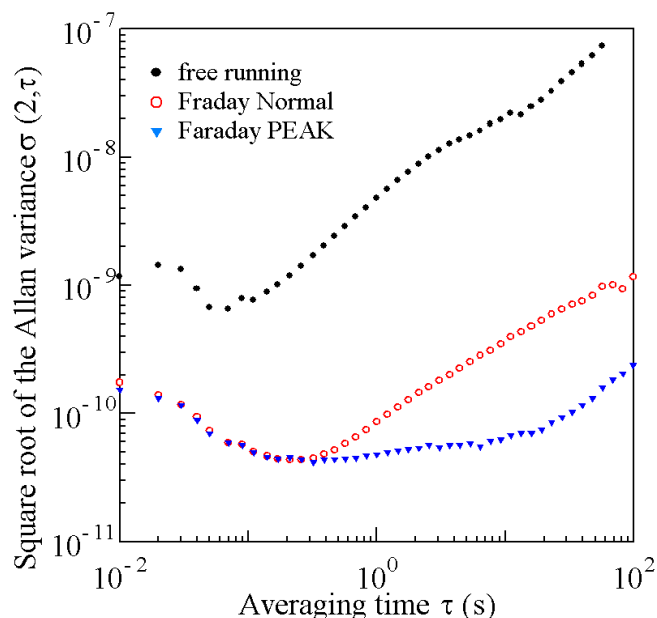


Fig. 6-5 Frequency stabilities

6.4 考察

今回の実験結果において最も気になる点は $\tau = 10^{-2} \sim 3 \times 10^{-1}$ の区間において Faraday PEAK 方式と Faraday Normal 方式の安定度が完全に重なっている点である。過去の実験から本来 Faraday PEAK 方式を用いることにより、短期における安定度改善というものが見られるという結果が得られている。それにも関わらず今回の Faraday PEAK 方式における安定化において予想どおりの結果が得られていない理由としては、過去に行われた実験との違いが安定度向上に影響しているものと考えられる。下に過去の実験と大きく異なる箇所を示す。

- ・ 半導体レーザの型番
- ・ レーザマウント
- ・ レーザ温度制御精度
- ・ レーザドライバならびに制御回路
- ・ ヘルムホルツコイル
- ・ PEAK 回路

上 4 つの項目については Faraday Normal 方式で全平均化時間において安定度が向上していることから影響しているとは考えられない。ヘルムホルツコイルについては、過去のものと比較すると直流磁界量と磁界範囲ともに増加、また単純に考えて発熱量も 2 倍になっ

ている。これらのことから現在の吸収波形は過去のものと比較して鋭いものが得られている。これがかえって Faraday Normal 方式と Faraday PEAK 方式での G_d の差を少なくし、安定度においても Faraday Normal 方式との差を少なくした可能性が考えられる。PEAK 回路については発振防止のために利得が過去の回路よりも減少している。この点も結果に大きく影響していると思われる。また、PEAK 回路は同一基板上に回路としては絶縁された形で 2 つの PEAK 回路が搭載されている。理論上は 2 つが互いに影響を及ぼすことはなく、及ぼさないように設計されてはいるが、実際、実験を行った時には、片方の回路のみ使用した時と両方を使用した時とでは片方のみ使用した際は信号が不安定になりにくかった。よって PEAK 回路は回路上だけでなく、基板上でも個々に分けるべきだと考えている。しかし長期においては安定度が向上していることから今回の結果は再実験による再現性の確認が必要不可欠である。

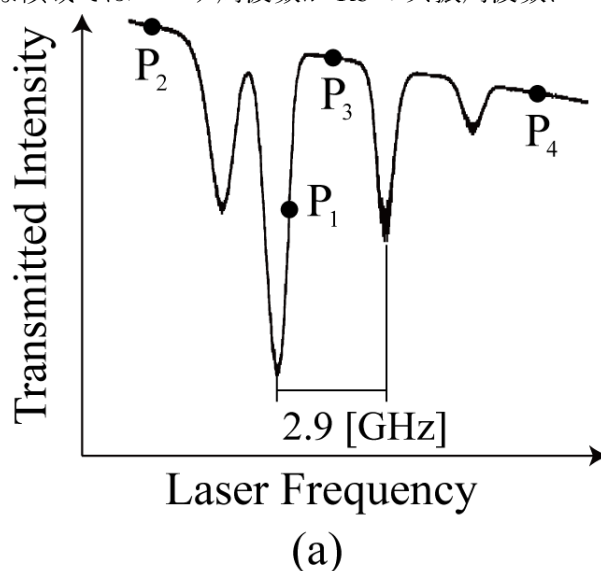
また、PEAK 方式を使った光学系を用いる際に説明上 LP2 を LP1 と比較して ± 45 度という表現をしているが、実際は BS によって反射されているため両方とも同じ方向に 45 度傾けている。PEAK 方式を用いた場合、その 2 つの LP の設定が大きく異なると切り替え点での信号の変調度合いも異なってしまう。これが安定度に影響を及ぼす可能性もあるために光学系の組み方を、ビート信号観測用に用いている BS を $\lambda/2$ 板と PBS に交換し、PEAK 用のセル通過後の BS の後に設置してある LP を BS の前に持ってくる。このようにすることで PBS によって透過する光は P 偏光となるため LP の設定角度を 45 度に設定することで、その後に設置してある BS で透過する光と反射する光が綺麗に対象の光となり切り替え点での変調の誤差をなくすることができる。

第7章 物理乱数の生成

近年、半導体レーザの強度雑音や戻り光雑音などを積極的に利用して、物理乱数の高速生成を行うという研究が注目され始めている^{(46-55), (57-61)}。これまでに報告された論文では、主に半導体レーザの戻り光雑音によるカオス特性を利用した乱数の高速生成が行われている⁽⁴⁷⁾⁻⁽⁵⁰⁾。一方、本研究室でも、半導体レーザ固有の強度雑音特性を利用して物理乱数を生成してきたが⁽⁴⁶⁾、現在の研究では、半導体レーザの周波数雑音特性を用いた物理乱数の高速生成を行っている^{(54), (55), (57-61)}。

7.1 周波数雑音を用いた物理乱数生成の原理

半導体レーザの周波数雑音は、周波数弁別器を用いると、スペクトルのランダムな動きに応じた振幅揺らぎの信号として変換される。このため、このメカニズム（機構、原理）を利用して物理乱数を生成することが可能である。本研究では、Rb 原子の D_2 吸収線（波長 780nm）を周波数弁別器として用いて、半導体レーザの周波数雑音を透過光強度信号に変換している。Fig.7-1 に、その変換原理を示す。Fig.7-1(a)では、レーザの注入電流を掃引することによって得られた Rb 原子の D_2 吸収線の波形を示している。吸収スペクトルが急勾配なとき、レーザ周波数のわずかな揺らぎでも、光強度においては、十分大きな揺らぎとして変換されることがわかる。それゆえ、吸収線スペクトルが最も急勾配な P_1 点にレーザ周波数は設定される。Fig.7-1 (b)は、レーザ周波数が P_1 点付近で揺らいだ時に、Rb 原子の D_2 吸収線によって、強度雑音に変換される様子を示している。 P_1 点は、急勾配な傾きであるため、大きな強度雑音信号を得ることができる。このため、この信号を光センサで検出すれば、周波数雑音に起因した物理乱数を生成することが可能となる。これに対して、参照用となる P_2 、 P_3 、 P_4 点のような領域では、周波数雑音は透過光強度雑音に変換されない。なぜなら、そのような領域ではレーザ周波数が Rb の共振周波数に一致しないためである。



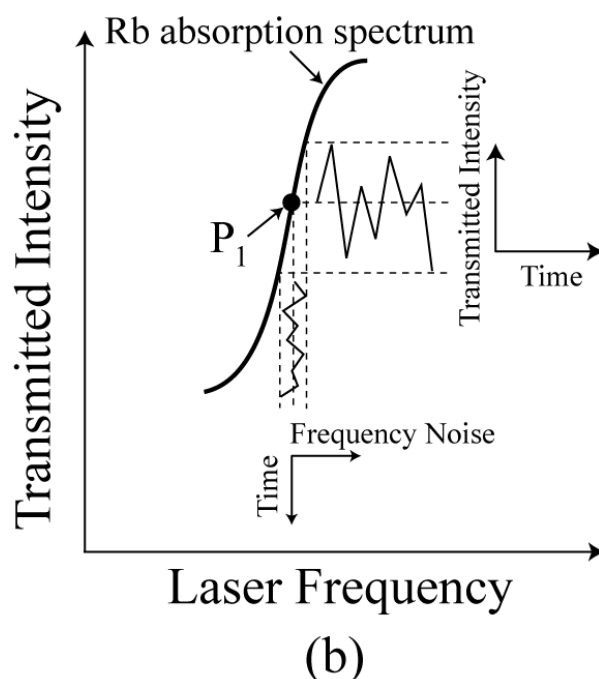


Fig. 7-1 (a) Observed Rb-D₂ absorption line and (b) Conversion of laser frequency noise to laser intensity variation. The laser frequency is set at point P₁, by tuning the injection current.

