半導体レーザの周波数雑音の無秩序性を用いた高速物理乱数生成に関する研究

(Study on high-speed physical random number generation using the randomness of the frequency noise of the laser diode)

新井　秀明

新潟大学大学院自然科学研究科博士後期課程

電気情報工学専攻

Abstract

In the communication through the network, it is essential to encrypt information to secure safety of the communication. An encryption method used for communication is a public key cryptosystem and a hybrid cryptosystem that put a public key cryptosystem and a private-key cryptosystem together mainly now. The safe grounds of these methods are to need vast calculation time to decode private key from a public key, but, by a cloud computing using the network accomplishing rapid progress and the development of the study of a quantum computer, the safe securing of information security by the cryptographic technology is becoming difficult for these past several years.

One method to solve this problem includes quantum cryptography communication technology using a quantum key distribution. Because the quantum communication can detect the wiretapping on the channel, we can realize complete secret communication by letting both transmission and reception believers share private key. The randomness of the private key (i.e., the random number for secret codes) becomes important to assure the safety of this technique. Therefore the development of the technique that can generate chaotic random numbers (i.e., physical random number) fast becomes the urgent need.

This thesis focuses on a very high-speed frequency noise of the laser diode to generate a physical random number fast, and assumed this frequency noise as a source for physical random number generation. We detected a high-speed frequency noise of the laser diode as a fluctuation of the transmitted light intensity using a frequency discriminator. This principle is the same as a principle of slope detection which is a kind of the demodulation technology in the FM communication. We used a Fabry-Perot type laser diode of wavelength 780nm for a noise source, and the D_2 absorption line of the rubidium atom for a frequency discriminator. We converted a transmitted light intensity signal into binary data by an A/D converter, and produced the binary physical random number sequences by extracting binary sequence from binary data. Generated physical random number sequences are statistically confirmed its quality by means of a *de facto* standard “NIST SP800-22” of the random number test for the secret code.

Physical random number sequences are generated from binary data by two methods. The first method produced random number sequences per digits using least significant bits of binary data obtained from the A/D converter of vertical resolution 8 bits in parallel. The second method produced the binary random number sequence by connecting the data of each digit of binary data to one. We can make the generation speed of the physical random number sequence faster than the sampling speed of the A/D converter by using these methods. And, the operation such as performing EX-OR (XOR) between different random numbers is necessary for using it as a random number for the code because the physical random number usually has bad equal

probability characteristics. The method called the Reverse XOR method that developed this XOR operation is recently suggested to improve the generation speed of the physical random number in other precedent studies. In this study, both this Reverse XOR and the normal XOR (XOR method) methods are used for generating a physical random number. And, a physical random number sequence generating speed of 120 Gb/s was confirmed by a method of generating random number sequences from several digits of 8-bits-binary-data in parallel. In addition, Improved XOR and Improved Reverse XOR methods proposed in this thesis generated the physical random number sequence faster than the normal XOR and the Reverse XOR methods. As a result, this thesis reported that a physical random number sequence was generated at 160 Gb/s.

The relations between the frequency discriminator and the oscillation frequency of the laser diode bring big influence in the quality of the physics random number in our physical random number generation method. This is because frequency properties of the detected noise signal will change by the relation between the slant of the frequency discriminator and the frequency of the laser diode. Therefore the relation between the frequencies of the oscillation spectrum of this laser diode and the frequency discriminator was investigated, and the most suitable condition for generating a physical random number was discussed.

In addition, the oscillation frequency of the laser diode greatly changes by a fluctuation of the environment temperature and the driving current. Therefore it is necessary to stabilize and control the oscillation frequency of the laser diode to the limited area within the absorption line of the rubidium atom in order to generate a physical random number stably for a long time. Therefore the oscillation frequency of the laser diode was controlled by using a technique of Phase-locked-Loop to the frequency of the slope of the rubidium atom absorption curve.

あらまし

ネットワークを介した通信において，情報を暗号化することは，通信の安全性を確保するために必要不可欠なことである．現在，主に利用されている通信用暗号方式は，公開鍵暗号方式や公開鍵暗号と共通鍵暗号を組み合わせたハイブリット方式である．これらの方式の安全性の根拠は，公開鍵から秘密鍵を解読するために莫大な計算時間を要することであるが，ここ数年飛躍的な進歩を遂げるネットワークを使用したクラウドコンピューティングや量子コンピュータの研究の進展によって，この暗号化技術による情報セキュリティの安全性確保は困難になりつつある．

この問題を解決する一つの方法として，量子鍵配送を利用した，量子暗号通信技術がある．量子通信は通信路上での盗聴を検出できるため，秘密鍵をこの方法で送受信者双方に共有させることで完全な秘密通信を実現することができる．この技術の安全性をより確かにするために重要になってくるのは，秘密鍵すなわち暗号用乱数の無秩序性である．そのため非常に無秩序な乱数，すなわち物理乱数を高速に生成できる技術の開発が急務になっている．

本論文では物理乱数を高速に生成するために，半導体レーザの非常に高速な周波数雑音に着目し，その雑音を物理乱数生成のための源とした．本論文では半導体レーザの高速な周波数雑音を周波数弁別器を用いて，透過光強度の変動として検出した．これは FM 通信における復調技術のスロープ検波の原理と同じものである．また半導体レーザは，波長 780nm 帯で発光するファブリ・ペロータイプのレーザを使用し，周波数弁別器にルビジウム原子の D_2 吸収線を用いた．透過光強度信号は，A/D コンバータによって 2 進数データに変換し，2 進数データから 2 進数列を抽出することで 2 進数の物理乱数列を生成した．生成された物理乱数列は，デファクト・スタンダードである暗号用乱数検定の NIST SP800-22 によって統計的に評価して，十分な品質であることを確認した．

本論文では，物理乱数列を 2 通りの方法で 2 進数データから抽出した．一つ目の方法は，垂直分解能 8 ビットの A/D コンバータから得られた 2 進数データの Least significant bits を利用して桁ごとに並列に乱数列を生成した．2 つ目の方法は，2 進数データの各桁のデータを 1 つに結合して 2 進数の乱数列を生成した．これらの方法を利用することで本論文では，物理乱数列の生成速度を A/D コンバータのサンプリング速度より速くすることが可能になる．また，物理乱数は等確率性が悪いため暗号用の乱数として使用するためには，別の乱数との間で排他的論理和（XOR）を行うなどの操作が必要である．最近の他の先行研究では，物理乱数の生成速度を更に向上させるために，この XOR 操作を発展させた Reverse XOR 方式と呼ばれる方法が提案されている．本研究で，我々も通常の XOR を用いた方法（XOR 方式）の他にこの Reverse XOR 方式を使用して物理乱数を生成した．そして本論文では，XOR 方式において 8 ビットの 2 進数データの各桁から並列的に物理乱数列を生成する方法によって物理乱数列を最大 120 Gb/s の速度で生成することに成功した．また本論文では，

さらに物理乱数列の生成速度を向上させるために，通常の XOR 方式と Reverse XOR 方式を改良した Improved XOR 方式と Improved Reverse XOR 方式を提案した．その結果，本論文では最終的に物理乱数列を最大 160 Gb/s の速度で生成することに成功した．

我々の物理乱数生成方法では，周波数弁別器と半導体レーザの発振周波数の中心周波数の関係が，生成される物理乱数の品質に大きな影響をもたらす．これは半導体レーザの発振スペクトルの中心周波数を周波数弁別器のどの周波数に設定するかによって，検出される雑音信号の周波数特性が変化してしまうためである．そこで本論文では，この半導体レーザの発振スペクトルの中心周波数と周波数弁別器の関係を調査し，その結果から物理乱数を生成するための最適な条件を調べた．さらに，その条件において実際に半導体レーザの周波数雑音から良質な物理乱数が生成できることを確認した．

また半導体レーザの発振周波数は，雰囲気温度や駆動電流の変動によって大きく変化する．そのため，物理乱数を長時間，安定的に生成するためには，半導体レーザの発振周波数を安定化し，さらに周波数弁別器であるルビジウム原子の吸収線の波長に半導体レーザの発振周波数を制御する必要がある．そのため本論文では半導体レーザの発振周波数を Phase-locked-Loop の技術を用いて制御し，ルビジウム原子吸収曲線のスロープの周波数に安定化することで，安定的に周波数雑音を検出できるシステムを構築した．

目次

第 1 章 序論

ネットワークを介した通信において，情報セキュリティの確保のために情報を暗号化して送ることは広く一般的に用いられているセキュリティ技術である．暗号アルゴリズムには，TDEA（Triple Data Encryption Algorithm）[1]や AES（Advanced Encryption Standard）などの共通鍵暗号（Common key cryptosystem）と RSA[2]に代表される公開鍵暗号（Public-key cryptography），Web 上の通信を暗号化する場合に用いられる SSL/TLS などの公開鍵暗号と共通鍵暗号を組み合わせたハイブリッド暗号がある．現在，主に利用されている通信用暗号は，公開鍵暗号とハイブリッド暗号であるが，これらの方式の安全性の根拠は公開鍵から秘密鍵を解読するために巨大な整数を素因数分解する必要があり，解読に莫大な計算時間を要することである．しかし，ここ数年飛躍的な進歩を遂げているスーパーコンピュータやネットワークを使用したクラウドコンピューティングの発達，量子コンピュータ[3]の研究の進展によって，これらの暗号化技術による情報セキュリティの安全性確保は困難になりつつある．

この問題を解決する一つの方法として，量子鍵配送[4]~[6]を利用した量子暗号通信技術がある．量子通信は通信路上での盗聴を検出できるため，秘密鍵（暗号用乱数）をこの方法で送受信者双方に共有させ，共有した暗号用乱数で暗号化した情報を，普通の通信回線で送ることで完全な秘密通信を実現することができる．近年では，実験段階ではあるが量子鍵配送によって実際に秘密鍵を送れる秘匿光通信システムも実現されている[7][8]．この方法は暗号化と復号に同一の鍵を用いる暗号方式である共通鍵暗号方式の一種であり，送受信者双方で共有する暗号用乱数が非常に強硬，すなわち予想することができない必要がある．そのため秘密鍵を生成するための乱数生成器（RNG：Random number generator）には，非常に無秩序で周期性を持たない乱数を生成する能力が要求される[4]．

乱数生成器で生成される乱数はその生成方法によって，擬似乱数（Pseudo random number）と物理乱数（Physical-random number）に大別される．擬似乱数は種（Seed）と言われる初期値から，数列の計算アルゴリズムを使って生成される乱数列である．疑似乱数生成器の生成速度は，計算器の計算速度に依存するため容易に高速化することが可能である．しかし本質的に周期性を持ち，暗号化用途ではセキュリティ確保に限界があると考えられている[9]．一方，物理乱数は電子回路の熱雑音やダイオードのショットキー雑音，放射性原子の崩壊により放出される放射線の検出などの物理的現象を基にして生成される．この物理乱数は，本質的に解読や予測が不可能であるという特徴を持ち，共通鍵暗号方式のための乱数として使用することが可能である．しかし疑似乱数とは逆に，その生成速度は源となる物理現象の速度に依存するため，擬似乱数と比べ一般的に低速になってしまう．この欠点は，大量のデータを暗号化する必要がある現在において，物理乱数を暗号用の乱数として使用することを難しくする要因の 1 つになっている．そのため近年，通信用暗号に使用するための物理乱数の高速生成に関する研究が，盛んに行われてきている[9]~[13]．

高速に物理乱数を生成する研究は，レーザ（Laser：Light Amplification by Stimulated Emission of Radiation）の一種である半導体レーザ（LD：Laser Diode）に起因する雑音を利用する方法がいくつか報告されている[9]~[13]．半導体レーザは，定常発振しているレーザ光の中に，自然放出によるランダムな光の電界ゆらぎが混入することで生じる強度（AM：Amplitude Modulation）雑音と周波数（FM：Frequency Modulation）雑音をともなって動作することが知られている．強度雑音について着目すると，一定の動作温度と定電流で駆動された半導体レーザの光出力変動，すなわち強度雑音は非常に小さいが，これに戻り光の存在が加わると光出力が不安定になり，非常に広い周波数帯域で大きな雑音を検出することができる．これを物理乱数生成に応用した研究[10]は，2008 年に報告され，17 Gigabit per second（Gb/s）の生成速度を達成し，物理乱数の生成速度を飛躍的に向上させた．

一方，半導体レーザの周波数雑音について着目すると，フリーランニング動作時であっても非常に広帯域に渡って雑音スペクトルを呈することが理論的・実験的に分かっている．この周波数雑音の帯域は，一般的なファブリペロータイプの半導体レーザ（Fabry-Perot type Laser Diode）で，およそ 1 GHz～3 GHz，垂直共振器面発光レーザ（VCSEL：Vertical Cavity Surface Emitting Laser）で，およそ 3 GHz～10 GHz 程度である．この周波数雑音を利用した乱数生成方法もいくつか提案されている[9][12]．これらの方法では，周波数雑音は独立した周波数雑音を持つレーザのビーム軸を重ねることで得られるビート信号（差周波数信号）によって検出される．また，論文 9 の研究では生成速度 20 Megabits per second（Mb/s）[9]の生成速度が達成されたことが報告されている．

一方，我々はこれらとは別の方法で，周波数雑音から高速に物理乱数を生成する方法を "Frequency noise characteristics of a diode laser and its application to physical random number generation."の中で提案した[13]．我々の方法では，周波数雑音を用いた高分解能分光法[14]の原理に着目し，ルビジウム（Rb）原子吸収線を周波数弁別器として利用することで，周波数雑音を透過光強度の変動として観測し，物理乱数の源となる雑音信号を検出している．実験において生成された物理乱数の生成速度は，3 Gb/s を達成し，半導体レーザの周波数雑音を使った物理乱数生成の方法としては非常に高速な生成速度を達成することに成功した．

我々は，半導体レーザの周波数雑音から得られた電気的なアナログ信号を A/D コンバータ（ADC：Analog-Digital Converter）によってデジタル信号に変換して，2 進数列を得ることで 2 進物理乱数列を生成している．このような生成方法の場合，最も単純な垂直分解能 1 ビットの ADC を乱数生成に利用すると，その生成速度は，ADC のサンプリング速度と同一の周期の速度で生成されると考えることができる．すなわち，500 Mega samples per second（MS/s）のサンプリング速度で得られた 2 進数データから物理乱数列を生成した場合，その生成速度は，500 Mb/s に相当すると換算できる．我々の研究では，垂直分解能 8 ビットの ADC を使用し，ADC から得られた 2 進数データの最下位ビット（LSB：Least significant bit）から最上位ビット（MSB：Most significant bit）までのすべての桁を利用して乱数列の生成を行った．この論文において，このような乱数生成方式の総称をマルチビット生成方式と呼

ぶこととする．この生成方法は，ADC から得られた 2 進数データの各桁から得られた 2 進数列（垂直分解能 2 ビット以上の ADC は，一度のサンプリングにおいて複数の桁ごとに 1 桁の 2 進数を同時に得られる.）を同時に乱数列の生成に使用することで，乱数の生成速度を ADC のサンプリング速度より向上させることができる．論文 13 の乱数生成速度も，この方法で生成したため，厳密には 500 Mb/s（500 MS/s）×6 LSBs = 3 Gb/s である．また，論文 10 の内田などの研究でも，2 進数データの LSBs（Least significant bits）を利用して物理乱数を生成している[10]．我々も本研究で，この ADC のマルチビット生成の方法によって物理乱数を生成して，その効果や課題について調べる．

また，物理乱数は等確率性が悪いため暗号用の乱数として使用するためには，別の乱数との間で exclusive OR（XOR）を行うなどの操作が必要である．内田などの最近の研究は，物理乱数の生成速度を更に向上させるために，この XOR 操作をさらに発展させた Reverse XOR（RXOR）method と呼ばれる方法を提案している．そして論文 15 の研究において，生成速度 1.2 Terra bits per second（Tb/s）の物理乱数生成器（P-RNG：Physical-Random Number Generator）を実現した[15]．本研究で，我々も通常の XOR を用いた方法（XOR method）の他にこの RXOR method を使用して物理乱数を生成し，更なる生成速度の向上を目指す.

我々の物理乱数生成方法では，周波数弁別器と半導体レーザの発振周波数の中心周波数の関係が，生成される物理乱数の品質に大きな影響をもたらす．これは半導体レーザの発振スペクトルの中心周波数を周波数弁別器のどの周波数に設定するかによって，検出される雑音信号の周波数特性が変化してしまうためである．そこで，我々は本論文で，この半導体レーザの発振スペクトルの中心周波数と周波数弁別器の関係を調査し，その結果から物理乱数を生成するための最適な条件を調べる．さらに，その条件において実際に半導体レーザの周波数雑音から良質な物理乱数が生成できることを確認する．物理乱数の品質は，国際標準とされる暗号用乱数検定の NIST SP 800-22[16]によって評価する．

半導体レーザの発振周波数は，雰囲気温度や駆動電流の変動によって大きく変化する．そのため，物理乱数を長時間，安定的に生成するためには，半導体レーザの発振周波数を安定化し，さらに周波数弁別器である Rb 原子の吸収線の波長に半導体レーザの発振周波数を制御する必要がある．本論文では，そのための半導体レーザの発振周波数安定化のシステムや，その周波数雑音を検出するためのシステムについても詳しく述べる．

以下に本論文の構成を示す．第 2 章では，物理乱数生成のための雑音源となる半導体レーザについて述べる．第 3 章では，半導体レーザの周波数雑音を検出する方法と，周波数雑音を検出するために使用する Rb 原子の吸収線について述べる．第 4 章では，物理乱数の実際の生成方法についてと生成した物理乱数の SP800-22 を使用した評価方法について述べる．第 5 章では，物理乱数を長期的に安定して生成するための半導体レーザの発振周波数の制御方法について述べ，また発振周波数が安定化された半導体レーザのその安定度の評価方法について述べる．第 6 章では，物理乱数を生成するための最適な条件として物理乱数生成のための XOR 演算のための 2 進数データの遅延時間について調べ，その結果と考察

を述べる．第 7 章では，周波数弁別器の周波数雑音を検出するための位置について調べ，その結果と考察を述べる．第 8 章では，物理乱数生成器の長期安定性を評価するために実際に構築した半導体レーザの発振周波数検出システムの安定度と，そのシステムから生成した物理乱数の品質の評価結果について述べる．第 9 章では，マルチビット生成方式や RXOR method を用いた物理乱数の高速生成に関する研究結果と，その考察を述べる．最後に，第 10 章で本研究についてまとめる．

第 2 章 半導体レーザ

本章では，物理乱数生成のための雑音源である半導体レーザについて簡単に説明する．先ず半導体レーザの動作原理などについて述べ，続いて半導体レーザの基本的な特性，最後に半導体レーザの周波数雑音について述べる．

2.1 半導体レーザの動作原理

2.1.1 半導体中における光の自然放出と誘導放出[17][18]

物質中の原子，分子の持つエネルギーの値は離散的であり，そのエネルギーの値はエネルギー準位と呼ばれている．一方，半導体中では原子が結晶構造を構成しており，原子密度が非常に大きいため，エネルギー準位が帯状のエネルギーバンドを形成する．Fig.2-1 は，その半導体のエネルギーバンド構造を示したものである．Fig.2-1 (a)に示されているように固体のバンド理論では，電子（Electron）によって満たされているエネルギーバンドを価電子帯（Valance band），電子が空のバンドを伝導帯（Conduction band），そして価電子帯と伝導帯の間の領域を禁制帯（Forbidden band）と呼んでいる．また，伝導帯の下端のエネルギー準位（E_c）と価電子帯の上端のエネルギー準位（E_v）の隔たり（$E_c - E_v$）は，エネルギーギャップ（Energy gap）またはバンドギャップ（Band gap）（E_g）と呼ばれる．

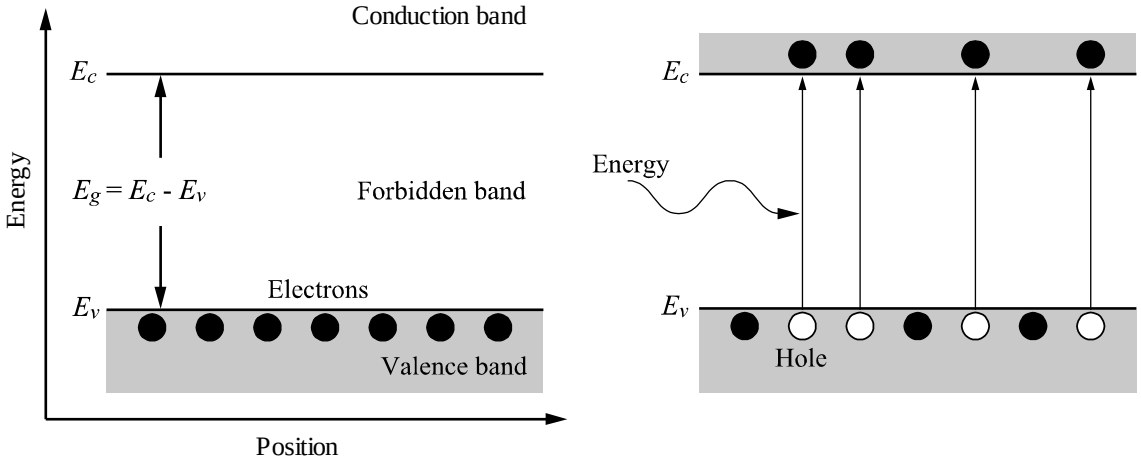
熱平衡（Thermal equilibrium）にある高純度の半導体に，何らかの形でエネルギーギャップより大きなエネルギーを与えると，Fig.2-1 (b)で示すように，価電子帯を占めていたいくつかの電子が伝導帯へと遷移し，価電子帯に電子の抜けた穴である正孔（Hole）が生じる．このような状態を励起状態（Excitation state）と呼ぶ．伝導帯に遷移した電子は，数ナノ秒程度伝導帯に留まった後で，Fig.2-2 (a)に示すように価電子帯に遷移して正孔と再結合する．このときエネルギーギャップに等しいエネルギーをもつ光子（photon）が放出される．すなわち，以下の関係式が成り立つ．

$$h\nu_0 = E_c - E_v \equiv E_g \tag{2-1}$$

ここで，hはプランク定数（6.626×10^{-34} J s），ν_0は光子の周波数である．このようにして発生する光は，自然放出（Spontaneous emission）光と呼ばれる．自然放出光は時間的にランダムに発生するため，その振幅，位相，周波数が不揃いである．また，空間的にランダムな方向に生じるため，指向性の悪い光となる．

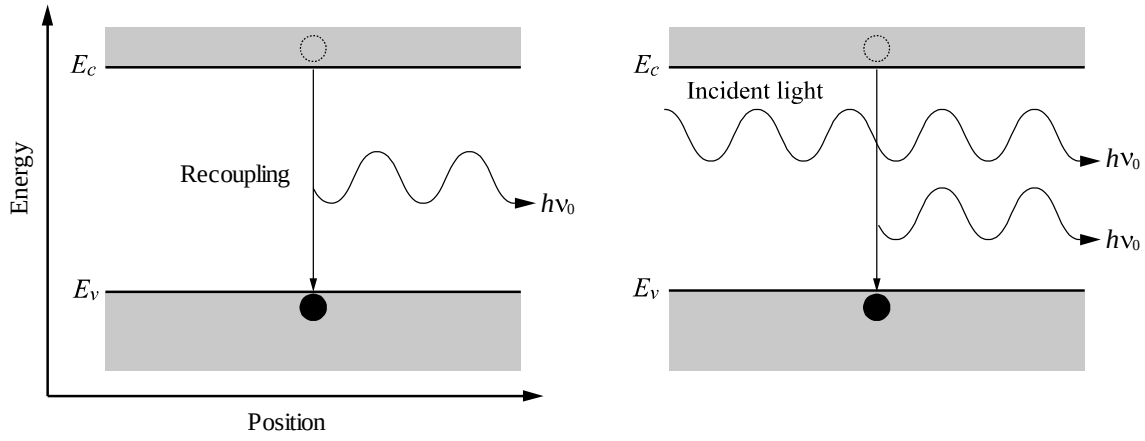
一方，Fig.2-2 (b)に示すように励起状態の半導体に周波数ν_0の光が照射されると，伝導帯に励起された電子が価電子帯に強制的に遷移され，入射光と同じ周波数の光が入射光と同じ方向に放射される現象が起こる．このとき放出された光は，指向性に優れ，位相，周波

数が揃っているコヒーレントな光となる．このような光の放出は，誘導放出（Stimulated emission）と呼ばれる．半導体が継続して発光し続けるためには，この誘導放出が次々と起こり光が増幅される必要がある．



(a) Thermal equilibrium state　　(b) Excitation state

Fig.2-1 Energy structure of a semiconductor.



(a) Spontaneous emission　　(b) Stimulated emission

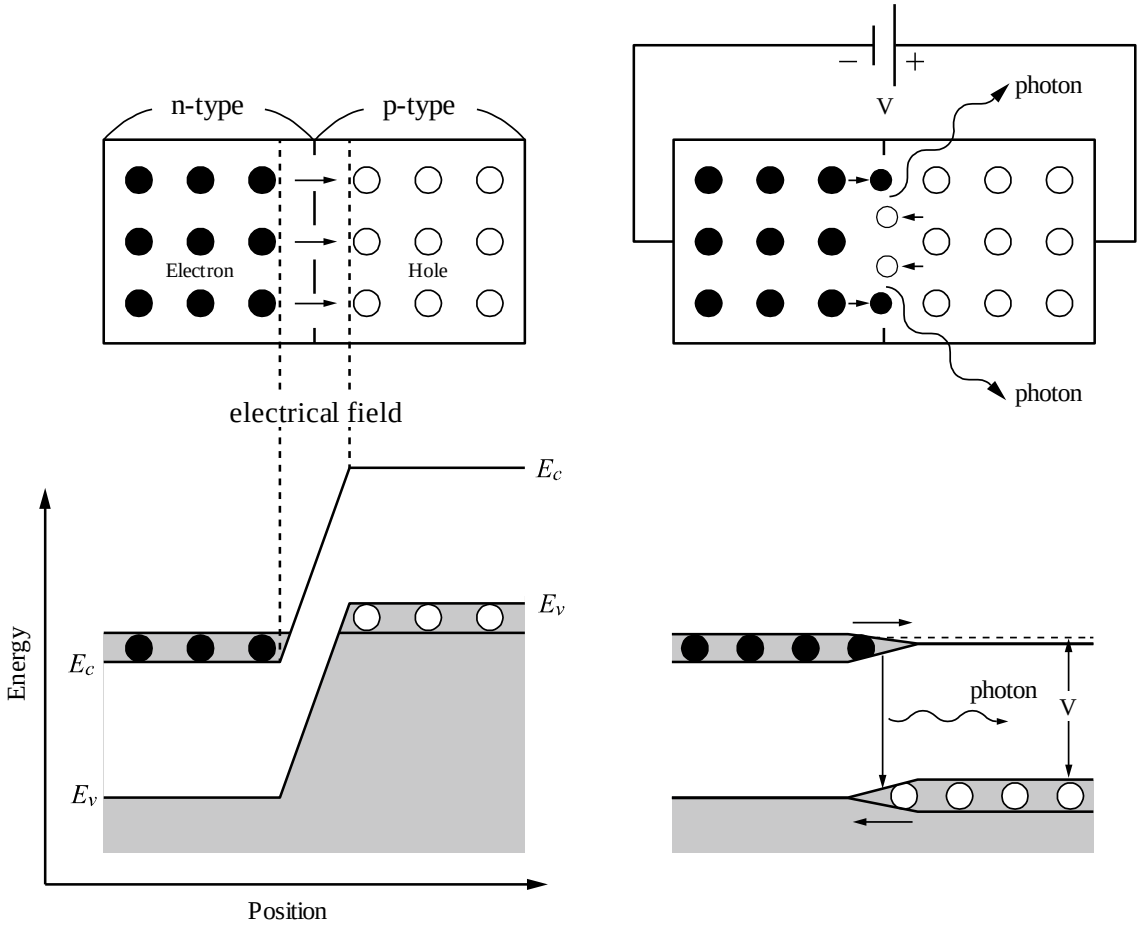
Fig.2-2 Light emission process.

2.1.2 pn 接合半導体による発光[17][18]

誘導放出により光を増幅するためには，入射光による誘導放出が吸収（光による電子の励起）または光励起を上回る必要がある．そのためには，半導体中で伝導帯の電子数が価電子帯の電子数より多い状態，反転分布を維持する必要がある．

半導体中で反転分布を形成するためには，pn 接合（p-n junction）を利用する方法が一般的である．半導体結晶に不純物を混ぜると，常に伝導帯中に自由に動ける電子が存在する n

形半導体と価電子帯中に自由に動ける正孔が存在する p 形半導体を作ることができる．この 2 つの半導体を使って，ひと続きの半導体結晶中に，n 形と p 形の領域をつくると Fig.2-3 (a)のように，その境界に自然に電界が生じて，電子と正孔がそれぞれの領域の中に保たれ，他領域には侵入して行かないようになる．この pn 接合に外から順方向に電圧を与えると Fig.2-3 (b)のように，電子と正孔が互いに他の領域に入っていくようになる．その結果 pn 接合付近では電子と正孔が共存し，反転分布が形成される．半導体中の反転分布が形成された領域では，電子と正孔の再結合によって生じた光によって次々と誘導放出が発生し，光が増幅される．



(a) Gap of between the electron and hole by the electric field in the p-n junction

(b) Electronic recombination and emission by the voltage

Fig.2-3. Light emission by the p-n junction.

2.1.3 ダブルヘテロ接合ダイオードレーザ[17][18]

実際の半導体レーザは，さらに Fig.2-4 に示すような p または n 形半導体（活性層：active layer）を n 形と p 形の半導体（クラッド層：clad layer）で挟みこんだダブルヘテロ（DH：

Double Hetero）構造をしている．Fig.2-5 (a)は，熱平衡状態にある場合のダブルヘテロ構造半導体のエネルギーバンド図である．熱平衡状態では n 形クラッド層の電子はヘテロ障壁を越えることができないが，順方向に電圧を印加する（順方向に電流を流す）と Fig.2-5 (b)のようにバンド構造が変化して，n 形クラッド層の電子がヘテロ障壁を越えて活性層に注入される．活性層に注入された電子は，p 形クラッド層のエネルギー準位が高いため，p 形クラッド層に拡散することができずに活性層内に蓄えられる．こうして電子や正孔が高密度に集まった活性層は大きな反転分布を得ることができる．これをキャリアの閉じ込め効果と呼ぶ．また活性層の屈折率をクラッド層の屈折率より大きくしておくと，光は屈折率の大きいところを通る性質があるため，電子と正孔の再結合によって発生した光は Fig.2-5 (c)のように活性層内に閉じ込められる．さらにここから半導体がレーザとして発振を得るためには，この活性層での発光をフィードバックして誘導放出を誘発させる必要がある．Fig.2-4 に示すようにダブルヘテロ構造の半導体にヘテロ面に垂直な 1 対の互いに平行な端面を作ると，活性層を伝わる光の一部は 2 つの端面（鏡面）で反射される．これがファブリペロー共振器として働くことになる．ダブルヘテロ構造の場合，活性層に発生した光は，活性層に沿って伝搬しやすいためほとんどの光は，ファブリ・ペロー共振器によって繰り返し反射され再び活性層を通過すると誘導放出が更に進み，一層光が増幅される．そしてファブリ・ペロー共振器内で定在波が発生すると周波数と位相が揃った光だけが増幅され，半導体レーザが発振に至る．

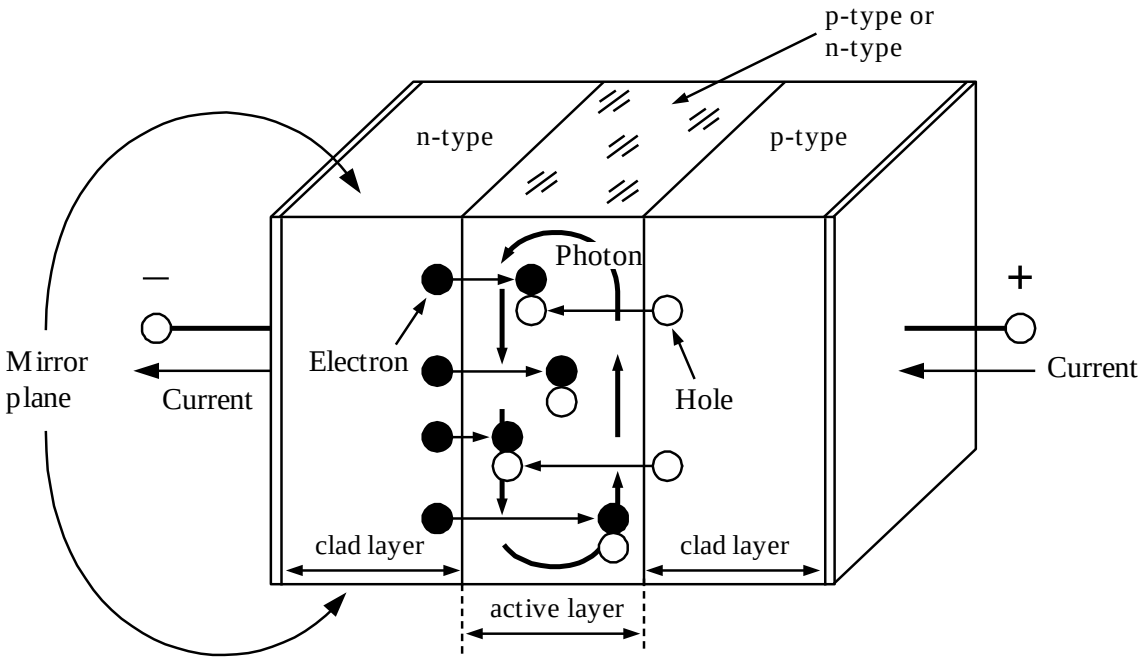
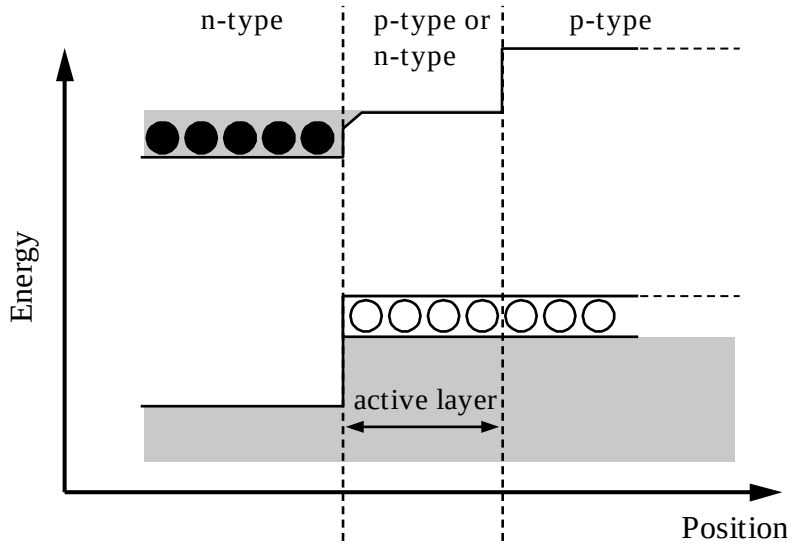
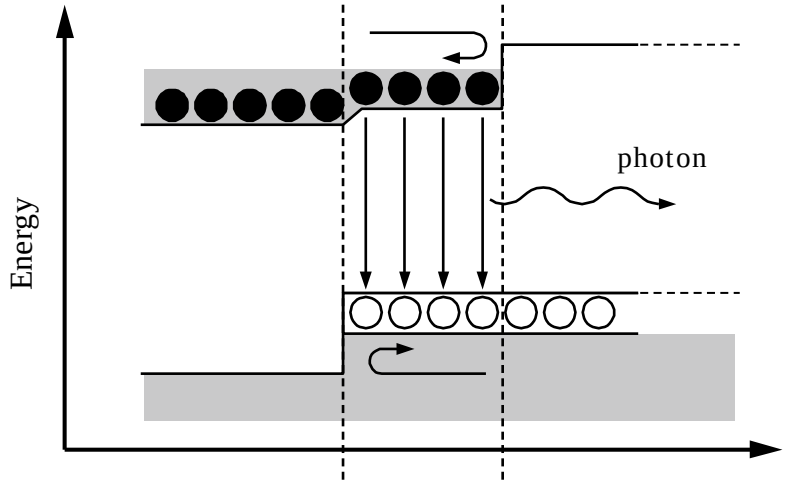


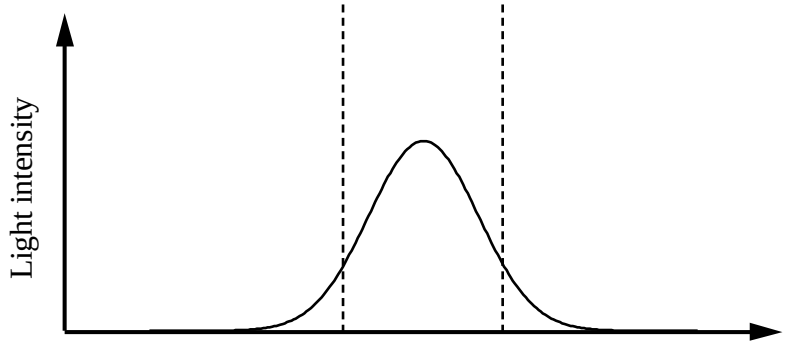
Fig.2-4 Double Hetero Structure Laser Diode.