Rb セルを透過して光検出器で得られた光強度信号は、デジタルオシロスコープに内蔵された A/D コンバータで 2 進数へ変換される。こうしてサンプリングされた電圧値は、AD 変換されて 2 進数データとなり、Fig. 7-2 に示すように、各ビットでデータを横方向で見た場合、8 組の乱数列を同時に生成することが可能となる。

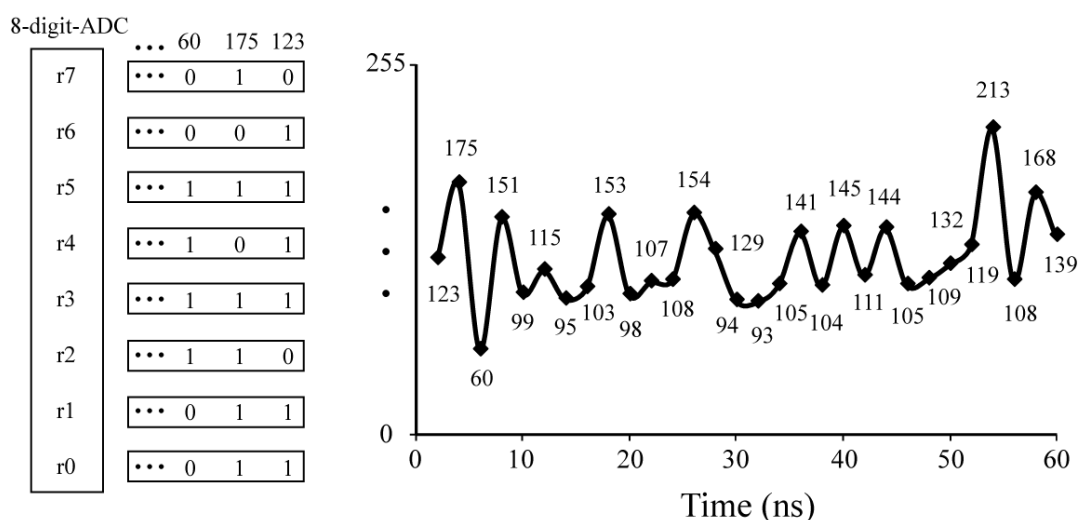


Fig. 7-2 Random number generation by means of transmitted light signals. A transmitted light signal is sampled at 500MHz. Its voltage is converted to 8-bit binary data, from which we obtain 8 random bit streams at a time.

7.2 物理乱数生成システム

Fig.7-3 に物理乱数生成のための実験系を示す。使用したレーザは、出力 70mW の単一モードレーザ (Sanyo, DL-7140-201) で、低雑音の電流源により 780nm でレーザ発振することができる。実験時は、レーザ周波数を Rb 原子の D_2 吸収線に合わせるために、注入電流やレーザ温度の条件を調整している。本研究では、注入電流を 73mA 付近で動作させ、レーザ温度は、温度コントローラ (Yamaki, KLT-2E) により 292 K に設定して実験を行った。なお、レーザ温度は 1/100K 以下で温度制御が施されている。

レーザ光は、光アイソレータを通過し、それから Rb セルを通過する。光強度信号は、アバランシェフォトダイオード (Hamamatsu, S2381, 1GHz bandwidth) によって検出され、その後の電圧信号は、高周波増幅器 (COSMOWAVE, LPA-G39WD, 50MHz-8GHz) によって増幅される。本研究では、デジタルオシロスコープ (LeCroy, Wave Runner 62Xi-A, 600MHz bandwidth) が、サンプリング速度が 500MS/s で、分解能が 8bit の AD コンバータ (ADC) として用いられる。このため、8bit の ADC でサンプリングされた光強度信号は、先に示した Fig.7-2 のように、8 桁のビット列に変換され、コンピュータに取り込まれる。その後、8 組のビット列は、暗号用乱数の統計的乱数性評価法として用いられている NIST の FIPS140-2⁽⁸³⁾ や SP800-22⁽⁸⁴⁾ の評価法を用いて検証する。また、本実験では、透過光強度の周波数雑音スペクトルを同時に測定するために、スペクトラムアナライザ (ROHDE&SCHWARZ, FSU3, 20Hz-3.6GHz bandwidth) も用いている。

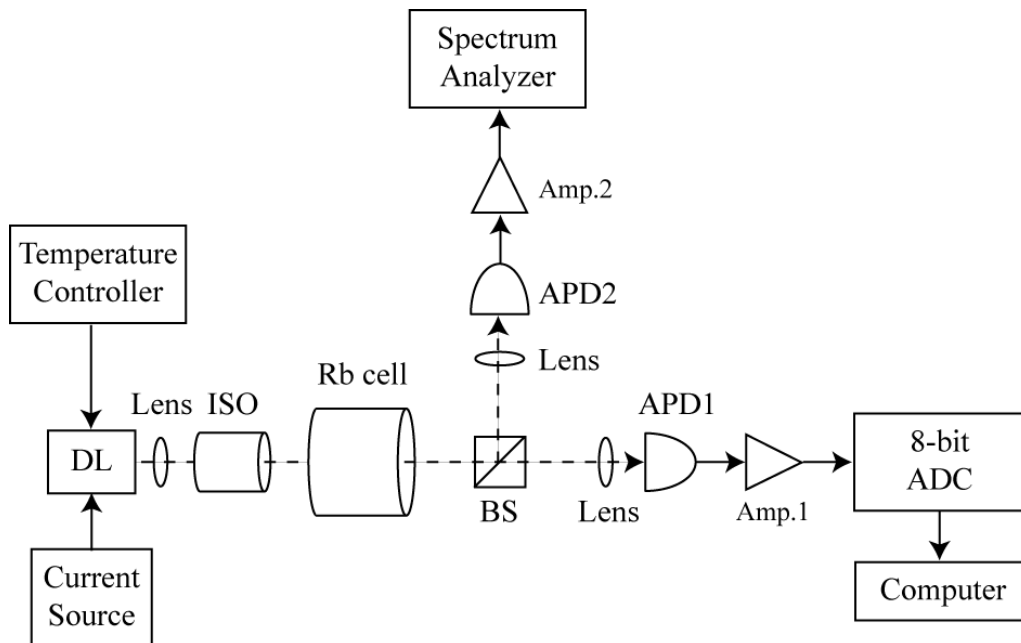


Fig. 7-3 Experimental setup. DL: Diode laser, ISO: Optical isolator, BS: Beam splitter, APD: Avalanche photo diode, Amp: Amplifier, ADC: Analog/digital converter.

7.3 実験結果と考察

藪崎らの論文では、Cs の D_1 吸収線を介してレーザ周波数がゆっくりと掃引された時、透過したレーザビームの強度変化が観測されたと報告^{(4.2), (4.3)}されているが、Fig. 7-4 は、Rb の D_2 吸収線を用いて同様の実験を行った時の波形を示している。レーザ周波数がゆっくりと掃引されるとき、レーザ周波数が Rb の D_2 吸収線に一致する領域では、レーザ周波数の変動が Rb の D_2 吸収線の傾きに応じて光強度に変換されていることが分かる。それ以外の領域では、レーザ周波数の変動が光強度へ変換されないことを示している。