(a) Energy band diagram in thermal equilibrium



(b) Energy band diagram out of thermal equilibrium



(c) Light intensity distribution

Fig.2-5 Energy band and Light intensity distribution of Double Hetero structure.

2.1.4 ファブリ・ペロー共振器とレーザ発振[17][18]

ファブリ・ペロー共振器（Fabry-Perot resonator）は，Fig.2-6 (a)に示すように 2 枚のミラーを平行に対向させたものである．前項でも述べたように，半導体レーザは，ファブリ・ペロー共振器内に光の定在波を生じさせることで発振に至る．この定在波は共振器のミラー間の光学的距離がその光の半波長の整数倍に等しいという条件を満たしたときに発生する．すなわち，光の波長をλ_m，ミラー間の光学的距離をl，レーザ媒質の屈折率を n とすると，光の波長は，以下の条件を満たす．

$$\lambda_m = \frac{2nl}{m} \qquad (m = 1, 2, 3, \cdots) \tag{2-2}$$

また(2-3)式を周波数に置き換えると，

$$\nu_m = \frac{cm}{2nl} \tag{2-3}$$

となる．ここで，c（3×10^8 m/s）は光速である．これらの式から，レーザが発振可能な周波数は連続ではなく飛び飛びの値となることが分かる．このmによって区別される状態を第m次の縦モードといい，隣り合う縦モードの周波数間隔$\Delta\nu_m$は，

$$\Delta\nu_m = \frac{c}{2nl} \tag{2-4}$$

と表すことができる．また縦モードの周波数は Fig.2-6 (c)で示すように$\Delta\nu_m$の間隔で等間隔に並ぶことになる．図では縦モードの幅$\Delta\nu_c$を持つように表してあるが，この幅は共振器の損失に依存している．そして，発振は Fig.2-6 (b)で示すような媒質の利得スペクトルと共振器の縦モードのスペクトルが重複する周波数の位置において生じる．

ここで，レーザが発振するための利得条件について述べる．レーザ発振が起こるためには，共振器内を伝わる光の，誘導放出による増幅利得が損失に打ち勝つ必要がある．共振器の損失は，共振器の壁面での散乱，吸収，さらに媒質での光の吸収による損失α_lの他に，結晶端面での損失があり，これらを合わせたものが共振器全体の損失となる．共振器全体の損失をα_{tl}とおくと，α_{tl}は以下のように求めることができる．

$$\alpha_{tl} = \alpha_l + \frac{1}{l}\cdot ln\left(\frac{1}{R}\right) \tag{2-5}$$

ここで，Rは鏡面の反射率である．Fig.2-4 のようにへき開面を利用したレーザでは，鏡面の反射率 R は，

$$R = \left(\frac{n-1}{n+1}\right)^2 \tag{2-6}$$

で表され，一般に半導体結晶の屈折率は n = 2.7 であるため R = 30%となる．

レーザを発振させるためには損失α_{tl}と同等以上の利得が必要であるため閾値利得 G_{th} は，

$$G_{th} = \alpha_{tl} \tag{2-7}$$

の条件を満たす必要がある．これがレーザ発振のための利得条件である．

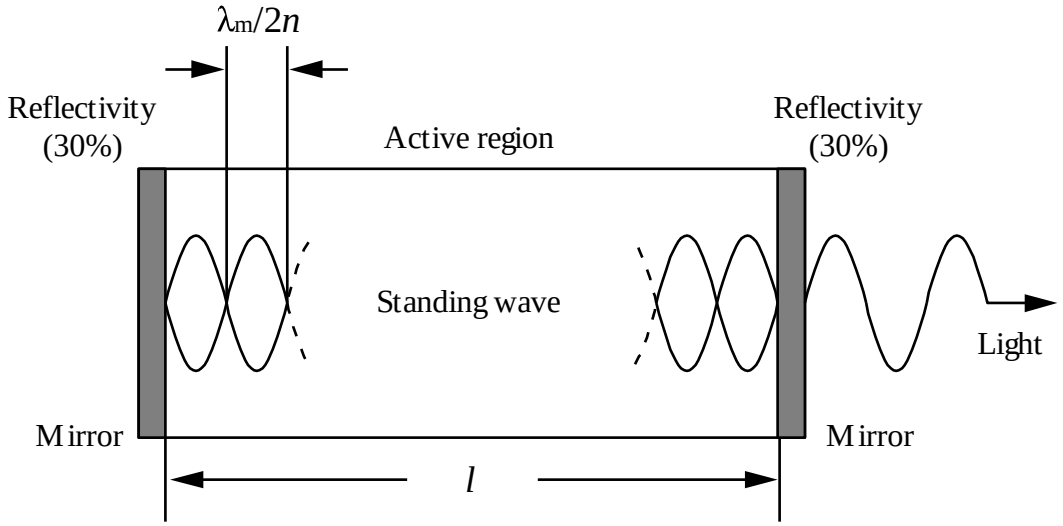
すでに述べたように，縦モードスペクトルは共振器損失の大きさに依存したスペクトル幅$\Delta\nu_c$を持ち，

$$Q_c = \frac{2\pi\nu n}{c\alpha_{tl}} \tag{2-8}$$

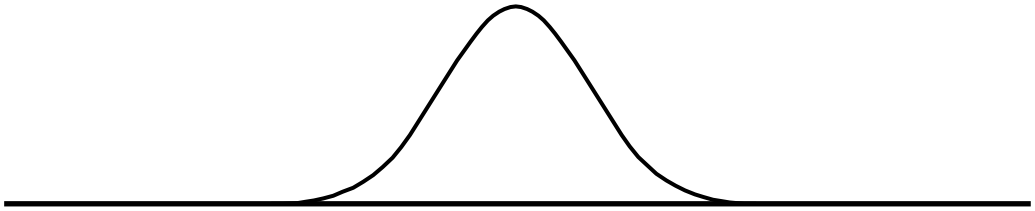
とおくと，スペクトル幅$\Delta\nu_c$は，

$$\Delta\nu_c = \frac{\Delta\nu_m}{Q_c} \tag{2-9}$$

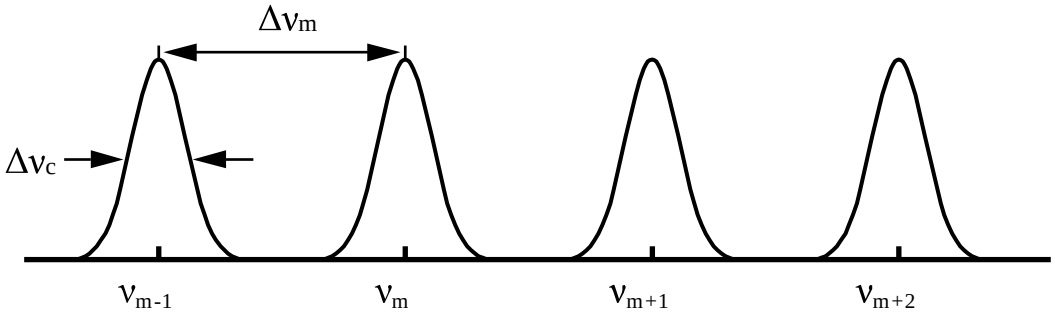
と表すことができる．ここで，Q_cは一般にQ値と呼ばれるスペクトルの鋭さを示す値で，共振器の性能を示す指標としてよく用いられる．



(a) Fabry-Perot resonator



(b) Gain spectrum of spontaneous emission



(c) Longitudinal mode

(d) Oscillation mode

Fig.2-6 Fabry-Rerot resonator and laser oscillation.

2.2 動作特性[17][19]～[22]

半導体レーザは他のレーザに比べて独特な動作上の特性を示す．本節では電流－光出力特性，及び周波数特性について述べる．

2.2.1 電流-光出力特性

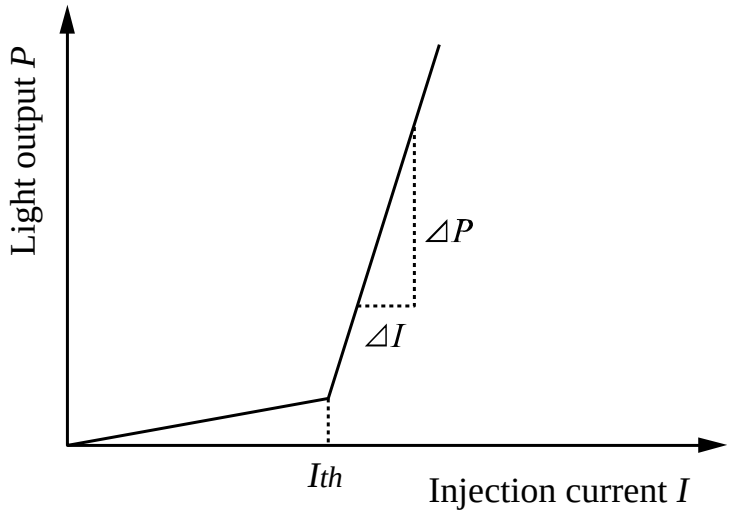


Fig.2-7 A semiconductor laser's light power - injection current characteristic.

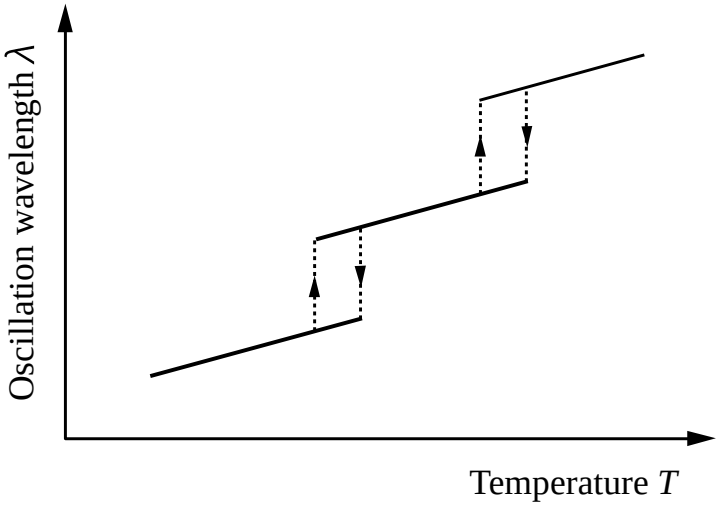
Fig.2-7 は，半導体レーザの注入電流（Injection current I）-光出力（Light power P）特性の典型的な例を示している．図から半導体レーザの光出力は注入電流が閾値電流（Threshold current I_{th}）に達するまでは非常に小さい値であることが分かる．これは活性層が十分なキャリア密度を得ることができず，利得条件を満足することができないために，自然放出による極弱い光しか発生しないからである．一方，注入電流が閾値電流を越えると光出力が急激に増大して素子はレーザ発振の状態になる．発振状態では，光出力は注入電流に対して直線的に増加する．このときの電流-光出力特性の傾き$\Delta P/\Delta I$は，レーザの効率の目安となる．また，次式で表されるように，閾値電流には温度依存性があり，温度の増加と共に指数関数的に増加する．

$$I_{th} = exp\frac{T_1}{T_0} \tag{2-10}$$

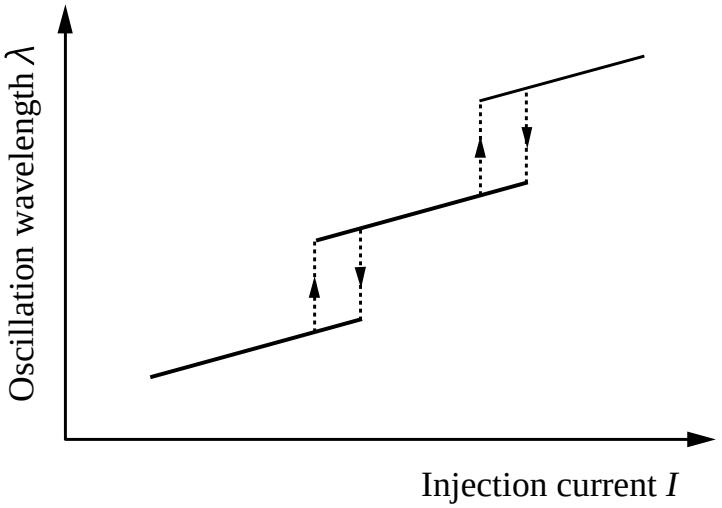
T_1は半導体レーザの活性層の温度，T_0は特性温度と呼ばれる閾値電流の温度依存性を特徴付けるパラメータである．閾値電流がこのような温度依存性を持つのは，活性層の伝導帯に存在する電子の一部が温度上昇に伴いヘテロ障壁を越えて p 形クラッド層に拡散されるこ

とにより，反転分布を得るのにより多くのキャリア数を必要とするためである．また，閾値電流は活性層の面積，ミラーの反射率，活性層とクラッド層のバンドギャップと屈折率の差など，多くの設計パラメータにも依存する．

2.2.2 周波数特性



(a) Oscillation wavelength - Temperature characteristic



(b) Oscillation wavelength - Injection current characteristic

Fig.2-8 A semiconductor laser's wavelength - temperature and injection current characteristic.

半導体レーザの発振周波数（発振波長：Oscillation wavelength λ）には温度（Temperature T）依存性と温度に起因する注入電流依存性が存在する．Fig.2-8 (a), (b)は，それぞれ，半導体レーザの発振波長に対する温度と注入電流の典型的な依存特性を示している．

図のように半導体レーザの発振波長が変わるのは，主に活性層内の屈折率が温度変化に比例して変化するためである．これは(2-2)式からも明らかである．注入電流の場合も，その変化に伴う活性層の温度変化が原因である．また，図中の不連続な部分は半導体レーザ特有のもので，モードジャンプ（あるいはモードホッピング）と呼ばれている．これは温度変化によってエネルギーギャップが変化し，縦モードが別のモードに切り替わることで起こる．

レーザの連続発振時の発振スペクトルは，(2-2)式の発振条件を満たす飛び飛びの縦モードからなり，その間隔$\Delta\lambda_m$は次式で表される．

$$\Delta\lambda_m = \frac{\lambda_m^2}{2n_{eff}l} \tag{2-11}$$

ただし，n_{eff}は分散を考慮した実効的な屈折率で，次式で表される．

$$n_{eff} = n - \lambda_m \cdot \frac{dn}{d\lambda_m} \tag{2-12}$$

レーザの光出力を増加していくと，n_{eff}が大きくなると共にスペクトルのパワーは1本の縦モードに集中していくため，その他のパワーは無視することができるようになる．これを単一縦モード発振という．単一縦モード発振している状態では，半導体レーザのスペクトル幅はほぼ自然放出光の存在により生じる位相揺らぎで決まる．

2.3 周波数雑音

単一縦モード半導体レーザの発振周波数の揺らぎは，温度揺らぎや機械的な振動に起因する共振器の伸縮，電子移動度の揺らぎに起因するフリッカー雑音の混入，自然放出光揺らぎおよびそれによって誘発された屈折率揺らぎなどに起因する光位相の変動などが原因である[23]．温度揺らぎや機械的振動，フリッカー雑音は，その性質上周波数が低い領域（0～数 MHz）の周波数の揺らぎを発生させる．対して，自然放出光揺らぎと屈折率揺らぎは，周波数が低い領域から高い領域まで広い周波数範囲（0～数 GHz）にわたってフラットな周波数の揺らぎを発生させる[24]．半導体レーザの発振原理に基づく本質的な周波数の揺らぎの原因は，この自然放出光揺らぎと屈折率揺らぎである．本論文では，私たちはこの自然放出光揺らぎと屈折率揺らぎに起因する周波数の揺らぎを，周波数雑音と呼ぶこととする．この半導体レーザの周波数雑音の性質を，Power Spectral Density（PSD）によって示す．半導体レーザの周波数雑音の Power Spectral Density（PSD）は，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付け加えることにより，次式のように求められる[23][25][26]．

$$PSD_{FM}(f) = \frac{(\delta f)_{ST}}{\pi}\left[1 + \frac{\alpha^2 f_R^4}{(f_R^2 - f^2)^2 + (\gamma_e/2\pi)^2 f^2}\right] \qquad (2\text{-}13)$$

ここで，αは電子密度の変化に伴う屈折率の変化によって導入されるスペクトル線幅増大係数（$|\alpha| = 2$～6），f_Rはレーザの過度的動作で観測される緩和振動周波数，γ_eはその緩和振動のダンピング定数である．$(\delta f)_{ST}$は Schawlow-Townes' formula 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揺らぎを表す．$(\delta f)_{ST}$は次式のように表される[23]．

$$(\delta f)_{ST} = \frac{h\nu_0}{8\pi P_0}\left(\frac{c}{nL}\right)^2 \left(\alpha_l L + ln\frac{1}{R}\right)\left(ln\frac{1}{R}\right) n_{sp} \qquad (2\text{-}14)$$

ここで，$h\nu_0$は光子のエネルギー，c は真空中の光速，P_0はレーザ共振器内の光電力，n はレーザ媒質の屈折率，L はレーザ共振器長，α_lはレーザ共振器内部損失，R はレーザ共振器端面反射率，n_{sp}は自然放出光係数（=1～2）である．単一縦モード半導体レーザの周波数雑音の PSD とレーザパワーの関係が Fig.2-9 に示されている．Fig.2-9 の周波数雑音の PSD は，代表的な単一縦モード半導体レーザのパラメータを素に，(2-13)式によって計算されている．Fig.2-9 から周波数雑音が，レーザのパワー（すなわち，注入電流）が大きいほど雑音レベルが小さくなること，そして緩和振動周波数で共鳴上のピークを持つことが確認できる[27]．緩和振動周波数の共鳴ピークの存在を無視した場合，周波数雑音は白色雑音の特性を数

GHz の帯域に持つといえる．この場合の白色雑音の PSD の値は，(2-13)式において$f \cong 0$の時の PSD とほぼ近似できる．よって，周波数雑音の PSD は，近似的に

$$PSD_{FM}(f) \cong \frac{(\delta f)_{ST}(1+\alpha^2)}{\pi} \tag{2-15}$$

と求めることができる[23][28]. (2-15)式の$(\delta f)_{ST}(1+\alpha^2)$は、Modified Schawlow-Townes' formula と呼ばれ，半導体レーザの発振スペクト幅の限界値を示す．(2-24)式から半導体レーザの周波数雑音の PSD は，半導体レーザの発振スペクトル幅と比例関係にあることが分かる．半導体レーザと他の種類のレーザとの相違点は，スペクトル線幅増大係数α が 0 でないことである．したがって半導体レーザの周波数雑音の PSD は，他の種類のレーザの周波数雑音の PSD と比べて，$(\delta f)_{ST}\alpha^2/\pi$だけ増大することになる．これは，半導体レーザが他の種類のレーザと比べ，大きな周波数雑音を持っていることを意味する．

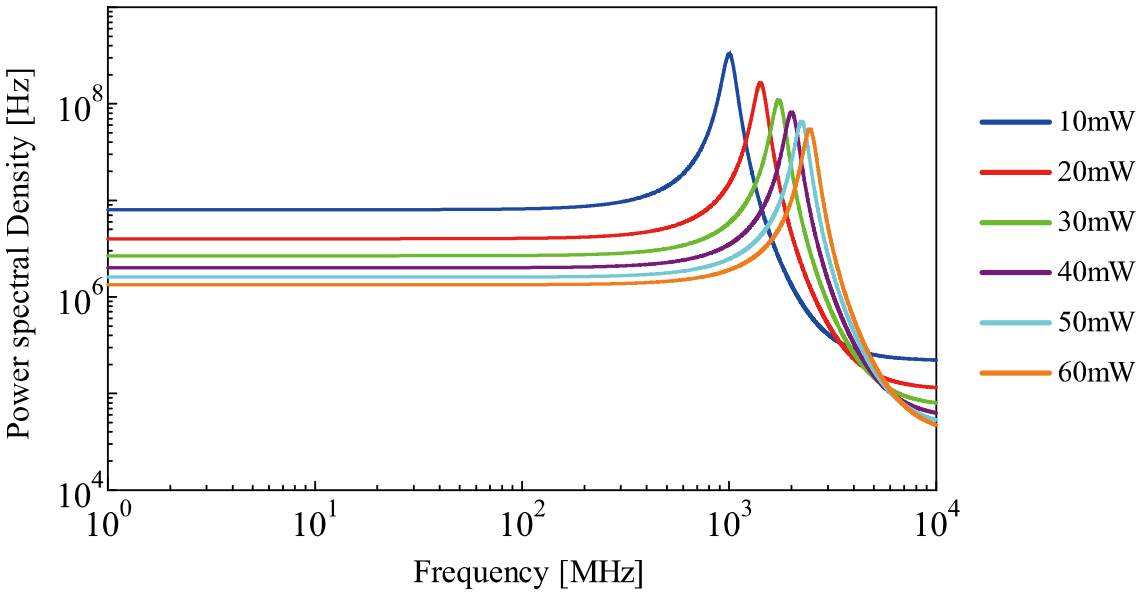


Fig.2-9 Dependence of diode lasers' frequency noise-related spectral density on its power.