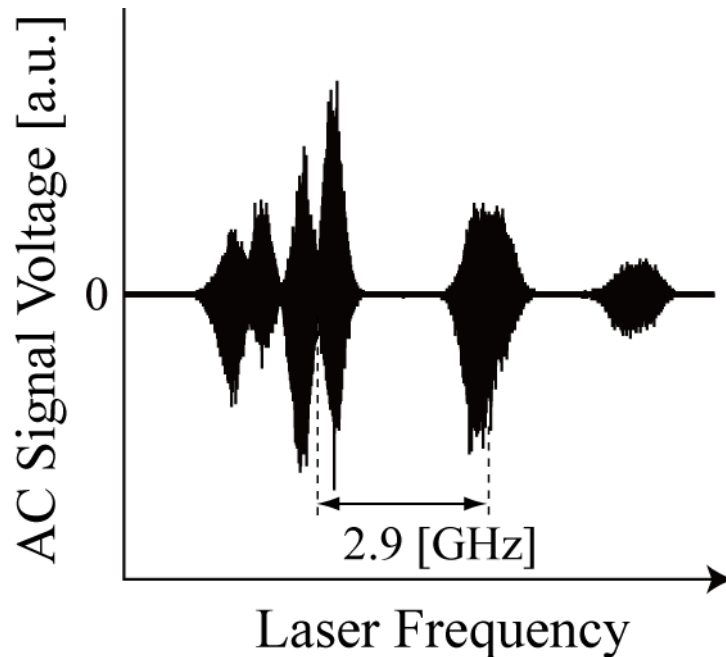
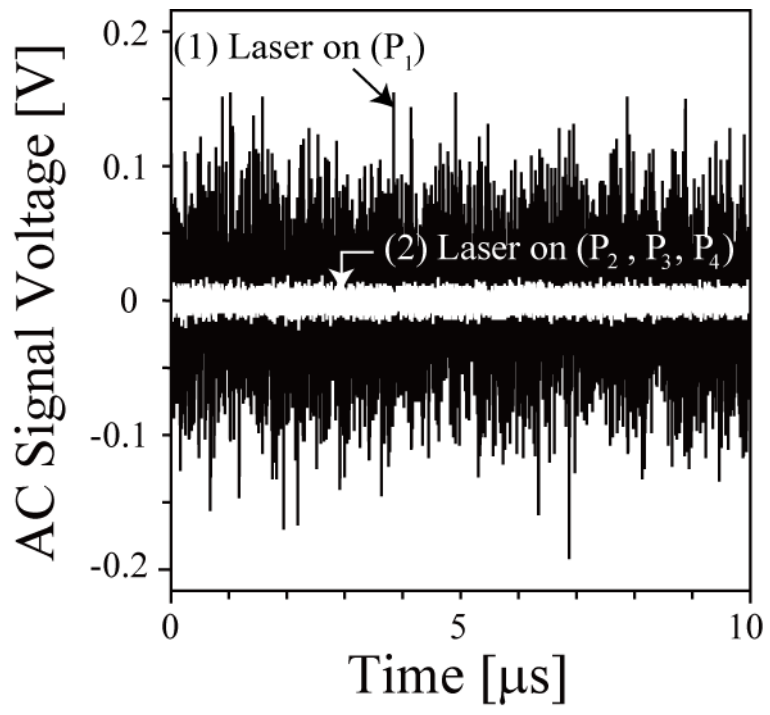
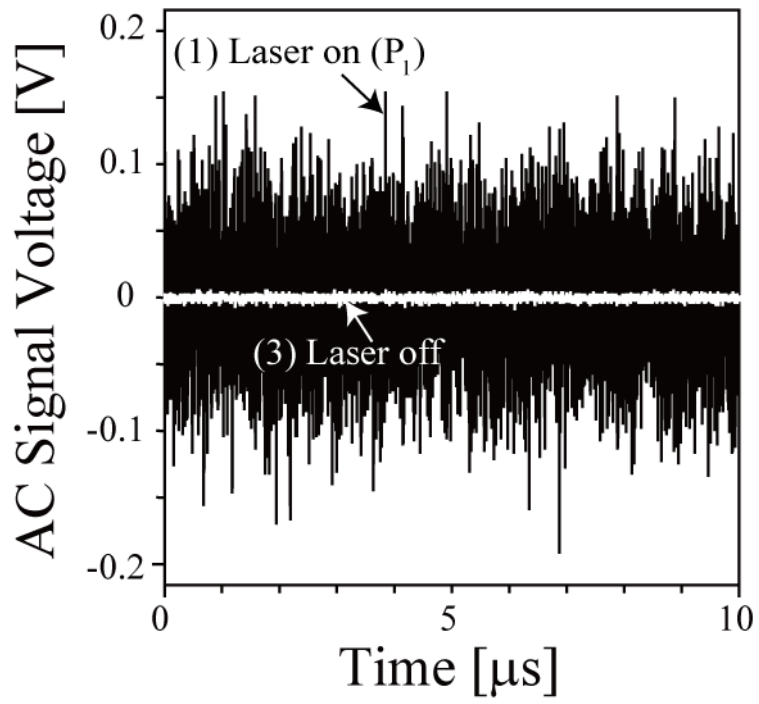


Fig. 7-4 Conversion of a frequency noise to a transmitted light intensity noise. As the laser frequency was slowly swept through the Rb- D_2 absorption line, we recorded the alternative current (AC) voltage output.

Fig.7-5 は、周波数弁別器で変換された光強度信号波形を示す。本実験では、注入電流を 73mA に調整することで、 P_1 点にレーザ周波数を設定する。この点は、先の Fig.7-1 で示したように、Rb の D_2 吸収線の傾きが最も急勾配な位置である。Fig.7-5 (a)における(1)は、デジタルオシロスコープ上に表示された信号波形を示している。また、(2)は、先の Fig.7-1 に示したように、 P_1 とは異なる点 (P_2 、 P_3 、 P_4) で観測された信号波形を示している。ここで、レーザ光が APD の前で遮られた時、Fig.7-5 (b)のような波形を得ることができた。これに対して、Fig.7-5 (c)は、スペクトラムアナライザによって測定された透過光の周波数雑音スペクトルを示している。結果として、本実験では、 P_1 点で観測された周波数雑音成分を 1GHz までの周波数帯域において十分に利用できていることがわかる。したがって、APD で検出されたこれらの雑音で生成した物理乱数を評価することにする。



(a)



(b)

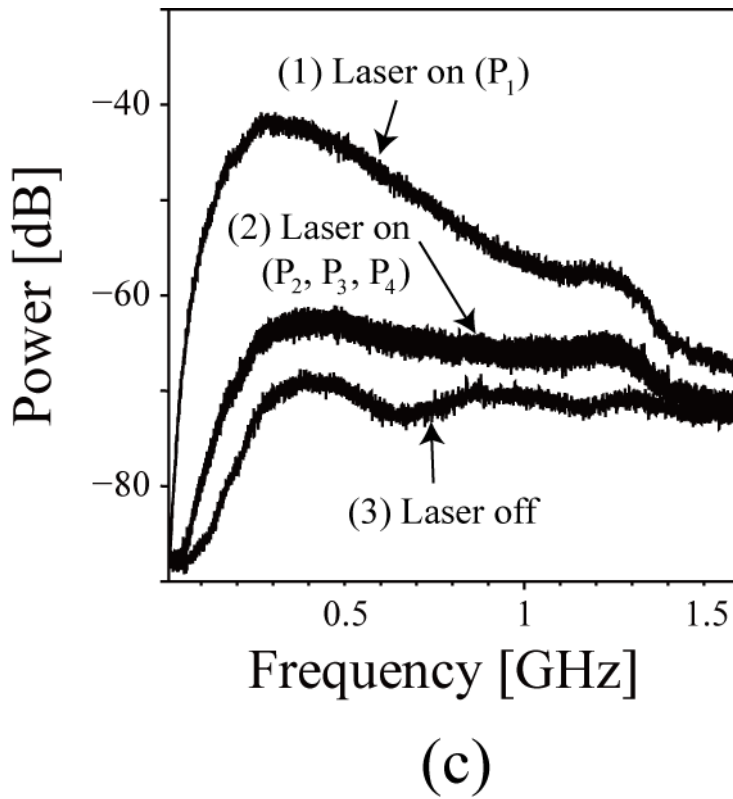


Fig. 7-5 Waveforms and spectra of transmitted light intensity signals. Detection of discriminator output: (Laser on/off). (1) the detection of the discriminator output at P_1 and (2) the detection of the discriminator output at P_2 , P_3 and P_4 and (3) the discriminator output is shut in front of the APD.

先の Fig. 7-2 に示した方法を用いると、8 組のビット列を作成することができる。まず始めに、暗号用乱数の統計的乱数性評価法として用いられている NIST の FIPS140-2 の評価法を用いて検証する。この評価法では、連続する 20,000 ビットの系列を用意して、4 つの検定を行い、その系列が乱数とみなせるか否かを確認することができる。評価法によって得られた結果から検定通過率を求め、それぞれ評価を行う。検定通過率は以下の式で求めている。

$$\text{検定通過率} = \frac{\text{検定を通過した回数}}{\text{実験を行った回数}} \times 100[\%]$$

生成結果を表 1 に示す。この表では、実験によって得られたデータを下位ビットから順に r_0 , r_1 , ..., r_6 , r_7 として表し、それぞれ各ビットについて 20,000 ビットから成るビット列を 10000 セット用意して検定を行った際の検定通過率を表している。表 1 からわかるように、 r_0 から r_5 までのビット列に対して、高い検定通過率を得ることができた。

Table 1 Results of NIST FIPS 140-2 statistical tests. Statistical randomness for a binary stream consisted of 20,000 digits, verified by four tests consisting of the “monobit-“, the “poker-“, the “runs-“ and the “long-run-“. We evaluated 10,000 sets of 20,000 binary numbers and calculated the examination pass rates, at every digit. “Total” means the examination pass rate of binary streams satisfied all four tests.

	r0	r1	r2	r3	r4	r5	r6	r7
Mono	99.96%	98.07%	99.87%	99.77%	99.96%	99.97%	99.11%	99.27%
Poker	99.99%	99.88%	99.99%	99.97%	100.0%	100.0%	97.57%	90.75%
Run	99.52%	98.23%	99.26%	99.29%	99.49%	99.50%	6.16%	0.01%
Longrun	99.94%	99.99%	99.97%	99.96%	99.96%	99.93%	99.98%	99.97%
Total	99.43%	96.55%	99.11%	99.07%	99.43%	99.43%	6.09%	0.016%