第 3 章 周波数雑音の検出

本章では，半導体レーザの周波数雑音の電量スペクトル密度の測定と雑音信号の検出方法について述べる．また半導体レーザの周波数雑音を検出するために使用する Rb 原子の吸収線について説明する．

3.1 マイケルソン干渉計による周波数雑音の電力スペクトル密度の測定[28][29]

半導体レーザの周波数雑音の電力スペクトル密度（PSD）の測定は，マイケルソン干渉計を用いて行うことができる．Fig.3-1 は，周波数雑音の PSD を測定するためのマイケルソン干渉計の実験系を示している．半導体レーザの周波数雑音，すなわち周波数のゆらぎは，マイケルソン干渉計によって強度のゆらぎに変換される．そのためマイケルソン干渉計の出力を光検出器で受光して，その交流成分をスペクトルアナライザーで観測することで PSD を測定することができる．

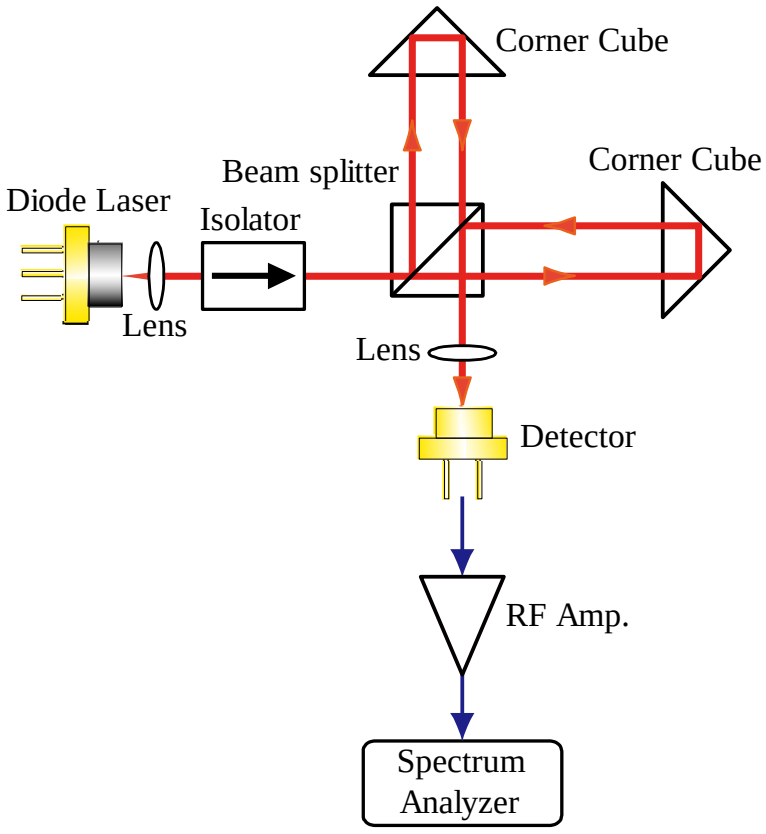


Fig.3-1 Measuring setup for DL's frequency-noise by a Michelson interferometer.

周波数雑音の PSD の測定原理について説明する．レーザ出射光の電界を

$$E(t) = A \cdot exp[j\{\omega_0 t + \phi(t)\}] \tag{3-1}$$

とおく．ここで，A，ω_0，$\phi(t)$はそれぞれレーザー光の電界振幅，平均角周波数および位相である．また強度雑音は小さいとして無視する．光検出器の出力電流$i(t)$は次式で与えられる．

$$i(t) = i_0 + \frac{i_1}{2} cos\{\omega_0 \tau_0 + \Delta\phi(t)\} \tag{3-2}$$

ここで，i_0とi_1はそれぞれ光検出器の出力電流の直流成分および交流成分である．また，

$$\tau_0 = 2l/c \tag{3-3}$$

であり，

$$\Delta\phi(t) = \phi(t + \tau_0) - \phi(t) \tag{3-4}$$

である．ここでlはマイケルソン干渉計の光路長差である．

測定では，マイケルソン干渉計の光路長差を調整して，

$$\omega_0 \tau_0 = \left(n + \frac{1}{2}\right)\pi \tag{3-5}$$

n：整数

となるようにし，また$\Delta\phi(t) \ll \pi/2$と仮定すると，(3-2)式は

$$i(t) = i_0 - \frac{i_2}{2} \cdot \Delta\phi(t) \tag{3-6}$$

となる．(3-6)式より，光検出器の出力電流の交流成分は時間τ_0内に生じた位相差$\Delta\phi(t)$に比例していることがわかる．ここで，$\Delta\phi(t)$の電力スペクトル密度を$PSD_{\Delta\phi}(f)$とすると，(3-4)式および周波数ゆらぎは光位相の時間微分であることより，次の関係式が成り立つ．

$$PSD_{\Delta\phi}(f) = (2\pi\tau_0)^2 \left[\frac{sin(\pi f\tau_0)}{\pi f\tau_0}\right]^2 PSD_{FM}(f) \qquad (3\text{-}7)$$

また，光検出器の出力電流$i(t)$の交流成分の電力スペクトル密度$PSD_i(f)$と$PSD_{\Delta\phi}(f)$は，次のような関係が成り立つ.

$$PSD_{\Delta\phi}(f) = \frac{PSD_i(f)}{(i_1/2)^2 R\Delta f} \qquad (3\text{-}8)$$

ここで，Rは受光回路の交流負荷抵抗，Δfはスペクトルアナライザーの分解能である．周波数雑音の電力スペクトル密度$PSD_{FM}(f)$は，スペクトルアナライザー上の電力スペクトルの値$PSD_i(f)$から(3-7)，(3-8)式を用いて計算処理すれば求められる．

3.2 周波数弁別器を使用した周波数雑音の検出

半導体レーザの周波数雑音の検出は，Fig.3-2 に示すようにレーザ光を周波数弁別器に入射し，その透過光を光検出器で受光して得られる電気信号を測定することで行う．この方法は，通信における FM 信号の復調技術として知られるスロープ検波の原理に類似している．周波数弁別器は，ファブリ・ペロー共振器[30][31][32]や原子・分子の吸収線[14][33]が用いられる．我々の研究では，周波数弁別器に Rb 原子の吸収線を使用する．レーザにおける周波数弁別器は，入射光の周波数に応じて透過光量が変化する光学素子である．この作用によって，周波数雑音は透過光強度の変化として検出される．

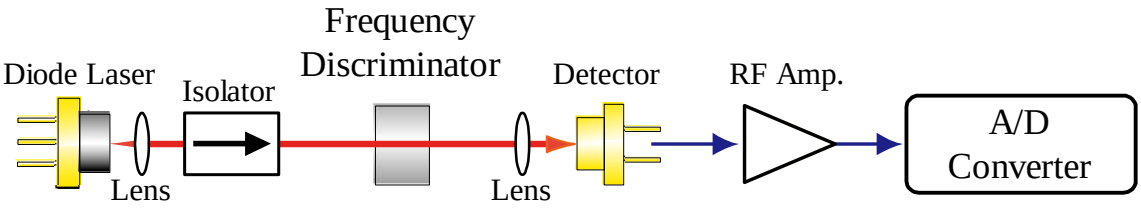


Fig.3-2 DL's frequency-noise detection system using a Frequency Discriminator.

半導体レーザの周波数雑音の検出原理について簡単に説明する．半導体レーザの周波数雑音は，半導体レーザの中心周波数が白色雑音の特性を持つ信号で周波数変調された状態であると仮定することができる．ここでは，説明を簡単にするために単一周波数で周波数変調されたレーザ光の電界を考える．レーザ光の電界E_{FM}は次式で表される．

$$E_{FM} = E_0 sin\left\{2\pi f_c t + \frac{f\Delta}{f_s} sin2\pi f_s t\right\} = E_0 sin(2\pi f_c t + \beta sin2\pi f_s t) \qquad (3\text{-}9)$$

ここで，f_cは半導体レーザの中心周波数，f_sは変調周波数，$f\Delta$は周波数偏移，βは変調指数である．また変調指数βは，変調の深さである周波数偏移$f\Delta$と変調周波数f_sより$\beta = f\Delta/f_s$と定義される．半導体レーザの周波数雑音の$f\Delta$は，周波数雑音が存在する帯域より非常に狭いため$\beta \ll 1$である．このとき，電界E_{FM}は，n次のベッセル関数J_nを用いて以下のように近似できる．

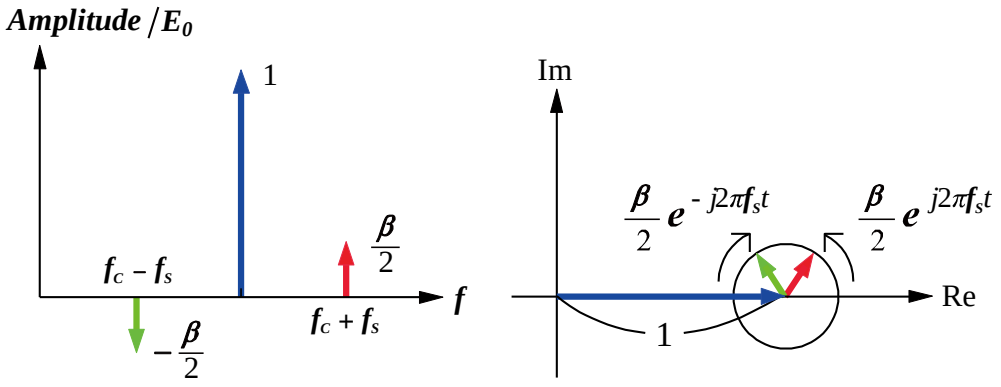
$$\begin{aligned} E_{FM} &\cong E_0\{J_0(\beta)sin2\pi f_c t + J_1(\beta)sin2\pi(f_c + f_s)t - J_1(\beta)sin2\pi(f_c - f_s)t\} \\ &\cong E_0\left\{sin2\pi f_c t + \frac{\beta}{2}sin2\pi(f_c + f_s)t - \frac{\beta}{2}sin2\pi(f_c - f_s)t\right\} \end{aligned} \qquad (3\text{-}10)$$

また式(3-10)のフェーザ表示は次式で表される．

$$E_{FM} = E_0\left\{e^{j2\pi f_c t} + \frac{\beta}{2}e^{j2\pi(f_c+f_s)t} - \frac{\beta}{2}e^{j2\pi(f_c-f_s)t}\right\}$$

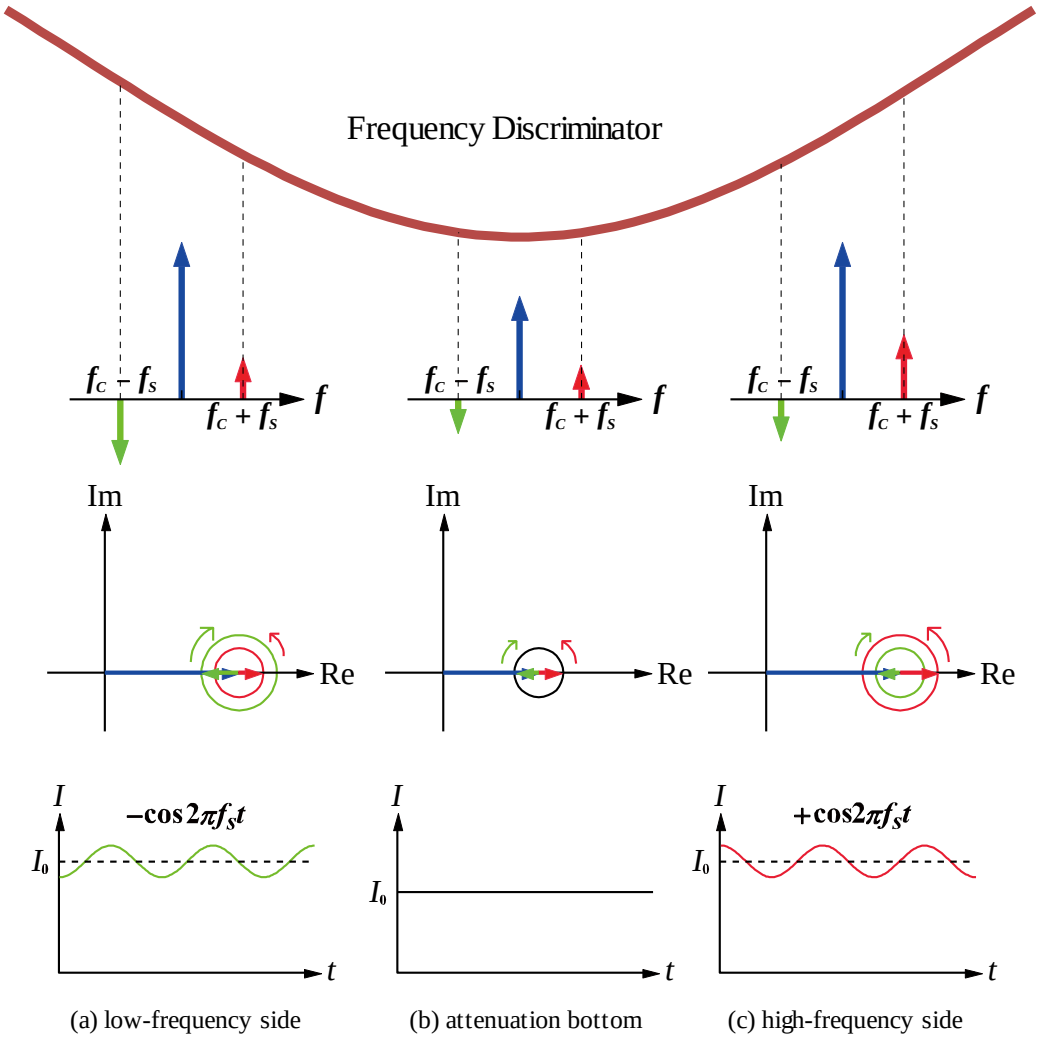
$$= E_0 e^{j2\pi f_c t}\left\{1 + \frac{\beta}{2}e^{j2\pi f_s t} - \frac{\beta}{2}e^{-j2\pi f_s t}\right\} \qquad (3\text{-}11)$$

Fig.3-3 (a)，(b)に，式(3-11)に対応する片側線スペクトルとフェーザ図が示されている．周波数変調のスペクトルは，低側波帯要素が高側波帯要素と逆符号となる．この 2 つの側波帯フェーザは，$e^{j2\pi f_c t}$で回転する複素平面上で，$\beta/2\, e^{j2\pi f_s t}$が反時計回り，$\beta/2\, e^{-j2\pi f_s t}$が時計回りに回転する．Fig.3-3 (b)より 2 つの側波帯フェーザによってレーザ光の電界の角周波数が変化することが分かる．また$e^{j2\pi f_c t}$のフェーザの大きさに比べ，2 つの側波帯フェーザの大きさが非常に小さいため（$\beta \ll 1$），レーザ光の電界振幅はほぼ一定と見なすことができる．Fig.3-4 には，周波数弁別器が周波数変調された半導体レーザの変調信号を検出する原理が示されている．周波数弁別器を透過したレーザ光は，入射レーザ光の発振周波数に応じて異なる減衰量で減衰される．これは，半導体レーザの中心周波数が周波数変調された場合，レーザ光の電界フェーザの左右のサイドバンドの大きさのバランスが崩れることを意味している．Fig.3-4 (b)の attenuation peak では，サイドバンドの大きさが等しいため，レーザ光の電界振幅は一定である．この場合レーザ光が周波数弁別器を通過した時の透過光強度は，一定の強度を示す．それに対して Fig.3-4 (a)，(c)のようにサイドバンドのバランスが崩れると，レーザ光の電界振幅に大きいほうのサイドバンドフェーザの影響が大きく表れる．これは，複素平面上ではレーザ光の電界振幅変調と同等の作用を持つ．よってレーザ光が周波数弁別器を通過した時の透過光強度には，サイドバンドフェーザの角周波数と同じ周期の信号が透過光強度の変化として現れる[33]．変調信号は，光検出器から得られた透過光強度信号の不要な直流成分をハイパスフィルタによって除去することで検出される．周波数雑音のような複数の周波数変調信号を検出する場合でも，$\beta \ll 1$であるならば，重ね合わせの理が成り立つため，同様の方法で検出することが可能である．



(a) Sideband electric fields　　(b) phasor diagram

Fig.3-3 Sideband electric fields of the FSK (Frequency Shift Keying) signal and its phasor diagram.



(a) low-frequency side (b) attenuation bottom (c) high-frequency side

Fig.3-4 Detection principle of a DL's FSK signal. Sideband electric fields, phasor diagram, and transmitted light intensity.