また、本研究では、他の報告でも使用され、より良い評価を与えられている SP800-22 を用いた評価も行った。この検定では、1G ビットに及ぶ 1 本のビット列が必要となるため、FIPS140-2 の検定で高い検定通過率を示した r0 から r5 までのビット列を必要な分だけ利用して 1G ビットのビット列を作成する。この際、ビット列と 2ms だけ遅延を施したそれ自身のビット列とで XOR を用いることで、ビット列において 0 と 1 を等確率に含むビット列を得ることができる。この方法は、参考文献 [50] にあり、SP800-22 のような疑似乱数の品質のための評価法を使用する際には、この操作は不可欠である。表 2 に SP800-22 を用いた場合の生成結果を示す。表から、このビット列は、全てのテストを通過していることがわかる。また、表 2 には、レーザオフの条件で得られたデータで作成したビット列に対する評価結果も掲載しており、こちらは、線形複雑度検定 (LinearComplexity test) 以外は全て検定を通過することはできないという結果が得られた。なお、P₂、P₃、P₄ 点における結果は、レーザオフの結果とほぼ同じだった。結果として、SP800-22 を用いた場合でも、周波数雑音に起因した透過光強度信号をもちいることで、テストを通過することを示すことができた。

レーザ周波数のドリフト、レーザパワーの強弱、Rb 蒸気の光学的厚さなどのパラメータは、Rb 原子の吸収線の傾きを変化させ、それにより周波数雑音から透過光強度へ変換された信号の振幅強度は決定される。そして、この振幅強度が大きければ、Fig. 7-2 から、上位ビット（例えば、r7,r6,r5）の数列でも 0 と 1 の発生率が均等に近づくため、乱数性もよくなり、振幅強度が小さければ、0 と 1 の発生率が不均一になり、上位ビットの数列から乱数性が悪くなると考えられる。このように、本実験では半導体レーザの周波数雑音に起因した物理乱数の生成を示すことができた。この実験では、500MS/s のサンプリング速度で、分解能が 8 ビットの ADC を使用したので、8 つのビット列すべてがテストを通過すると、フルスピードで 4Gb/s の生成速度を得ることが可能である。今回の実験結果では、6 つのビット列が検定を通過したので、3Gb/s の生成速度を得ることができた。

Table 2 Results of NIST Special Publication 800-22 statistical tests. A set of 1000 sequences generated using the lower 6-digits is evaluated. Each sequence contains 1 Mbits data. Significance level =0.01 , the P value (uniformity of p values) should be larger than 0.0001, while the proportion should be greater than 0.9805608.

Statistical test	Laser on (P_1)			Laser off		
	P value	Proportion	Result	P value	Proportion	Result
Frequency	0.120909	0.9830	Success	0.000000	0.0310	Failure
BlockFrequency	0.099513	0.9880	Success	0.000000	0.0000	Failure
CumulativeSums	0.068999	0.9820	Success	0.000000	0.0200	Failure
Runs	0.803720	0.9930	Success	0.000000	0.0000	Failure
LongestRun	0.494392	0.9900	Success	0.000000	0.0000	Failure
Rank	0.131122	0.9920	Success	0.000000	0.0000	Failure
NonOverlappingTemplate	0.022760	0.9890	Success	0.000000	0.0000	Failure
OverlappingTemplate	0.560545	0.9890	Success	0.000000	0.0000	Failure
Universal	0.034942	0.9880	Success	0.000000	0.0000	Failure
ApproximateEntropy	0.352107	0.9950	Success	0.000000	0.0000	Failure
RandomExcursions	0.042950	0.9866	Success	----	----	Failure
RandomExcursionsVariant	0.064103	0.9900	Success	0.000000	1.0000	Failure
Serial	0.467322	0.9890	Success	0.000000	0.0000	Failure
LinearComplexity	0.494392	0.9890	Success	0.618385	0.9930	Success

我々の物理乱数システムでは、よい結果を得ることができた。しかしながら、現在の物理乱数生成システムで、ランダムで高速な周波数弁別器の出力を精密に検出し測定するには、APDの遮断周波数（1GHz）やADCの性能（アナログ帯域 600MHz、サンプリング速度 500MS/s、分解能 8ビット）が生成速度を制限しているため、より高速な光検出器やより高性能なADCを導入する必要がある。また、より一層、物理乱数の生成速度を向上させる場合には、雑音源である端面発光型半導体レーザの周波数雑音帯域は、数 GHz であるため、数十 GHz にも及ぶ周波数雑音スペクトル特性を持つ VCSEL を用いることが期待される。これにより、より高速に乱数列を生成し、上位ビットでの検定透過率も向上させることができるので、物理乱数の生成速度を飛躍的に増加させることが可能である。

この他の課題として、現在の物理乱数システムにおける半導体レーザ光源は、温度制御のみがほどこされたフリーランニング状態であるため、レーザ周波数を安定化した状態で物理乱数を生成する必要がある。これにより、無用な低周波成分を除去することができるため、物理乱数の生成速度を向上させることができると考えられる。

第 8 章 周波数安定化時の物理乱数

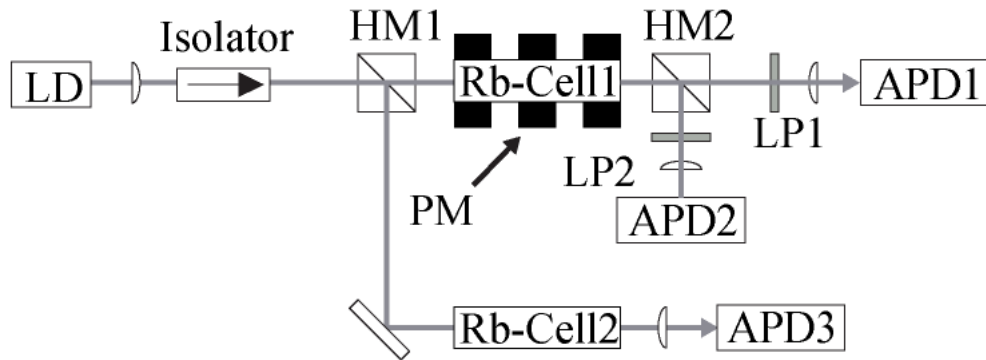
第 7 章では、半導体レーザの周波数雑音を周波数弁別器を用いて透過光強度信号を検出することで、物理乱数を生成することが可能であることを示した。しかしながら、注入電流や温度による雑音を減らすことができれば、品質の良い大量の物理乱数を生成することが可能となるため、レーザ周波数の安定化を行う必要がある。

8.1 実験方法

今回行った実験では、物理乱数の生成に使用する半導体レーザの雑音は、交流分のみを利用している。この理由として、半導体レーザの出力は直流分に対して雑音（交流分）が非常に小さくて埋もれてしまうため、直流・交流分両方を含む信号から生成しようとすると、変動が小さく乱数にならなかったことが挙げられる。このため実験では交流分だけを取り出し、激しく変動する信号から物理乱数の生成を行った。以下にその実験方法を示していく。

Fig.8-1、Fig.8-2 が今回使用した光学系及び実験系である。半導体レーザの出力光はレンズでコリメートされたのち、戻り光誘起雑音の発生を防ぐためのアイソレータを通り、ハーフミラー（HM1）で光路を 2 つに分けられる。一方の出力光は環状のフェライト磁石で磁界を印加した Rb セル 1 に入射され、ファラデー効果によって偏光面が回転する。そして、偏光面が回転したレーザ光は HM2 で再び 2 つに分けられ、偏光方向に対し角度をつけた LP を通過し、それぞれアバランシフォトダイオード（APD1、APD2）で受光される。APD1 と APD2 で得られた光強度信号は減算器に入力される。このとき減算器から出力される差分の信号が零クロス点を持つ誤差信号となる。そして、PID 制御回路を介して半導体レーザの注入電流に誤差信号をフィードバックすることで安定化が行われる。なお、半導体レーザには温度コントローラを用いて $\pm 1/1000(\text{K})$ の精度のマウントの温度制御を施す。

もう一方のレーザ光は、Rb セル 2 を通過したのち APD3 で受光され、RF アンプで増幅されたのち、デジタルオシロスコープに内蔵された AD コンバータによりサンプリングが行われる。これにより、サンプリングされた電圧信号は、バイナリデータとしてコンピュータに取り込まれる。生成されたビット列の信頼性に関しては、暗号用乱数の統計的乱数性を評価する NIST の FIPS140-2 により評価される。



PM : Permanent Magnet APD : Avalanche Photo Diode
 HM : Half Mirror LP : Linear Polarizer
 LD : Laser Diode

Fig.8-1 Optical setup

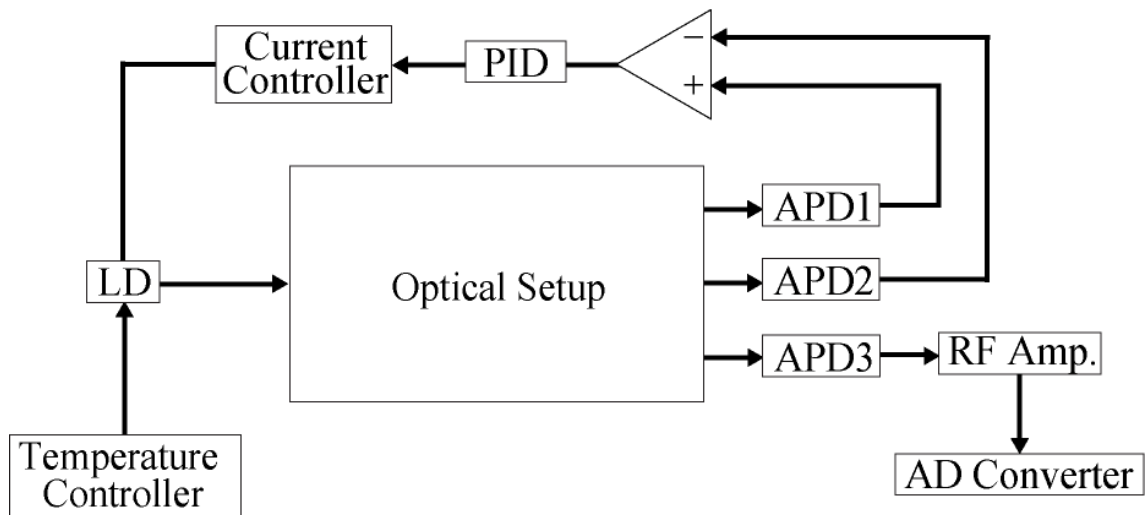


Fig.8-2 Experimental setup

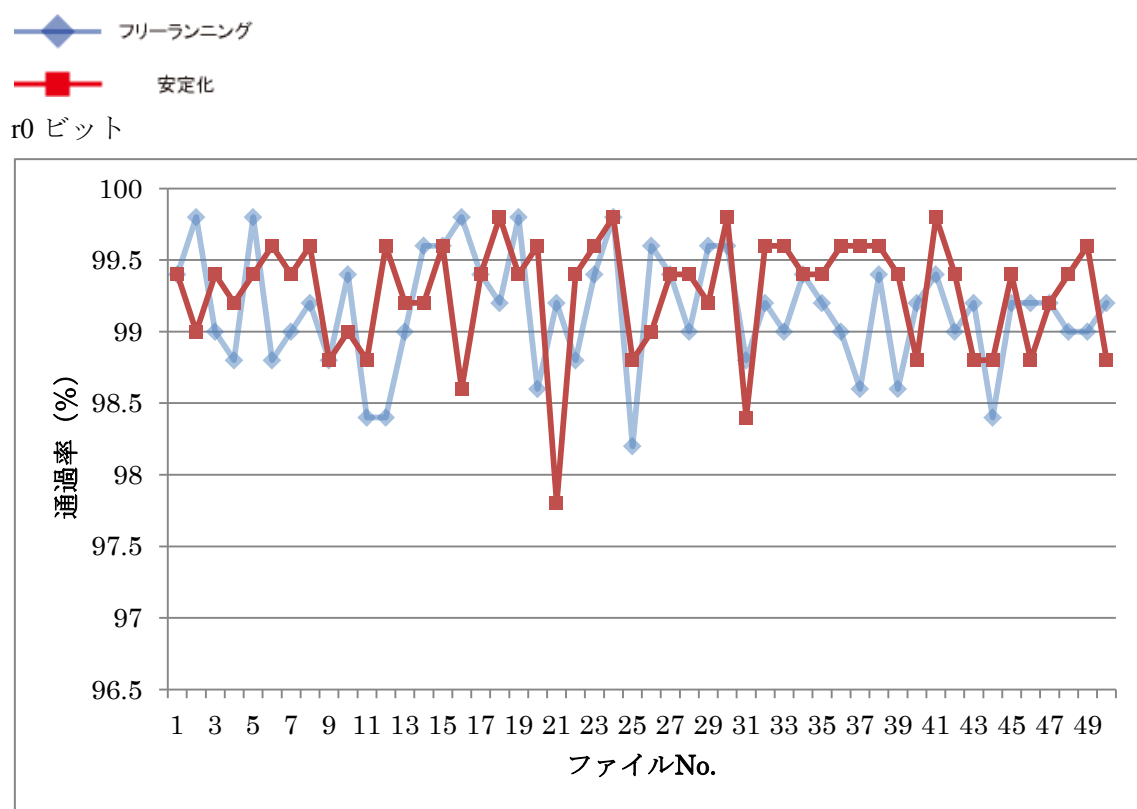
8.2 実験結果と考察

Fig.8-3 にこの実験で得られた乱数を FIPS140-2 に通したときの検定通過率のグラフを示す。縦軸は検定通過率を示しており、検定通過率は次式で求められる。

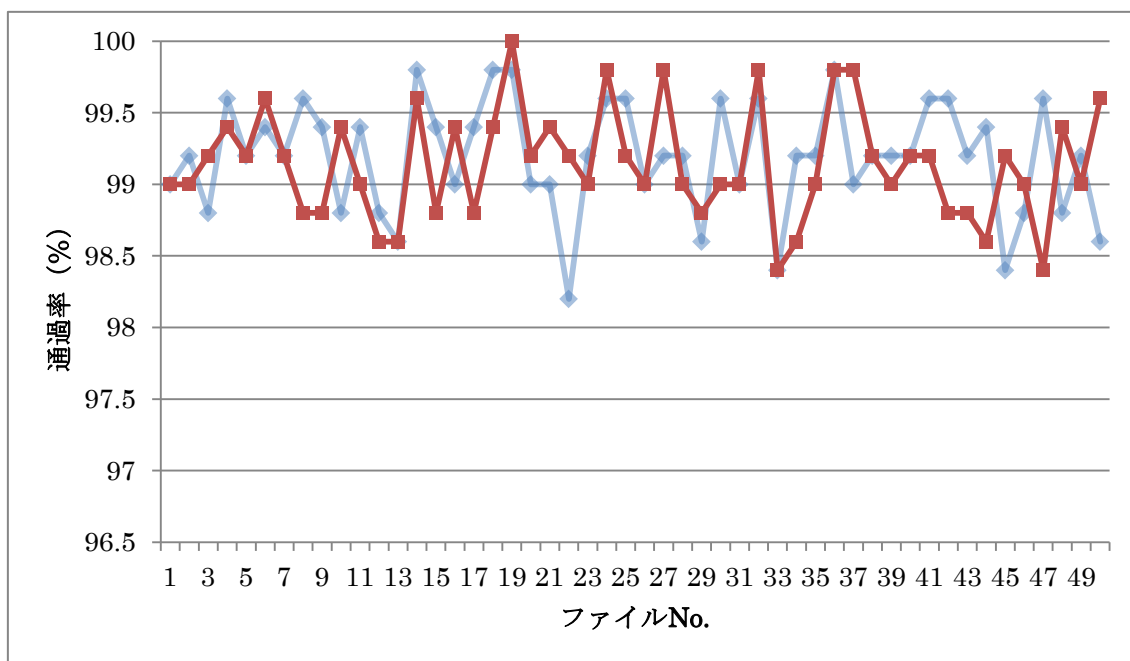
$$\text{検定通過率} = \frac{\text{検定を通過した回数}}{\text{実験を行った回数}} \times 100[\%]$$

横軸は、扱ったファイルの番号を表しており、時系列順に並べてある。この検定通過率は、各ビットについて 500 回検定を行い、そのうち何回検定を合格したかを意味している。また、◆のマーカで表されているグラフはフリーランニング時における乱数の通過率を表しており、■のマーカで表されているグラフは発振周波数安定化を施したレーザによる乱数の通過率を表している。なお、r0~r7 ビットまでのデータを乱数検定に通したが、r4~r7 ビットに関してはフリーランニング・安定化共に通過率が 0%だったので省略した。