3.3 ルビジウム原子の吸収線[34][35][36][37]

周波数弁別器として使用する Rb 原子は，原子番号 37，原子量 85.5 のアルカリ金属原子である．自然界には質量数が 85 と 87 の同位体がそれぞれ 72%，28%の割合で存在する．また Rb 原子は，最外殻電子が基底状態から励起状態へと遷移するときのエネルギー差によって決まる波長の光を吸収し，その吸収スペクトルの数は，最外殻電子のとり得るエネルギー準位の数によって決まっている．以下に Rb 原子の原子構造について説明する．

Rb 原子では，K 殻から N 殻の 4p 準位までの電子が，原子の芯となって安定している．そのため Rb 原子の吸収線は，最外殻電子の O 殻の 5s と 5p 準位の間での遷移に対応する．量子力学では，このエネルギー準位の違いを，電子の軌道角運動量に比例する量子数 L で表す．L の値は 5s 準位と 5p 準位で，それぞれ $L = 0$，$L = 1$ となる．また，この遷移に伴う L の変化量をΔLとすると，$\Delta L = \pm 1$を満たすもの以外の遷移は許されないという規則がある．これは選択規則と呼ばれる．また，電子は殻の周りを回る角運動量の他に，それ自身の軸の周りに大きさが$\pm 1/2$の角運動量を持っている．これは電子スピンと呼ばれ，この電子スピンによる付加角運動量を S とすれば，L と S の相互作用による原子の全角運動量を新しい量子数 J で表現することができる．J は次のベクトル和で表される．

$$J = L + S \tag{3-12}$$

式(3-12)は，L と S が J の周りで歳差運動をしていることを示している．その様子は Fig.3-5 に示されている．

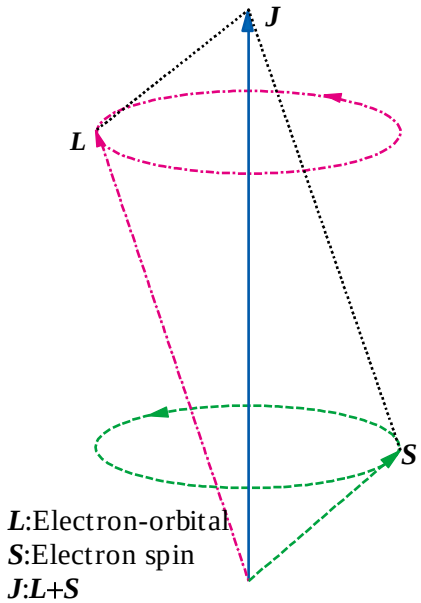
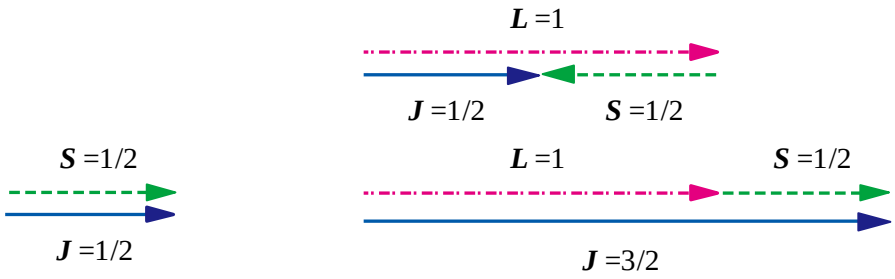


Fig.3-5 Precession of angular momentum around ***J***.

また，(3-12)式より，J，L，S には以下の関係が成り立つ．

$$J = L + S, L + S - 1, L + S - 2, \Lambda, |L - S| \qquad (3\text{-}13)$$

最外殻電子が 1 つである Rb 原子は，$S = 1/2$であるため，式(3-13)より 5s 準位は$J = 1/2$，5p 準位は$J = 1/2$，$J = 3/2$（2 つの準位に分裂している）である．また，J には L と同様に選択規則があり，$\Delta J = 0, \pm 1$となる．ただし，$J = 0 \rightarrow J = 0$への遷移は禁止されている．Fig.3-6 は，その J のベクトル図である．



(a) 5s($\boldsymbol{L}$ =0, $\boldsymbol{S}$ =1/2)　　(b) 5p($\boldsymbol{L}$ =1, $\boldsymbol{S}$ =1/2)

Fig.3-6 Vector diagram of $\boldsymbol{J}$.

この 5s 準位（$J = 1/2$）から 5p 準位（$J = 1/2$）への遷移スペクトル線と 5p 準位（$J = 3/2$）への遷移スペクトル線は，それぞれ D_1 線（周波数 377THz、波長 794.76nm），D_2 線（周波数 384THz、波長 780.02nm）と呼ばれる．さらに，原子核も自身の軸の周りに角運動量を持っており，同位元素によって異なる値をとる．これは核スピンと呼ばれる．この核スピンによる付加角運動量を量子数 I とすれば，全角運動量 F は次のベクトル和で表される．

$$F = J + I \qquad (3\text{-}14)$$

Fig.3-7 は，I と J が F を軸として歳差運動を行っている様子を示している．
また，F は(3-14)式より，

$$F = J + I, J + I - 1, J + I - 2, \Lambda, |J - I| \qquad (3\text{-}15)$$

の関係が成り立つ．I は ^{85}Rb 原子で$I = 5/2$，^{87}Rb 原子で，$I = 3/2$である．5s，5p 準位は F の数だけ分岐するが，この場合の選択規則も$\Delta F = 0, \pm 1$であり，$F = 0 \rightarrow F = 0$の遷移は禁止されている．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．Fig.3-8 は，その F のベクトル図である．また Fig.3-9 と Fig.3-10 は，それぞれ L，J，F を考慮した ^{85}Rb と ^{87}Rb 原子の 5s，5p 準位の分岐の様子を示したものである．

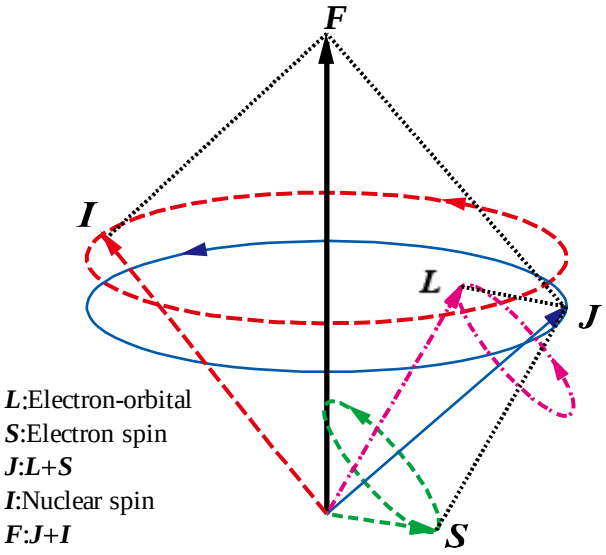
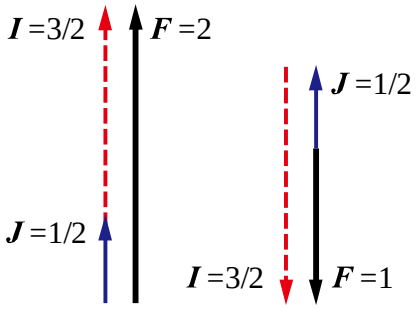
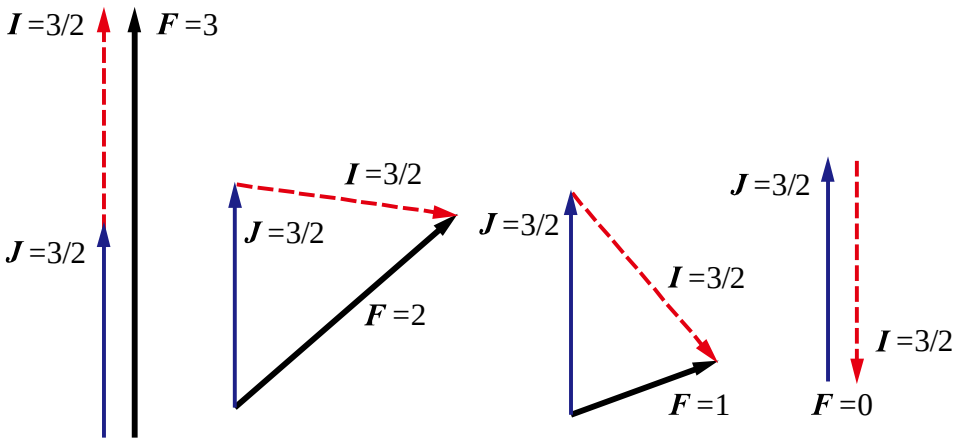


Fig.3-7 Precession of angular momentum around ***F***.

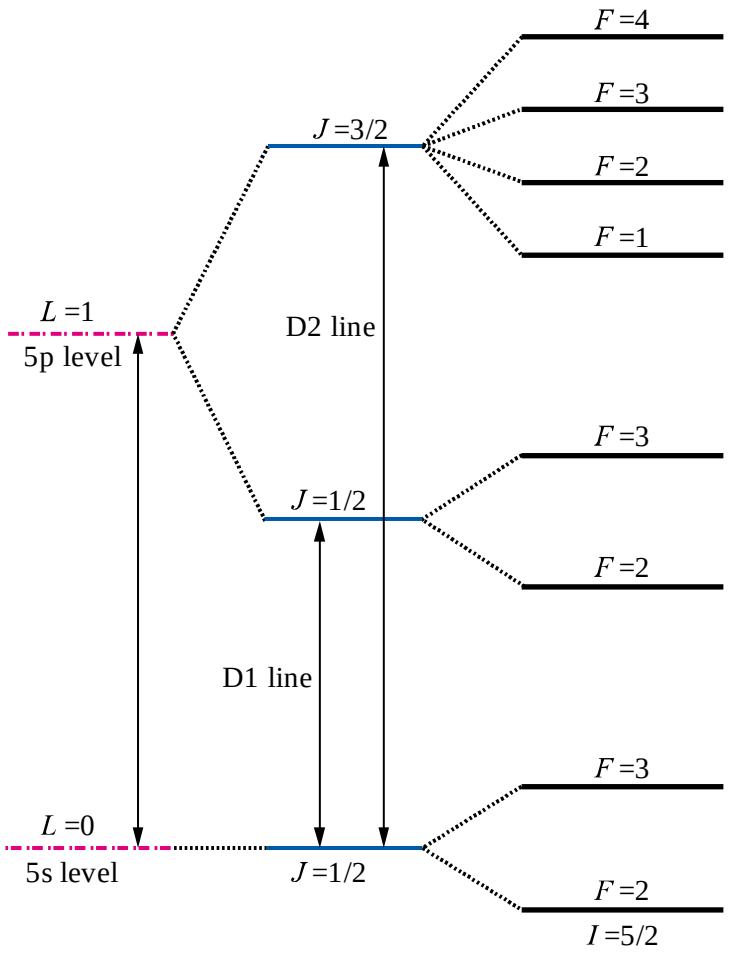


(a) 5s5p(***J*** =1/2, ***I*** =3/2)



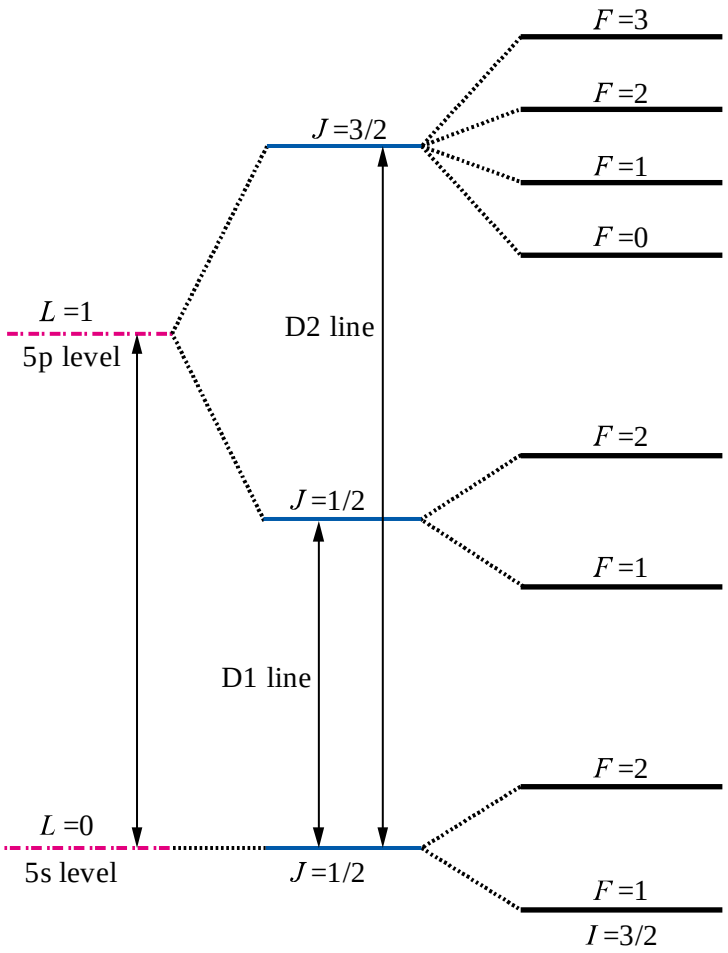
(b) 5p(***J*** =3/2, ***I*** =3/2)

Fig.3-8 Vector diagram of ***F***.



(a) Normal structure (b) Fine structure (c) Hyperfine structure

Fig.3-9 Spectrum separation of the ^{85}Rb absorption line.



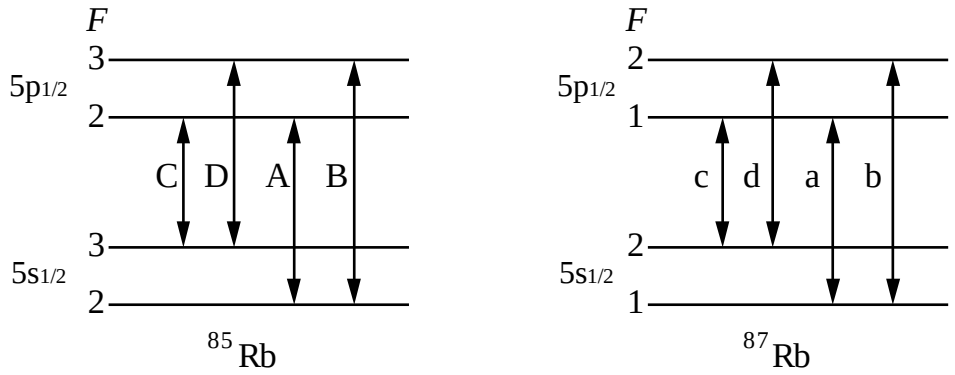
(a) Normal structure (b) Fine structure (c) Hyperfine structure

Fig.3-10 Spectrum separation of the ^{87}Rb absorption line.

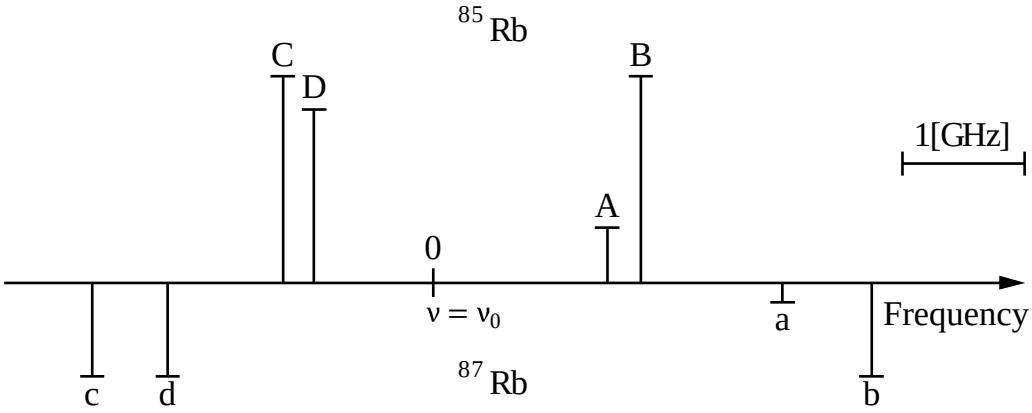
超微細構造では，Rb 原子の吸収スペクトルは，^{85}Rb と ^{87}Rb を合わせて D_1 線で 8 本，D_2 線で 12 本存在する．これらのスペクトル線は全て同じ強さでは無く，F，I，J の有理式で定義される強度規則により定まる相対強度となる．その位置も同様に F，I，J の有理式から相対的位置（相対周波数）となって求まる．Table 3-1 と Table 3-2 に，それぞれ D_1 線と D_2 線の相対強度と相対的位置の値を示す．また，Fig.3-11 と Fig.3-12 に，それぞれ D_1 線と D_2 線の可能な遷移と相対強度，相対的位置を示す．

Table 3-1 Intensity of each spectrum of hyperfine structure of the Rb-D_1 line.

^{85}Rb			^{87}Rb		
Transition	$\nu - \nu_0$(GHz)	Relative intensity	Transition	$\nu - \nu_0$(GHz)	Relative intensity
A	1.563	28.6	a	3.765	7.4
B	1.926	100.0	b	4.581	37.2
C	-1.482	100.0	c	-3.075	37.2
D	-1.119	80.0	d	-2.259	37.2



(a) Energy level and transition

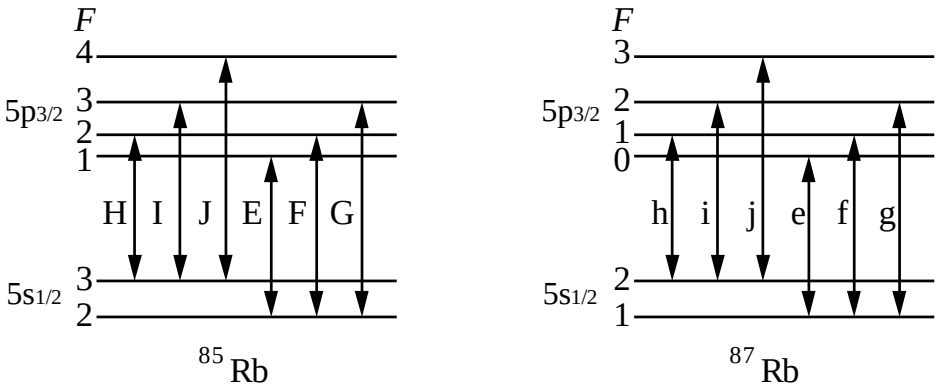


(b) Relative position of each spectrum

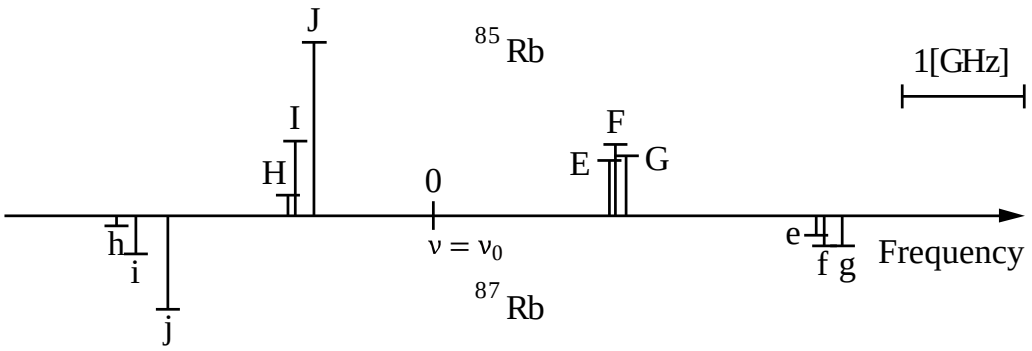
Fig.3-11 Hyperfine structure of the Rb-D_1 line.

Table 3-2 Intensity of each spectrum of hyperfine structure of the Rb-D_2 line.

^{85}Rb			^{87}Rb		
Transition	$\nu - \nu_0$(GHz)	Relative intensity	Transition	$\nu - \nu_0$(GHz)	Relative intensity
E	1.659	33.4	e	3.969	6.4
F	1.692	43.2	f	4.041	16.1
G	1.765	34.6	g	4.203	16.1
H	-1.353	12.3	h	-2.799	3.2
I	-1.289	43.2	i	-2.637	16.1
J	-1.167	100.0	j	-2.370	45.0



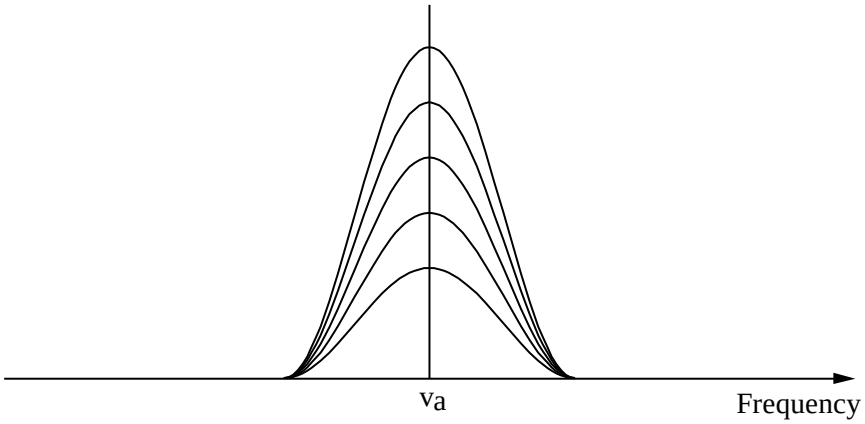
(a) Energy level and transition



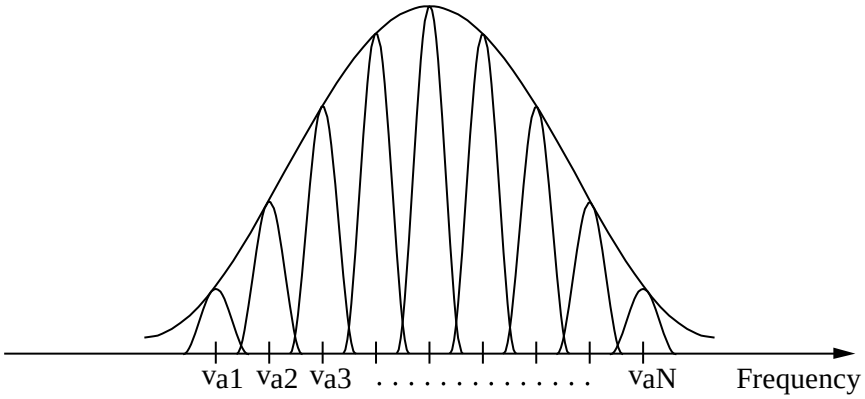
(b) Relative position of each spectrum

Fig.3-12 Hyperfine structure of the Rb-D_2 line.

3.4 スペクトルの広がり[34][38][39]



(a) Homogeneous broadening



(b) Inhomogeneous broadening

Fig.3-13 Spectrum broadening.

実際に観測される原子の吸収スペクトルは，光が入射した全原子の吸収スペクトルを重ね合わせたものであり，そのためエネルギーと時間の不確定性から広がりを持つことになる．各々の原子の持つ共鳴周波数ν_0が互いに等しく，それらのスペクトルが互いに区別できない場合，それらを重ね合わせてできるスペクトルの広がりは，均一広がりと呼ばれる．均一広がりには，あるエネルギー準位に存在する電子が，他の準位に遷移する時間（自然寿命）における不確定性に起因するものと，原子間の衝突に起因するものがある．これらのスペクトルの広がりの幅はそれぞれ自然幅，衝突幅と呼ばれる．自然幅は，不確定性原理によりその半値全幅（FWHM）$\Delta\nu_N$は次式で表される．

$$\Delta\nu_N = \frac{1}{2\pi\tau} \tag{3-16}$$

ここで，τは電子の自然寿命である．このスペクトルの形状は Fig.3-13 (a)に示すようにローレンツ型であることが知られている．Rb 原子の場合は，励起準位の寿命は $2p_{3/2}$ 準位で 28.1 [ns]であることから，(3-16)式により自然幅は約 6 MHz と求めることができる．一方，衝突幅は，気化した原子の圧力に比例するため，本研究で使用した Rb 原子の封入されたセルの圧力下（約 10^{-6} [Torr]）では，ほとんど無視することができる．

また，各々の原子の持つ共鳴周波数が少しずつ異なる値を持つとき，これらを重ね合わせて得られるスペクトルは自然幅とは形状が異なる．このスペクトルの広がりは，不均一広がりと呼ばれ，その幅は不均一幅と呼ばれる．この不均一広がりの原因のほとんどは，セル内の原子の熱運動による共鳴周波数のドップラーシフトである．今，原子の共鳴周波数をν_0とし，入射光の進行方向に沿った速度成分をvとすると，この原子の共鳴周波数νはドップラー効果によりシフトしる．νは次式で表される．

$$\nu = \nu_0 + kv \tag{3-17}$$

ただし，$k = \nu/c$である．vは一般に正負に分布しているので，スペクトルは全原子の熱運動速度分布の幅により不均一に広がる．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うため, 速度分布がvと$v + dv$の間にある原子数$N(v)dv$は,

$$N(v)dv = \frac{N_0}{\sqrt{\pi}u} \cdot exp\left(-\frac{v^2}{u^2}\right)dv \tag{3-18}$$

となる．ただし，N_0は全原子数，uは最確速度である．この最確速度は速度の大きさ，すなわち，速さの分布が最大となる速さのことをいい，気体の温度を T，原子の質量を M，ボルツマン定数をk_Bとすれば，次式のように表される．

$$u = \sqrt{\frac{2k_BT}{M}} \tag{3-19}$$

ここで，(3-17)式より得られる$v = \nu - \nu_0/k$を(3-18)式に代入すると，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,

$$G(\nu) = \frac{1}{\sqrt{\pi}ku} \cdot exp\left\{-\left(\frac{\nu - \nu_0}{ku}\right)\right\} \tag{3-20}$$

が得られる．このような不均一広がりは，同じ速度成分を持つ原子の自然幅の重ね合わせ

として考えられる．これは Fig.3-13 (b)に示すようにガウス型であり，その半値全幅$\Delta\nu_D$は次式で表される．

$$\Delta\nu_D = \frac{2\sqrt{ln2u}}{c}\cdot\nu_0 = \frac{2}{c}\cdot\sqrt{\frac{2k_BT\cdot ln2}{M}}\cdot\nu_0 \qquad (3\text{-}21)$$

この$\Delta\nu_D$をドップラー幅という．Rb 原子のドップラー幅は常温（300 K）で約 515.5 MHz となる．このように Rb 原子の場合，一般的な条件下では，均一幅に比べドップラー幅の方が非常に広いため Rb 原子の吸収スペクトル幅は，ドップラー幅によって決定されることになる．また，周波数弁別器の周波数特性も，このドップラー幅によって決定される．Fig.3-14 は，実際に観測された Rb 原子の D_2 吸収スペクトルを示している．また，Fig.3-15 はドップラー幅を考慮した Rb 原子の D_2 線の理論吸収スペクトル（吸収係数）を示している．Fig.3-15 に示すように ^{85}Rb の 6 つの吸収線と ^{87}Rb の 6 つの吸収線は，ドップラー幅によって 4 つの吸収スペクトルとして観測されている．この 4 つの吸収曲線の傾斜部分が，周波数弁別器として使用される．

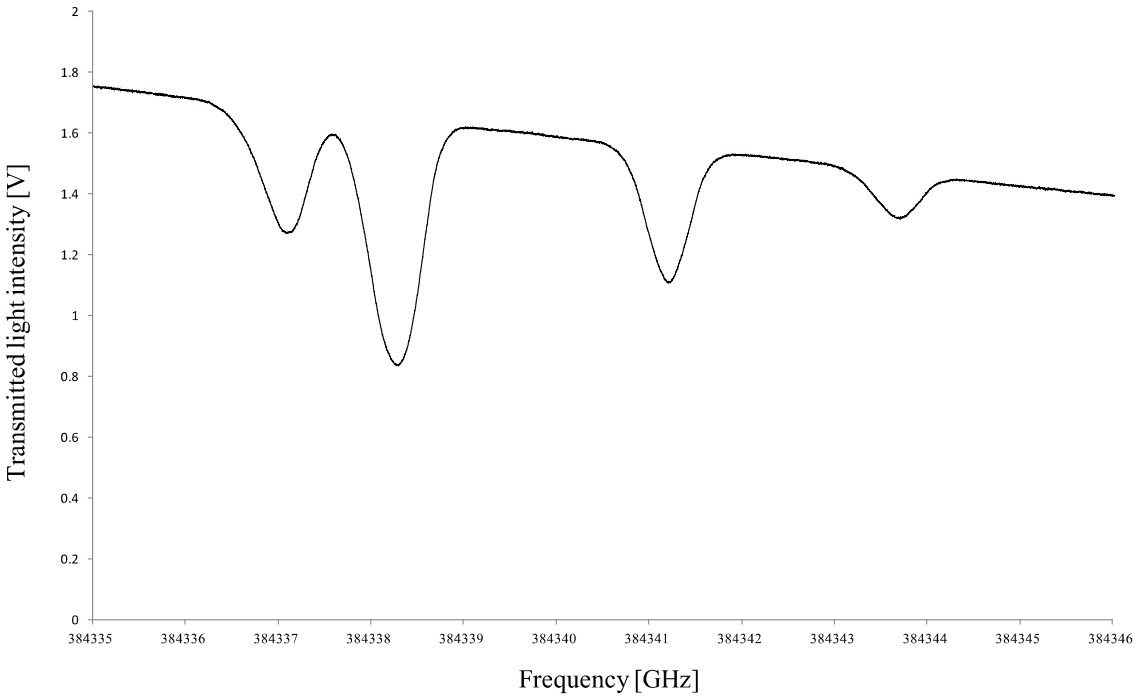


Fig.3-14 Observed profile of the Rb-D2 absorption line.

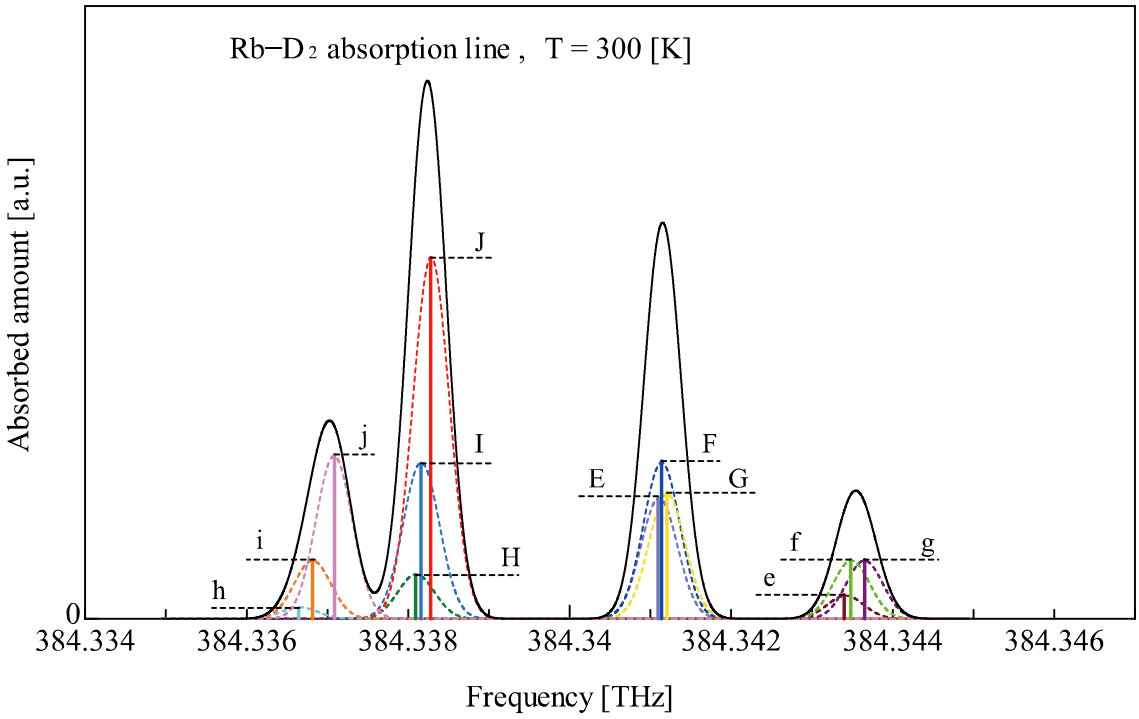


Fig.3-15 Theoretical profile of the Rb-D_2 absorption line.

第 4 章 物理乱数の生成

本研究では半導体レーザの周波数雑音を，物理乱数のソースとして用いることで，物理乱数の高速生成を実現する．本章では，まず物理乱数の生成原理について説明し，続いて乱数の評価方法について説明する．

4.1 物理乱数の生成原理

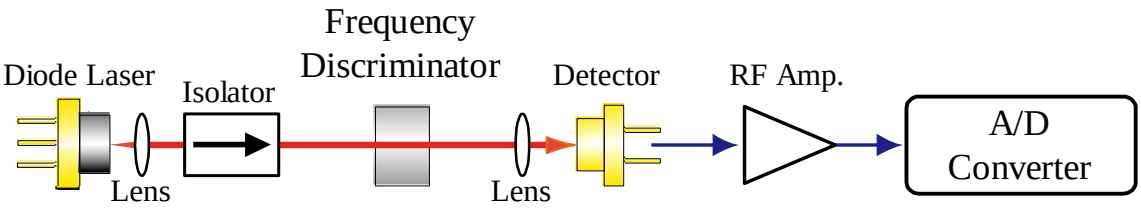


Fig.4-1 DL's frequency-noise detection system using a Frequency Discriminator.

物理乱数の生成原理の概要を以下に示す．

① 半導体レーザの周波数雑音を，Fig.4-1 に示すように周波数弁別器を使って光の強度雑音に変換し，光検出器で電気的なアナログ信号として検出する．

② 検出された電気的雑音信号を，Fig.4-2 に示すようにデジタルオシロスコープの ADC によってデジタル信号，すなわち 2 進数のデータに変換し，取得する．

③ 得られた 2 進数データを使って排他的論理和（XOR：Exclusive-OR）演算を行い，カオス現象に特有のスパイクやバイアスの影響を軽減し，かつ等確率性を確保する．

④ XOR 演算を行った 2 進数データから 2 進数列（物理乱数列）を抽出する．

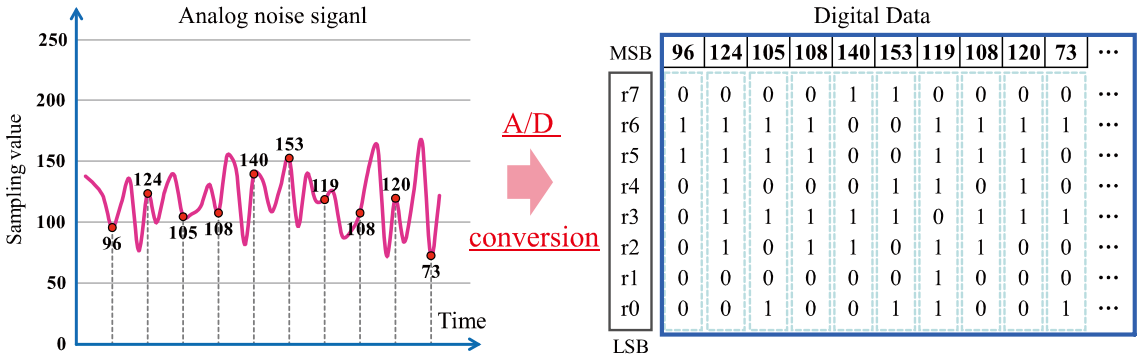


Fig.4-2 Analog-Digital conversion.

以下に物理乱数を生成するための XOR 演算の方法や，2 進数データから 2 進数列（物理乱数列）を生成する方法について具体的に説明する．

4.1.1 物理乱数生成のための排他的論理和演算

2 進数表現した数値の各ビットに対し, 2 を法とした剰余体$\mathbb{Z}/[2]$での加減算を求めた結果を，ビットごとの排他的論理和，排他的ビット和と呼ぶ．このビットごとの排他的論理は，0 を偽，1 を真とみなした論理演算における排他的論理和と考えることができる．Table 4-1 に，その排他的ビット和の真理値表である．

情報理論の分野において，異なる 2 進乱数列同士のビットごとの排他的論理和演算は，2 進乱数列の等確率性を向上させる効果があることがよく知られている．そのため，乱数列の長さが長くなると等確率性を満たすことが難しくなる物理乱数列の欠点を補うために，その生成過程によくビットごとの排他的論理和演算（XOR 演算）が用いられる．この物理乱数列を生成するための XOR 演算は，完全に異なる時間に生成された独立した 2 進数データや時間的に遅延した同一の 2 進数データを用いて行われることが多い．以下に，本研究で使用した A/D コンバータから得られた 2 進数データとその遅延された 2 進数データの間で XOR 演算を行う処理方法について説明する．

Table 4-1 Truth-value of Exclusive-OR.