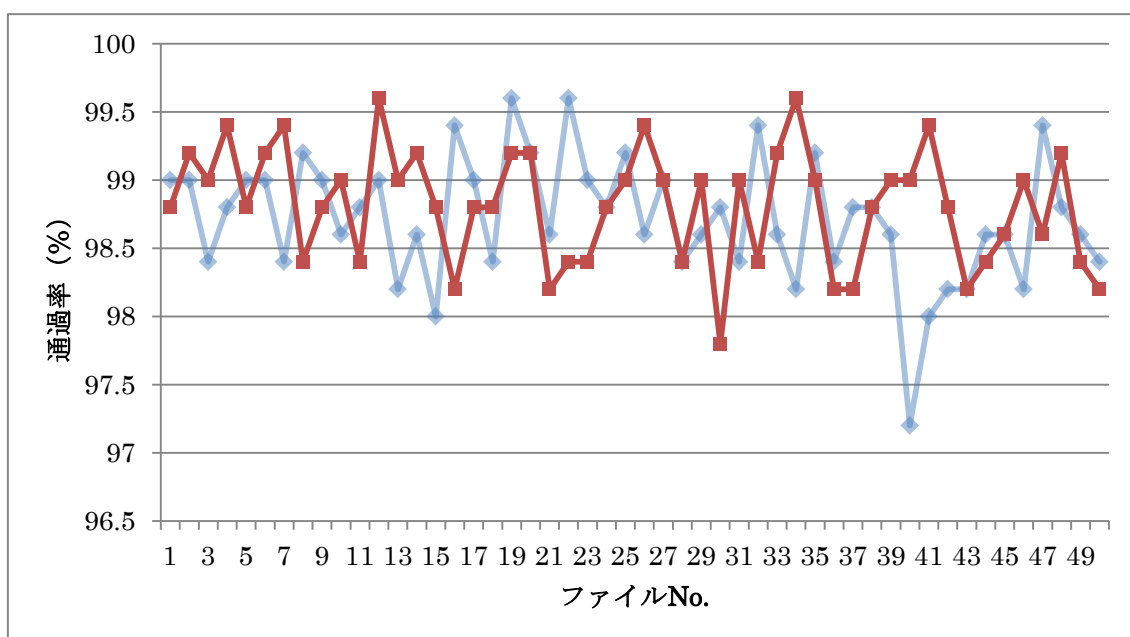
Fig.8-3 より安定化を施した半導体レーザによって生成される物理乱数とフリーランニング時の半導体レーザによって生成される物理乱数の乱数検定通過率は r0~r3 までそれぞれの通過率が同じような値をとることが分かる。



r1 ビット



r2 ビット



r3 ビット

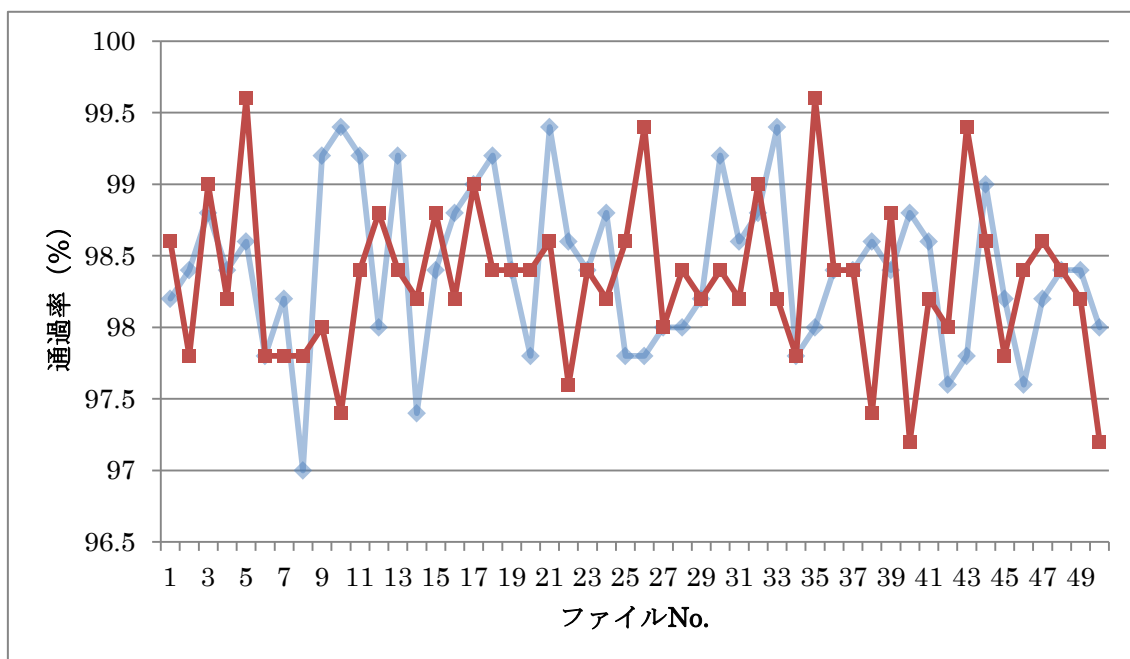


Fig.8-3 Pass rate

第9章 結論

本論文では、半導体レーザの周波数雑音特性に着目し、半導体レーザの周波数安定化の実験と、半導体レーザの周波数雑音を用いた物理乱数の新しい生成法に関する実験について報告した。

半導体レーザの周波数安定化には、発振周波数と参照周波数の差を検出するためにレーザの駆動電流に微小変調を加える直接変調方式があり、本研究では、スペクトル幅の狭い Rb 原子の飽和吸収線のドップラーフリースペクトル線を用いる方法で安定化を行ってきた。今回の実験では、Rb セルを加熱することで得られる制御信号の改善により、周波数安定度の向上を目的として実験を行った。結果として、吸収線の吸収量、 G_d 共に増加し、制御信号は改善されたが、周波数安定度としては、多少改善された程度であり、大幅な周波数安定度の向上は見られなかった。今後更なる安定度の向上を目指すには、SN 比の S (制御信号) の向上と同時に N (ノイズ) を低減させる必要があると考えられる。また、今回の実験で周波数安定度に大きな差が見られなかった原因として、半導体レーザの駆動ドライバや安定化に用いているロックインアンプによる限界があると考えられる。

また、本研究では、直接変調方式の他に、間接変調方式による安定化も行ってきた。この方式では、ファラデー効果を利用して Rb セルにヘルムホルツコイルで外部より磁界変調を加えることでレーザの偏光面の回転角変化を透過光強度の変化として捉えることで制御信号を得ている。また、この安定化法では、安定化しようとしている半導体レーザの周波数そのものには変調を加えないため、発振スペクトルを広げずに済むといった利点がある。今回の実験は、レーザマウントの温度制御を 1000K 程度に抑制した状態、つまりノイズを低減させた状態で Faraday PEAK 方式を用いる事で制御信号を向上させることを目的として行った。結果として、平均化時間でおおよそ 0.3 秒以降において Faraday Normal 方式と比べて安定度の向上が確認できたが、過去の実験における Faraday PEAK 方式の結果とは異なる結果となってしまったために、この実験においては再実験が必要であると考えられる。

以上に述べた半導体レーザの雑音を制御する研究は精密光計測や高分解能分光などの応用を目的として長年行われているが、これらの雑音は積極的に応用される場合もあり、最近では、物理乱数を高速に生成するという研究が盛んに行われている。現在報告されている物理乱数の生成速度としては、参考文献[49]に掲載された 300 Gb/s が最速であり、この雑音源としては、半導体レーザカオスが用いられている。一方、本研究では、半導体レーザの周波数雑音を利用して物理乱数の新しい生成法について提案し実験を行った。この実験では、半導体レーザの周波数雑音を周波数弁別器によって、より大きな透過光強度信号に変換して物理乱数を生成し、 3 Gb/s の生成速度を実現することができた。しかしながら、今回の実験では、APD の遮断周波数 (1 GHz) や ADC の性能 (アナログ帯域 600 MHz 、サンプリング速度 500 MS/s 、分解能 8 ビット) が生成速度を制限しているため、高速な生成はできていない。この生成速度を改善するためには、高速応答が可能な光検出器、広帯域な高

周波増幅器、高速で高分解能な AD コンバータの導入が必要となる。また、高速に変動しかつランダムな特性をもつ雑音源を用意することも必要である。半導体レーザの周波数雑音スペクトラムは、数 GHz まで広がっているが、数十 GHz にも及ぶ周波数雑音スペクトル特性を持つ VCSEL を雑音源とすれば、より高速に変動するランダムな雑音信号が得られ、上位ビットでの検定透過率も向上させることができるので、物理乱数の生成速度を飛躍的に増加させることが可能であると考えられる。また、今回の実験では、レーザの周波数はフリーランニング状態で雑音変換ポイントに設定して実験を行ったため、長時間かけてその設定点で物理乱数を生成する場合は、レーザ周波数を安定化する必要がある。

この点に関しては、ファラデー無変調方式を用いた半導体レーザの周波数安定化を行い、物理乱数の生成を行った。この方式では注入電流に変調を加える必要がないため、レーザ周波数に周期的な変動が乗らないという利点がある。今回の実験では、レーザ周波数に安定化をかけることで雑音が抑制され、生成される乱数の検定透過率が悪くなることも予想されたが、今回の実験結果からはフリーラング時と同等の検定透過率が得られることが分かった。今後は別のレーザ周波数を用いた物理乱数生成を行い、今回の結果との比較や、NIST の SP800-22 を用いた乱数の評価、そして乱数が周波数雑音と光強度雑音のどちらが支配的な状態で生成されているのかを調べるのが課題となる。