Proposition A	Proposition B	A⊕B
1（真）	1（真）	0（偽）
1（真）	0（偽）	1（真）
0（偽）	1（真）	1（真）
0（偽）	0（偽）	0（偽）

Fig.4-3 は，垂直分解能 8 ビットの ADC から得られた 2 進数データ（Binary Data）の XOR 操作の方法を示している．ADC の垂直分解能が 8 ビットである場合，Binary Data は，8 桁（1Byte）の 2 進数が, 0～255 の 10 進数字を表している Data として取得される．この Binary Data が，XOR 演算された 2 進数データ（XOR Data）を生成するための源となるもとデータ（Original Data）である．XOR の操作は，この Original Data と Original Data に遅延を施した Delay Data との間で行う． Original Data の遅延は 1Byte 単位で行われ，Delay Data は，遅延を施して減った先頭の Data を遅延によって余った末尾の Data で補うことで生成される．（Data の遅延は，Original Data 上では 1Byte 単位の遅延であるが，2 進数の各桁においては bit 単位の遅延であることに注意する必要がある.）この 2 つの Binary Data の XOR 演算で生成された Binary Data が，物理乱数列を生成するための源となる XOR Data である．物理乱数列は，この XOR Data から 2 進数列を抽出することで生成する．

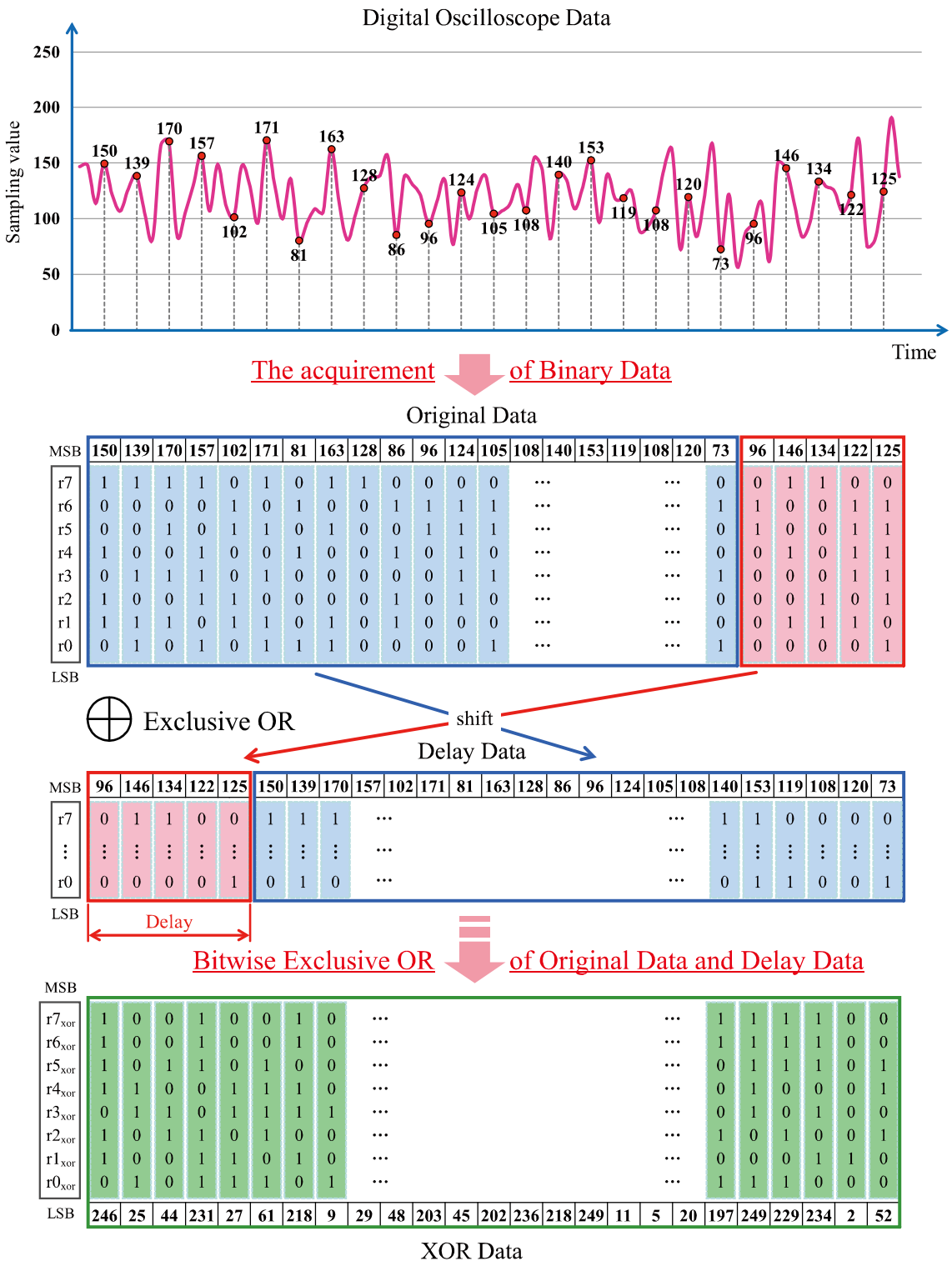


Fig.4-3 Exclusive-OR operation by 8bits binary sequence.

4.1.2 並列生成方式と結合生成方式

XOR Data から物理乱数列を生成する方法について以下に説明する．我々は，本研究において 2 種類の生成方式を使用した．1 つは，Fig.4-4 に示されている XOR Data から複数の乱数列を並列的に生成する方法である．もう 1 つは，Fig.4-5 に示されている XOR Data から 1 つの乱数列を直列的に生成する方法である．これらの生成方式を区別するために我々は，これらの生成方式の特徴から前者を並列生成方式（Parallel generation method），後者を結合生成方式（Coupling generation method）と呼ぶこととした．

前者の並列生成方式は，複数の乱数列を同時に生成する方式である．具体的には，XOR 操作によって得られた 2 進数の最上位ビット（MSB）から最下位ビット（LSB）までの桁ごとにデータを抽出して，それを桁ごとに結合することで桁ごとに乱数列を生成する．この生成方式では，垂直分解能が 8 ビットの ADC を用いた場合，乱数列が同時に 8 つ生成される．乱数の生成速度は，乱数が 8 つ並列に生成されるため ADC のサンプリング速度の 8 倍になる．

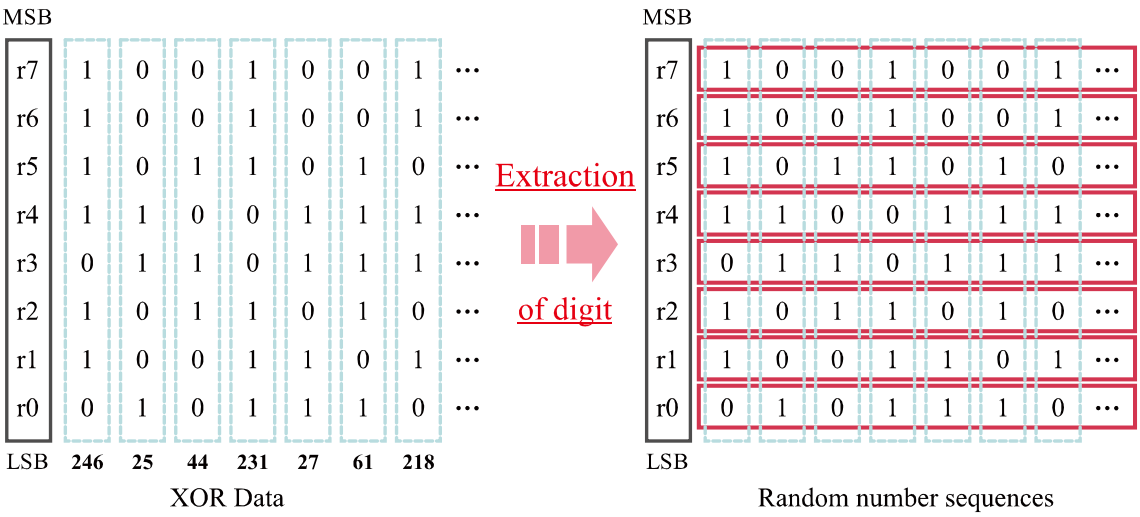


Fig.4-4 The generation of Random number sequence with the parallel generation method.

一方後者の結合生成方式は，各桁のデータを 1 つに繋げて 1 つの長い乱数列を生成する方式である．具体的には，XOR Data から 1 バイトごとにデータを抽出して 2 進数の r0(Least Significant bit)から例えば r0，r1 そして r2 の 3 ビットを結合して 1 つの乱数列を生成する．この乱数列の上位ビットは，r7 から r1 まで選択可能である．（LSB だけから生成される乱数列は，並列生成方式の r0 bit から生成される乱数列と同一であるため結合生成方式において除外する．）Fig.4-5 では，例として r5 までの場合の乱数列の生成の方法が示されている．乱数の生成速度は，選択したビットの数に依存する．垂直分解能 8 ビットの ADC の場合，最大でサンプリング速度の 8 倍の速度で乱数を生成することができる．

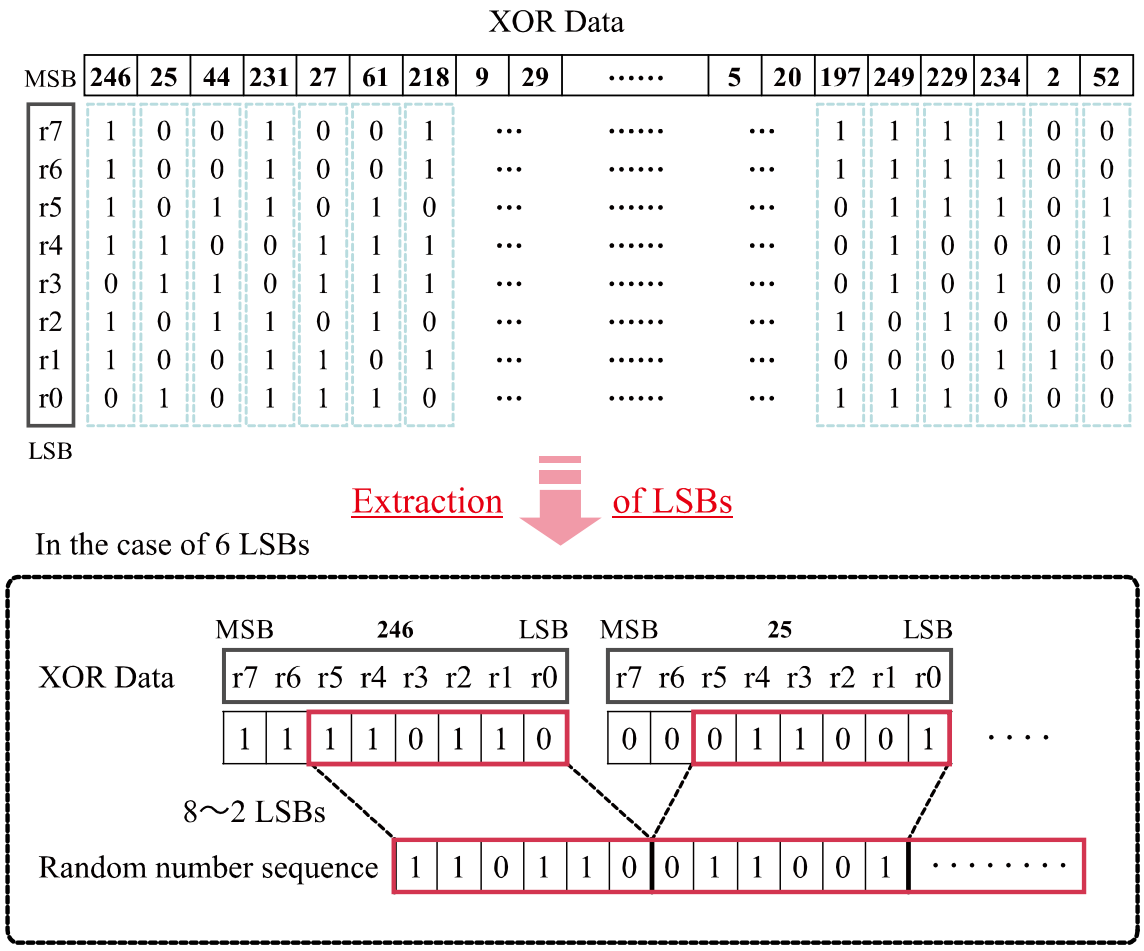


Fig.4-5 The generation of Random number sequence with the coupling generation method.

4.1.3 Reverse XOR 方式

ある振幅雑音が ADC によって 2 進数に変換された時，その振幅雑音に対する感度は，2 進数の各桁によって異なる．具体的には，MSBs に比べ LSBs が，その振幅雑音のより細かな変化に反応する確率が高い．同様に雑音信号が ADC によって 2 進数に変換された場合，LSBs は，その雑音信号のより細かな変化を検出しやすいため，MSBs に比べ複雑な変化をする．この事実は，各桁を使って物理乱数を生成する場合（並列生成方式），上位の桁から生成された乱数の無秩序性が，下位の桁から生成された乱数の無秩序性よりも劣ることを意味する[40]．この問題を解決するために提案された方法が，XOR 操作（Reverse XOR 方式と区別するために，前述した 2 進数列の XOR 操作を XOR 方式と呼ぶこととする．）を更に発展させた Reverse XOR 方式と呼ばれる方法である[41][42]．この方法は，上位の桁と下位の桁の間で XOR 演算を行うことで上位の桁の劣る無秩序性を相殺することができる．

Fig.4-6 に，Reverse XOR 操作の方法が示されている．Reverse XOR 方式は，2 つの独立し

た異なるBinary Dataを必要とする.（時間的に遅延した同一の2進数データは使用できない.）2 つの独立した異なる Binary Data を得るためには，半導体レーザの周波数雑音検出システムから別々の時間に取得された独立した異なるデータを使用する手段と 2 台の独立した周波数雑音検出システムから別々に得られたデータを使用する手段がある．前者の場合，物理乱数の生成速度が，後者と比べて 1/2 になることに注意する必要がある．これらの手段によって得られた 2 つの独立した Binary Data が，Reverse XOR Data を生成するための源となる Original Data1 と Original Data2 である．Reverse XOR の操作は，この Original Data1 と Original Data 2 から生成された Reverse Data との間で XOR の操作を行うことで実現する．Original Data2 から生成される Reverse Data は，Original Data2 の MSBs と LSBs を入れ替えたデータである. この Original Data1 と Reverse Data の 8 桁の 2 進数列の XOR 演算で生成された Binary Data が，物理乱数列を生成するための Reverse XOR Data である．Reverse XOR 方式を用いた物理乱数は，XOR 方式と同様にこの Reverse XOR Data に並列生成方式と結合生成方式を適用して生成する.

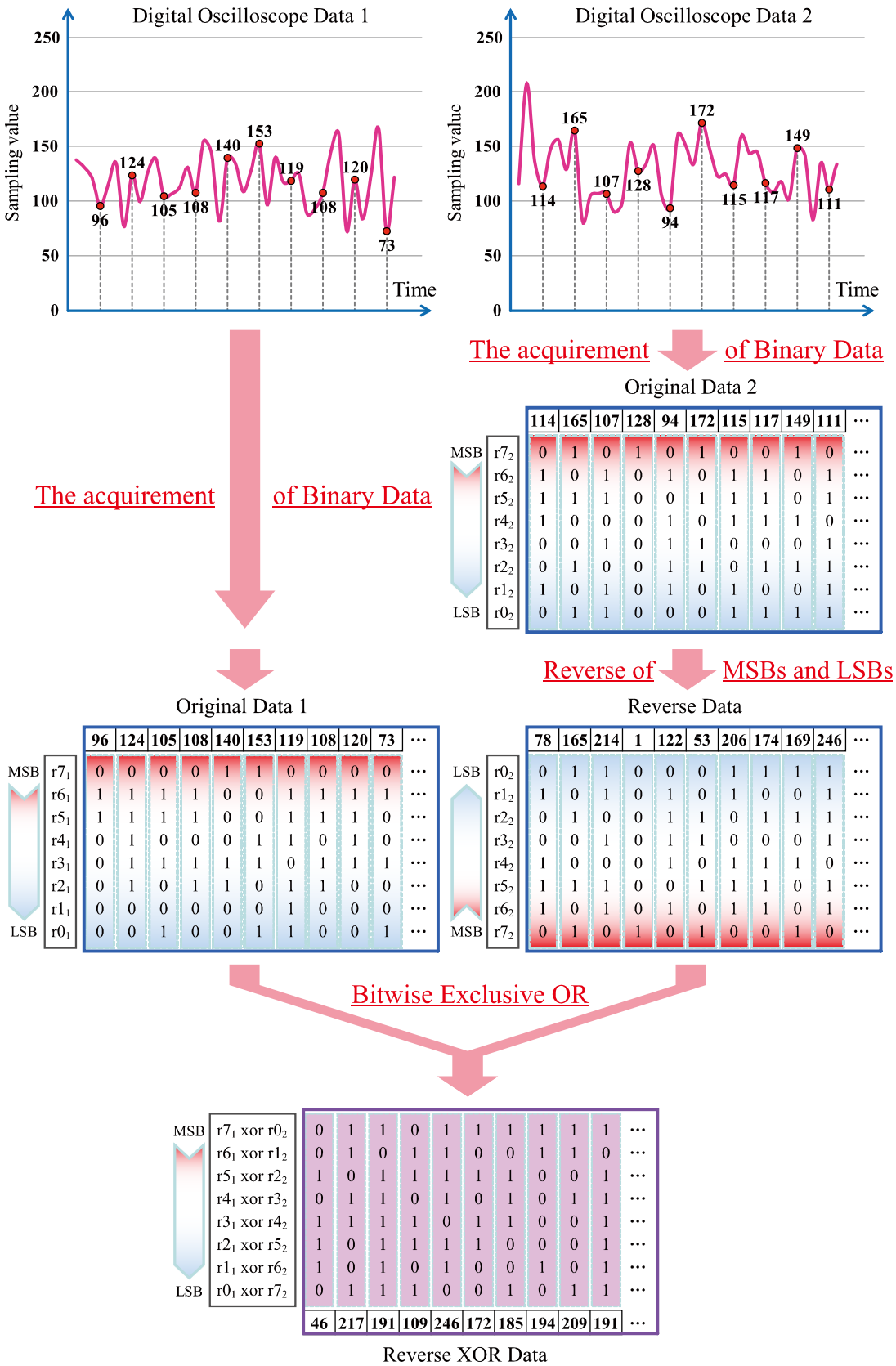


Fig.4-6 Reverse XOR method.