謝辞

本論文を作成するにあたり、指導教官の佐藤孝教授から、終始適切な助言を賜り、また丁寧かつ熱心なご指導を賜りました。ここに感謝の意を表します。

実験にあたりまして具体的に実験方法などについて、土井康平氏に指導していただきました。ここに感謝の意を表します。

また、日常の議論を通じて多くの知識や示唆を頂いた佐藤研究室の後輩の皆さまに感謝いたします。

参考文献

1. 栖原敏明, “半導体レーザの基礎,” 共立出版 (1998)
2. 伊藤良一, 中村道治, “半導体レーザ [基礎と応用],” 培風館 (1989)
3. Y. Yamamoto, “AM and FM Quantum Noise in Semiconductor Lasers - Part I: Theoretical Analysis,” IEEE J. Quantum Electron., **QE-19**, 34 (1983).
4. Y. Yamamoto, S. Saito, and T. Mukai, “AM and FM Quantum Noise in Semiconductor Lasers - Part II: Comparison of Theoretical and Experimental Results for AlGaAs Lasers,” IEEE J. Quantum Electron., **QE-19**, 47 (1983).
5. 沼居貴陽, “半導体レーザ工学の基礎,” 丸善株式会社 (1996)
6. M. Ohtsu, H. Fukada, T. Tako, and H. Tsuchida, “Estimation of the Ultimate Frequency Stability of Semiconductor Lasers,” Jpn. J. Appl. Phys., **22**, 1157 (1983).
7. R. Lang, and K. Kobayashi, “External Optical Feedback Effects on Semiconductor Injection Laser Properties,” IEEE J. Quantum Electron. **QE-16**, 347 (1980).
8. 大津元一, 中川賢一, “半導体レーザーの周波数制御とその応用,” 応用物理, **58** (1989), 1428
9. 大津元一, “コヒーレント光量子工学,” 朝倉書店 (1990)
10. 田幸敏治, 大津元一, 土田英美, “半導体レーザーの周波数安定化,” 応用物理, **52** (1983), 407
11. Shigeo Nagano et al “Displacement measuring technique for satellite-to-satellite laser interferometer to determine Earth’s gravity field”, Meas. Sci. Technol. **15** (2004) 2406-2411.
12. T. Uehara, A. Sato, S. Maehara, T. Nimonji, T. Sato, M. Ohkawa, T. Maruyama, S. Kawamura : "Comparison of three semiconductor laser systems for gravitational wave detection", Optical Engineering, Vol. 48, 034302, 2009
13. 榛葉實, “光ファイバ通信概論,” 東京電機大学出版局 (1999)
14. T. Yabuzaki, A. Ibaragi, H. Hori, M. Kitano and T. Ogawa, “Frequency-Locking of a GaAlAs Laser to a Doppler-free Spectrum of the Cs-D₂ Line”, Jpn. J. Appl. Phys. **20** (1981) L451.
15. H. Tsuchida, M. Ohtsu, T. Toshiharu, N. Kuramochi and N. Oura, “Frequency Stabilization of

- AlGaAs Semiconductor Laser Based on the $^{85}\text{Rb-D}_2$ Line”, Jpn. J. Appl. Phys. **21** (1982) L561.
16. HIROKAZU HORI, YOSHINOBU KITAYAMA, MASAO KITANO, TSUTOMU YABUZAKI AND TORUOGAWA, “Frequency stabilization of GaAlAs Laser Using a Doppler-Free Spectrum of the Cs-D₂ Line”, IEEE J. Quantum Electron., **QE-19**, No.2, February 169 (1983).
 17. T. Sato, M. Niikuni, S. Sato and M. Shimba, “Frequency stabilization of a semiconductor laser using Rb-D₁ and D₂ absorption lines”, Electron. Lett., Vol.24, No.7, pp.429-437, 1988
 18. U. Tanaka and T. Yabuzaki, “Frequency stabilization of Diode Laser Using External Cavity and Doppler-Free Atomic Spectra”, Jpn. J. Appl. Phys. **33** (1994) 1614.
 19. H. Talvitie, M. Merimaa, E. Ikonen, “Frequency stabilization of a diode laser to Doppler-free spectrum of molecular iodine at 633 nm”, Opt. Commun. 152 (1998) 182-188.
 20. T. Nimonji, S. Ito, A. Sawamura, T. Sato, M. Ohkawa and T. Maruyama, “New Frequency Stabilization Method of a Semiconductor Laser Using the Faraday Effect of the Rb-D₂ absorption Line”, Jpn. J. Appl. Phys. **43** (2004) 2504.
 21. S. Maehara, H. Kobayashi, T. Sato, M. Ohkawa, T. Maruyama, T. Yoshino, H. Kunimori, M. Hosokawa, H. Ito, Y. Li, S. Nagano and S. Kawamura, “Oscillation frequency stabilization of a diode laser for the laser interferometer in a satellite-to-satellite tracking system” Proc. SPIE, **5628**-19, 2004.
 22. C. Affolderbach, G. Miletì, “Tuneable, stabilised diode lasers for compact atomic frequency standards and precision wavelength references”, Optics and lasers in Engineering 43 (2005) 291-302.
 23. S. Maehara, Y. Kurosaki, T. Sato, M. Ohkawa, T. Maruyama, T. Yoshino, H. Kunimori, M. Hosokawa, H. Ito, Y. Li, S. Nagano, S. Kawamura, “Frequency stabilization of laser diode light-sources in satellite-to-satellite laser interferometers”, Proc. SPIE, 6115-79, 2006.
 24. 佐藤孝, 須貝浩之, 榛葉實, “Rb-D₂ 線を用いた半導体レーザの高速変調時における波

- 長安定化”, 信学論 (C), Vol.J-69C, No.5, pp.600-608 (1986)
25. 佐藤孝, 小泉春吾, 斎藤敏紀, 榛葉實, “半導体レーザの変調時における周波数安定化”, 信学論 (C), Vol.J71-C, No.10, pp.1450-1457 (1988)
 26. 秋山浩二, 吉武哲, 大手明, 古賀保喜, 中段和宏, 大島新一, “Rb 吸収線を用いた無変調出力の半導体レーザ周波数安定化”, 電学論, Vol.109-C, No.1, pp.22-27 (1989)
 27. 陸川均, 佐藤孝, 仲川昌弘, 榛葉實, “Rb 原子のファラデー効果を用いた半導体レーザの周波数安定化”, 信学論 (C-1), Vol.J74-C-1, No.5, pp.176-183 1991
 28. 上野隆, 陸川均, 中澤孝男, 佐藤孝, 榛葉實, “Rb 原子吸収のファラデー効果を用いた半導体レーザの発振周波数安定化と発振周波数制御”, 信学論 (C-1), Vol.J75-C-1, No.6, pp.460-467 1992.
 29. 二瓶靖厚, 小林吉久, 佐藤孝, 榛葉實, “PEAK 方式による半導体レーザの直接変調時における周波数安定化”, 電学論 (C), Vol.112-C, No11, pp697-704, 1992
 30. 小林吉久, 二瓶靖厚, 水本潤一, 佐藤孝, 榛葉實, “改善された直接変調方式による PEAK 方式を用いた半導体レーザの周波数安定化”, 電学論 (C), Vol.113-C, No.5, pp.309-314, 1992
 31. 上野隆, 中澤孝男, 中野博之, 佐藤孝, 榛葉實, “Rb 原子の飽和吸収分光信号におけるファラデー効果を用いた半導体レーザの周波数安定化”, 信学論 (C-1), Vol.J76-C-1, No.1, pp.10-17 (1993)
 32. 中澤孝男, 中野博之, 上野隆, 佐藤孝, 榛葉實, “磁気光学効果を用いた半導体レーザの周波数安定化と飽和吸収分光光学系”, 信学論 (C-1), Vol.J76-C-1, No.8, pp.285-293 (1993)
 33. Takashi SATO, Jun'ichi MIZUMOTO, Yoshihisa KOBAYASHI, Makoto ISHIGURO, Masashi OHKAWA, Takeo MARUYAMA and Minoru SHIMBA, “Frequency Stabilization of a Semiconductor Laser under Direct Frequency Shift Keying Using the Saturated Absorption

- Signal”, Jpn. J. Appl. Phys., Vol.33, pp. 1608-1613, 1994
34. 佐藤孝, 石黒誠, 水本潤一, 渡部博道, 大河正志, 丸山武男, 榛葉實, “異なる FSK 変調条件における半導体レーザの周波数安定化”, 電学論 (C), Vol.115-C, No.5, pp.728-735 1995
 35. 中野博之, 渡部直紀, 佐藤孝, 大河正志, 丸山武男, 榛葉實, “ゼーマン効果を用いた半導体レーザの発振周波数安定化における制御信号の改善”, 信学論 (C-1), Vol.J80-C-1, No.2, pp.55-63 (1997)
 36. 渡部博道, 東秀樹, 中野博之, 佐藤孝, 大河正志, 丸山武男, 榛葉實, “直接 FSK 変調時の半導体レーザの周波数安定化－変調方式と安定度の評価－”, 電学論 (C), Vol.117, No.8, pp.1119-1125, 1997
 37. A. Hemmerich, D. H. McIntyre, D. Schropp, Jr., D. Meschede and T. W. Hansch, “Optically Stabilized Narrow Linewidth Semiconductor Laser For High Resolution Spectroscopy”, Opt. Commun. 75 (1990) 118-122
 38. L. Ricci, M. Weidemüller, T. Esslinger, A. Hemmerich, C. Zimmermann, V. Vuletic, W. König, T. W. Hänsch, “A compact grating-stabilized diode laser system for atomic physics”, Opt. Commun. 117 (1995) 541-549
 39. L. D. Turner, K. P. Weber, C. J. Hawthorn, R. E. Scholten, “Frequency noise characterisation of narrow linewidth diode lasers”, Opt. Commun. 201 (2002) 391-397
 40. L. Hogstedt, O. B. Jensen, J. S. Dam, C. Pedersen, and P. Tidemand-Lichtenberg, “500nm Continuous Wave Tunable Single-Frequency Mid-IR Light Source for C-H Spectroscopy,” Laser Physics, 2012, Vol.22, No.11, pp.1676-1681.
 41. 李瑛, 長野重夫, 松原健祐, 小嶋玲子, 熊谷基弘, 伊東宏之, 小山泰弘, 細川瑞彦, “超狭線幅クロックレーザの開発”, 情報通信研究機構季報, Vol.56 Nos.3/4 2010
 42. T. Yabuzaki, T. Mitsui, and U. Tanaka, “New Type of High-Resolution Spectroscopy with a Diode Laser,” Phys. Rev. Lett., **67**, 2453 (1991).

43. 藪崎努, “レーザー光による原子物理”, 岩波書店 (2007)
44. 長坂健二, 高橋朋一, “物理乱数と疑似乱数”, 法政大学工学部研究集報, 第 39 号 (2003)
45. 茂呂友子, 斉藤義明, 堀潤一, 木竜徹, “A-D 変換器の最下位ビットを用いた暗号用乱数生成法”, 電子情報通信学会論文誌 A, Vol.J88-A, No.6, pp.714-721, 2005.
46. 千葉純, 土井康平, 佐藤孝, 大平泰生, 大河正志, 丸山武男, “半導体レーザーの雑音特性を利用した自然乱数の生成に関する考察”, LQE, 107(71), 45-48, 2007-05-18
47. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, “Fast physical random bit generation with chaotic semiconductor lasers,” Nat. Photon., **2**, 728 (2008).
48. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, “Ultrahigh-Speed Random Number Generation Based on a Chaotic Semiconductor Laser,” Phys. Rev. Lett., **103**, 024102 (2009).
49. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, “An optical ultrafast random bit generator,” Nat. Photon. **4**, 58-61 (2009).
50. K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, “Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers,” Opt. Express, Vol. 18 No. 6, 5512 (2010).
51. B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, “High-speed quantum random number generation by measuring phase noise of a single-mode laser,” Opt. Lett., **35**, 312 (2010).
52. H. Guo, W. Tang, Y. Liu, and W. Wei, “Truly random number generation based on measurement of phase noise of a laser,” Phys. Rev. E, **81**, 051137 (2010).
53. C. R. S. Williams, J. C. Salevan, X. -W. Li, R. Roy and T. E. Murphy, “Fast physical random number generator using amplified spontaneous emission”, Opt. Express 18, 23584 (2010)
54. H. Nishimura, K. Doi, T. Ushiki, T. Sato, M. Ohkawa, and Y. Ohdaira, “Physical-random number generation using laser diodes’ inherent noises,” *Proc. SPIE*, 7597-22(2010).
55. 前原進也, 土井康平, 牛木哲郎, 佐藤孝, 大平泰生, 大河正志, “半導体レーザーの周波数雑音を用いた物理乱数の高速生成, ” LQE, 110(66), 23-26, 2010-05-21
56. Xiaowen Li, Adam B. Cohen, Thomas E. Murphy and Rajarshi Roy, “Scalable parallel physical random number generator based on a superluminescent LED”, Opt. Lett., Vol.36, No.6, 1020 (2011).
57. T. Ushiki, K. Doi, S. Maehara, T. Sato, M. Ohkawa, and Y. Ohdaira, “Super fast physical-random number generation using laser diode frequency noises,” *Proc. SPIE*, 7933-87(2011).

58. 土井康平、新井秀明、前原進也、高森大希、松本良彦、佐藤孝、大平泰生、坂本秀一、大河正志、“半導体レーザの周波数雑音を応用した高速物理乱数生成,” *LQE*, 111(56), 9-12, 2011-05-13
59. H. Takamori, K. Doi, S. Maehara, K. Kawakami, T. Sato, M. Ohkawa, and Y. Ohdaira, “Fast Random-Number Generation Using a Diode Laser’s Frequency Noise Characteristic,” *Proc. SPIE*, 8255-75(2012).
60. 川上航平、前原進也、土井康平、新井秀明、近藤堯信、清水直弥、佐藤孝、坂本秀一、大平泰生、大河正志、“面発光型半導体レーザの周波数雑音を利用した物理乱数の生成に関する研究” 信学技報 112(184), 9-12, 2012-08-23
61. Shinya Maehara, Kohei Kawakami, Hideaki Arai, Kenji Nakano, Kohei Doi, Takashi Sato, Yasuo Ohdaira, Shuichi Sakamoto, Masashi Ohkawa, “Frequency noise characteristics of a diode laser and its application to physical random number generation”, *Opt. Eng.* 52 (1), 014302 (January 07, 2013)
62. http://www.micro-photon-devices.com/products_qrn.asp
63. 松本眞, “乱数生成：ランダムを作る可能性, 不可能性, 妥協”, 数理科学, 2006 年 9 月号 16-20, サイエンス社.
64. サイモン・シン, “暗号解説”, 新潮社 (2001)
65. 原康夫, “物理学,” 学術図書出版社 (1991)
66. 飯島徹穂, “レーザ光のおはなし,” 日本規格協会 (2004)
67. 西原浩, 裏升吾, “光エレクトロニクス入門,” コロナ社 (1997)
68. 山田実, 飯山宏一, “半導体レーザーの雑音測定,” レーザー研究 (1991-08)
69. 伊藤良一, 中村道治, “半導体レーザ [基礎と応用],” 培風館 (1989)
70. 末松安晴, 伊賀健一, “光ファイバ通信入門 (改訂 4 版),” オーム社 (2006)
71. 霜田光一, “レーザー物理入門,” 岩波書店 (1983)
72. 黒崎芳晴, “Rb 吸収線で制御されたファブリ・ペローエタロンのスペクトルを用いた半

導体レーザの発振周波数安定化”，新潟大学大学院自然科学研究科生産システム専攻

平成 16 年度 修士論文

73. 中野博之，“Rb 原子の吸収線の磁気光学効果を用いた半導体レーザの発振周波数安定化”，新潟大学大学院自然科学研究科生産システム専攻 平成 9 年度 博士論文
74. 佐々木良一，“インターネットセキュリティ入門”，岩波新書（1999）
75. 今井秀樹，“暗号のおはなし（改訂版）”，日本規格協会（2003）
76. 西野哲朗，“量子コンピュータ”，ナツメ社（2007）
77. 石井茂，“量子暗号”，日経 BP 社（2007）
78. 平野功，“原子スペクトル入門”，技報堂出版（2000）
79. 平野功，“原子・光・磁気の解析”，技報堂出版（2004）
80. 平野功，“Cs-D₂ 線の飽和吸収スペクトルを用いた AlGaAs 半導体レーザの安定化，”計量研究所報告，**34-3**（1985）203-206
81. 柳沢充佑，“半導体レーザの発振周波数安定化～Rb 原子の飽和吸収分光法によって得られる制御信号の改善～”，新潟大学大学院自然科学研究科数理・情報電子工学専攻 平成 19 年度 修士論文
82. 佐藤旭，“ファラデー効果を用いた半導体レーザの発振周波数安定化—制御信号の向上と飽和吸収分光法による安定度評価—”，新潟大学大学院自然科学研究科数理・情報電子工学専攻 平成 20 年度 修士論文
83. Information Technology Laboratory, “Security requirements for cryptographic modules,” NIST Federal Information Processing Standards Publication 140-2 (2001).
84. A. Rukhin et al., “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” NIST Special Publication 800-22 Revision 1a, http://csrc.nist.gov/groups/ST/toolkit/rng/stats_tests.html (2010).
85. 松本良彦，“Rb 原子の D₂ 線におけるファラデー効果を用いた半導体レーザの発振周波数安定化～無変調磁界を用いた周波数弁別信号生成と安定度評価～”，新潟大学大学院自然科学研究科電気情報工学専攻 平成 23 年度 修士論文
86. 古川元一，“半導体レーザの雑音特性を用いた物理乱数の生成～発振周波数安定化が物理乱数に及ぼす影響に関する考察～”，新潟大学工学部電気電子工学科 平成 23 年度 卒業論文
87. 応用物理学会編，“半導体レーザーの基礎，”オーム社（1987）

88. 山口一郎，角田義人編，“半導体レーザーと光計測，”学会出版センター（1992）
89. レーザー学会編，“レーザーハンドブック 第2版，”オーム社（2005）