4.2 乱数の評価方法

暗号用乱数のランダム性の評価には，一般的に統計的検定が使用される．代表的な統計的検定には，NIST（National Institute of Standards and Technology）の FIPS 140-2 や SP800-22，ダイハードテストなどがある．特に SP800-22 は，多くの乱数研究においてデファクト・スタンダードとして使用されている．本章では，SP800-22 についての説明と，SP800-22 を使用した乱数の評価方法について説明する．

4.2.1 乱数検定 NIST SP800-22

SP800-22 は，NIST によってハードウェアベースもしくはソフトウェアベースの暗号用物理乱数生成器または疑似乱数生成器によって生成される 2 進数列のランダム性をテストするために開発された統計的検定である．そのテスト内容は，15 種類（サブテストを含めた場合；188 種類）の独立した統計的検定から構成させる．Table 4-2 に，15 種類の各統計的検定の名前と検定概要を示す．

Table 4-2 SP800-22 の全 15 種類の検定項目

No.	統計テスト名	検定概要
1	Frequency	1Mbit 中の 0 と 1 の個数の偏り
2	Block Frequency	256bit ブロック中の 0 と 1 の個数の偏り
3	Cumulative Sums	0/1 を-1/1 に変換して順次加算したときの最大値の偏り
4	Runs	連（1 または 0 の連続）の数の偏り
5	Longest Runs	256bit ブロック中の最長連の長さの偏り
6	Rank	bit 列を 32×32bit の行列で表現したときの回数の偏り
7	Discrete Fourier Transform	離散フーリエ変換後のピーク高さが閾値を超える数の偏り
8	Non-overlapping Template	任意の 9bit パタンの出現回数の偏り
9	Overlapping Template	9bit がすべて 1 のパタンの出現回数の偏り
10	Universal	任意の 7bit パタンの出現回数の偏り
11	Approximate Entropy	11/10bit で取りうるパタンのマッチ数の偏り
12	Random Excursions	0/1 を-1/1 に変換して順次加算したときの（-4～4）の出現回数の偏り
13	Random Excursions Variant	0/1 を-1/1 に変換して順次加算したときの（-9～9）の出現回数の偏り
14	Serial	16/15/14bit で取りうるパタンのマッチ数の偏り
15	Linear Complexity	5000bit 毎の数列の線形複雑度の偏り

15 種類の各統計的検定は，すべて「テストされる 2 進数列が，完全な乱数である」という仮説を帰無仮説としている．各統計的検定では，統計量 *P-value* が計算される．統計量 *P-value* は，「完璧な乱数生成器が，テストされる数列よりもランダムでない数列を生成する確率」である[16]．SP800-22 では，統計量 *P-value* を評価する有意水準αを，1%（$\alpha = 0.01$）に設定している．よって各統計的検定で *P-value*$\geq \alpha$である場合，各統計的検定の帰無仮説が棄却されず，ターゲットの 2 進数列のランダム性が認められる．

一度の SP800-22 の検定を実行するためには，複数の 2 進数列（SP800-22 のターゲットとなる数列は，1,000 bit 以上の長さの 2 進数列です.）がテストされる必要がある．そして，それぞれの 2 進数列ごとに各統計的検定の結果が得られる．SP800-22 の合否は，各統計的検定の合格率と各統計的検定の *P-value* の分布の均一性をそれぞれ統計的検定によって評価することで決定される．各統計的検定の合格率は，二項検定によって評価され，各統計的検定の *P-value* の分布の均一性は，x^2-検定によって評価される．SP800-22 の合格は，個々の統計的検定が，この 2 つの統計的検定を同時に合格する時に認められる．これら 2 つの統計的検定は，それぞれ Proportion test，　P-value_T test と呼ばれる．

・Proportion test

Proportion test は，全 188 種類の統計的検定を合格した 2 進数列の割合（Proportion）を二項検定によって評価する．Proportion の許容範囲は，以下に定義される信頼区間によって決定される．

$$\hat{p} \pm 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}} \tag{4-1}$$

$\hat{p} = 1 - \alpha$，m は，それぞれ各統計的検定の信頼水準とテストされる 2 進数列の数を示している．この信頼区間は，2 項分布の近似値として正規分布を使用して計算したものである．また，この区間は Proportion の標準分布の 3 倍と一致する．2 進数列の数が m = 1,000 である場合，Proportion の範囲（Fig.4-7 参照）は，(4-1)から以下のように求まる．

$$\hat{p} \pm 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}} = 0.99 \pm 3\sqrt{\frac{0.99(0.01)}{1000}} = 0.99 \pm 0.0094392 \tag{4-2}$$

この条件を満たした場合，検定サンプルにランダム性が認められる．

・**P-value$_T$ test**

P-value$_T$ test は，各統計的検定の *P-value* の分布の均一性を，x^2-検定によって評価する．x^2-検定は，「各々の統計的検定から得られる *m* 個の *P-value* が，0 と 1 の間の 10 の部分区間（Fig.4-8 参照）に一様に分布する」という帰無仮説を証明するために行う．計算の方法は，以下の通りである．

$$x^2 = \sum_{i=1}^{10} \frac{((F_i - m)/10)^2}{m/10} \qquad (4\text{-}3)$$

ここで，*Fi* は 0 と 1 の間の 10 の部分区間のうちの 1 つの *P-value* の数である．
そして、*P-value$_T$* は，

$$P\text{-}value_T = igamc(9/2, x^2/2) \qquad (4\text{-}4)$$

と計算される．ここで，*igamc* は不完全なガンマ関数である．*P-value$_T$* は，有意水準 0.01% によって評価される．

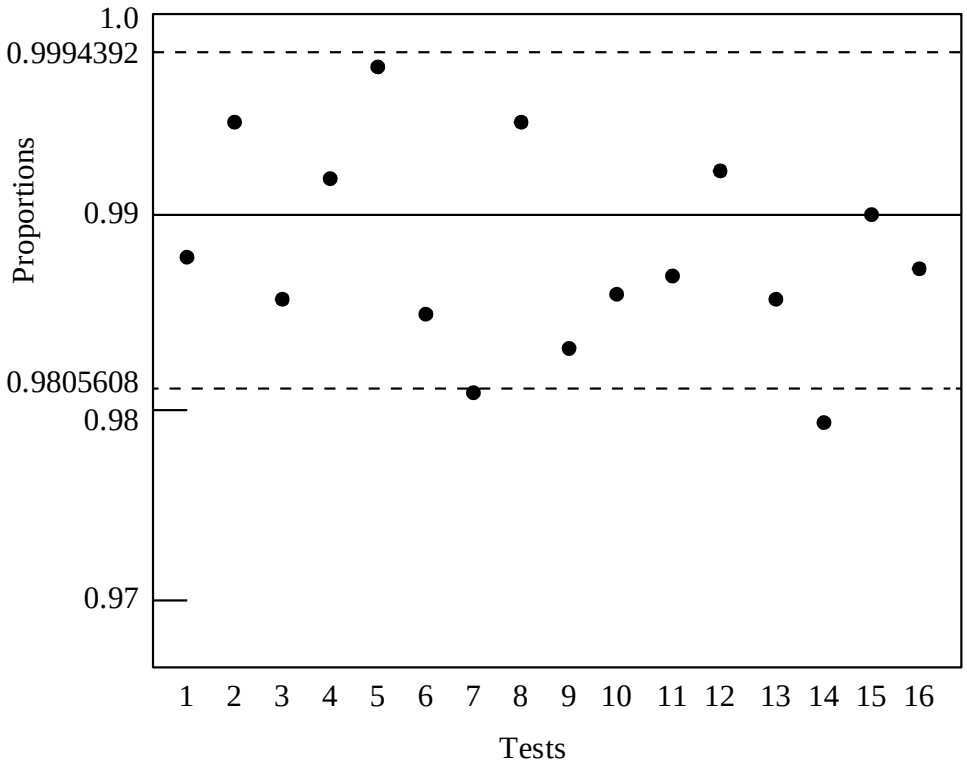


Fig.4-7 P-value Plot

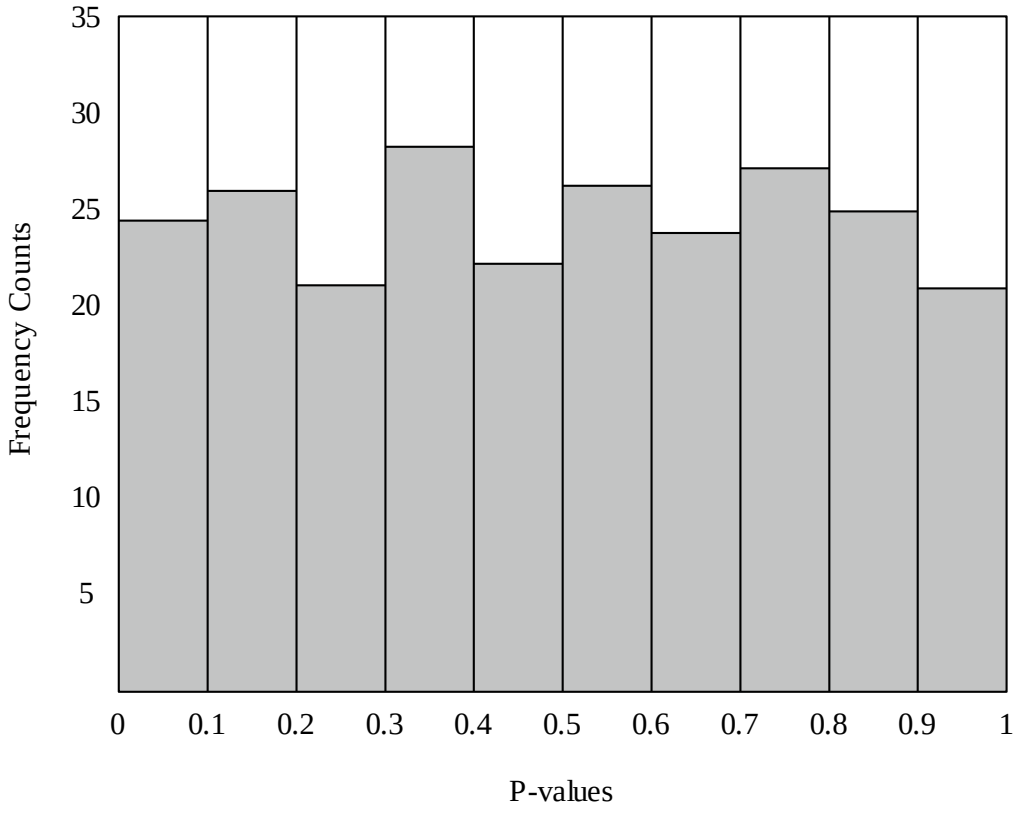


Fig.4-8 Histogram of P-values

SP800-22は，これらの統計的検定のどちらか一方でも失敗する場合には，現象が統計的な例外なのか，非ランダム性のはっきりとした証拠であるのかどうか決定するために異なるサンプルを使って更なる実験を行う必要がある．

4.2.2 乱数検定合格率の評価

SP800-22 によって生成された物理乱数のランダム性を評価するためには，SP800-22 を複数回行い，その検定合格率を二項検定によって評価する必要がある．二項検定には，真の乱数の SP800-22 の検定合格率を基に算出された二項分布が用いられる．真性乱数の SP800-22 の合格率の理論値は，山口によって計算されており[43]，個々の統計的検定の合格率は，それぞれ 99.656880% （m = 1,000）である．よって SP800-22 全体の検定合格率は，$0.99656880^{188} = 0.52404652$より, およそ 52%になる. また, Discrete Fourier Transform (DFT) Test の理論的欠陥[44][45]を考慮し, DFT Test を除外した場合, SP800-22 全体の検定合格率は，$0.99656880^{187} = 0.52585082$より，およそ 53%になる．

本研究では，DFT Test を除外して SP800-22 を実行する．二項検定の帰無仮説は,「生成された乱数列が真の乱数である」ということである．二項分布 $B(n, p)$の場合，検定統計量は，

$$z = \frac{X - np}{\sqrt{np(1-p)}} \tag{4-5}$$

として得られる．X は検定に合格した回数（確率変数），p は乱数列が SP800-22 を合格する確率（0.52585082），n は検定回数（試行回数）である．二項分布は，正規分布によって近似される．したがって検定統計量 z は，標準正規分布 $N(0,1)$に従う．有意水準を$\alpha = 0.01$とした場合，棄却域は，標準正規分布の-2.57 以下と 2.57 以上の領域である．検定回数が n=100 であるとき，検定統計量 z が棄却域の中に入る場合の確率変数 X の条件は，$0 \leq X \leq 39$（$-10.53 \leq z \leq -2.72$）と$66 \leq X \leq 100$（$2.69 \leq z \leq 9.50$）である．これらの範囲で帰無仮説が棄却されるため統計学的に有意でない検定合格率の範囲（信頼区間）は，$40 \leq X \leq 65$である．乱数列の検定合格数がこの信頼区間の中に入るとき，その乱数列が，高い品質の乱数列であると判断できる．

第 5 章 半導体レーザの発振周波数制御とその評価法

本研究では，半導体レーザの周波数雑音を安定的に検出するために，半導体レーザの発振周波数を制御する必要がある．周波数雑音を検出するための半導体レーザの発振周波数は，Phase-locked-Loop（PLL）の技術を用いて制御し，周波数弁別器である Rb 原子吸収曲線のスロープの周波数に安定化する．また，PLL 制御に使用する周波数参照となる半導体レーザの発振周波数は，Rb 原子の偏光信号を偏差信号に用いて，Rb 原子吸収線（超微細構造）の波長に安定化する．

本章では，先ず偏光信号を用いた半導体レーザの発振周波数制御の原理について説明し，続いて PLL 技術を用いた周波数シンセサイザの原理について説明する．それから，発振周波数の安定度の評価法について述べる．

5.1 半導体レーザの発振周波数制御の原理

現在，半導体レーザは光通信，光記録、光計測などの分野で光源として広く用いられている．しかし動作特性上，注入電流や温度により発振周波数が変化するため，高コヒーレンスを必要とする応用分野では発振周波数の安定化が必要不可欠である．そのため長年に渡り，原子または分子の共鳴スペクトル線やファブリペロー共振器などの周波数参照に半導体レーザの発振周波数をロックすることで，半導体レーザの発振周波数を安定化する多くの技術が開発された[46][47]．原子・分子吸収線やファブリペロー共振器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検出する研究[30][31][32]も，これらの派生研究として研究されてきた側面を持つ．よって半導体レーザから周波数雑音を安定かつ持続的に検出するためには，これらの安定化技術を利用することが有効である．

我々は，PLL 制御のための周波数基準となる半導体レーザの発振周波数を安定化するために，その中から Rb 原子吸収線の偏光信号[48][49][50]を制御信号に用いた無変調安定化方式を採用した．この方式は，光学系以外に必要な装置が減算回路のみであるため安定化システムの小型化が非常に容易であるというメリットがある．また他の方式で必要な，半導体レーザの注入電流への直接変調が必要ないため，半導体レーザの周波数雑音に周期信号が重畳されないメリットがある．特に後者のメリットは，半導体レーザの周波数雑音を物理乱数の生成に利用する場合に，生成される乱数の品質に関わってくるため非常に重要である．

本節では，まず 5.1.1～5.1.3 項で PID 制御について述べ，5.1.4 項で実験に使用した光検出器について述る．また 5.1.5 項と 5.1.6 項で Rb 吸収線の偏光分光信号について述べ，最後に 5.1.7 項で PLL を用いた半導体レーザの発振周波数の制御方法について述べる．

5.1.1 比例・積分・微分制御[51][52]

本研究では偏光分光で得られた零クロス点を持つ電気信号（偏差信号）をレーザの駆動電流源（レーザドライバ）にフィードバックすることで駆動電流を調整し，発振周波数の中心周波数の制御を図っている．我々は目標となる周波数と実際のレーザの発振周波数の差（偏差あるいは制御偏差）をなくすために，制御対称の数学モデルに頼らない現物ベースの制御技術である PID 制御を利用する．我々の PID 制御は，偏差信号を PID 調節器に入力し，出力された操作信号をレーザの駆動電流に加算することで実現する．その PID 制御による制御系の基本形を Fig.5-1 に示す．

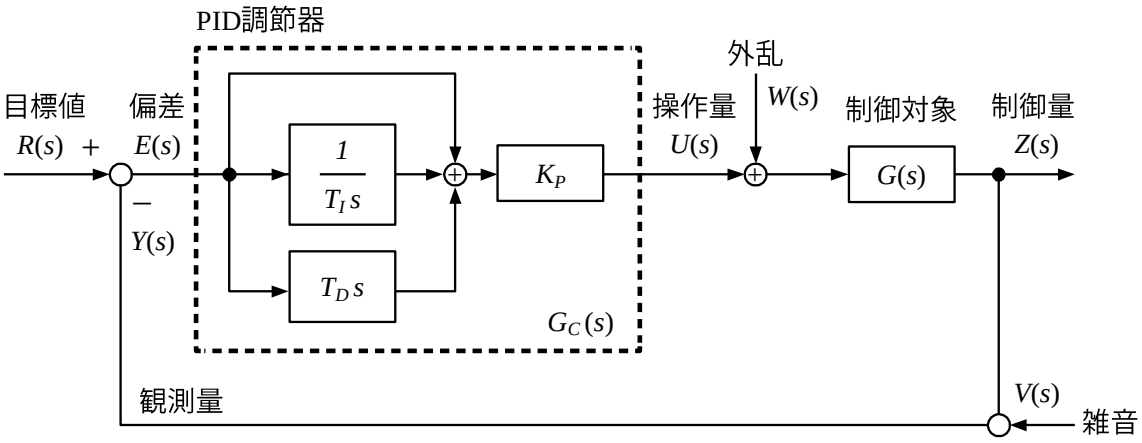


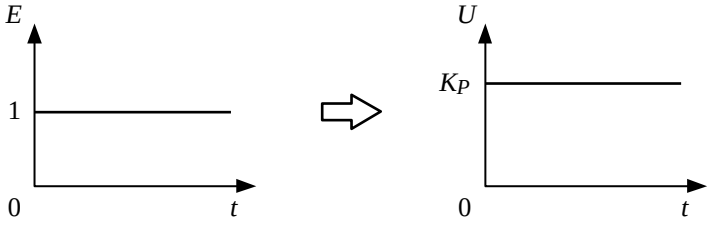
Fig.5-1 Basic PID control system.

Fig.5-1 に示された制御系は，制御量，操作量，外乱がそれぞれ一つずつのスカラー制御系である．簡単のため外乱は，操作量に加算される形で制御対象に加わるとし，雑音を除いた観測量と制御量は同じものであるとしている．目標値から観測量を引いたものが，偏差である．PID 調節器は，PID 制御を実行する制御装置（制御回路）である．

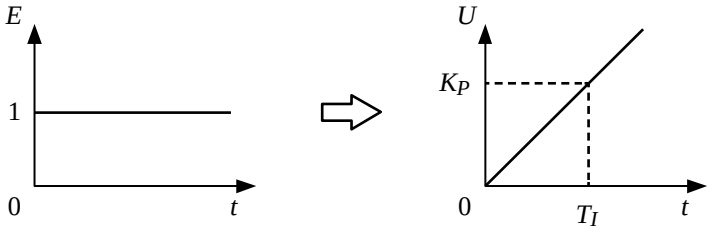
PID 調整器には 3 つの制御動作が存在し，各動作は，比例動作（Proportional（P）動作），積分動作（Integral（I）動作），及び微分動作（Derivative（D）動作）である．それぞれの動作の役割は次のようになる．

- **比例動作**：偏差を小さくする．
- **積分動作**：定常偏差またはオフセット（制御対象に比例制御のみを行うと，目標値や外乱のステップ状態変化に対して最終的に残る一定の偏差）を零にする．リセット（reset）動作とも呼ばれる．
- **微分動作**：偏差の増減（時間変化率）を小さくする．また一種の予見動作である．レート（rate）動作とも呼ばれる．

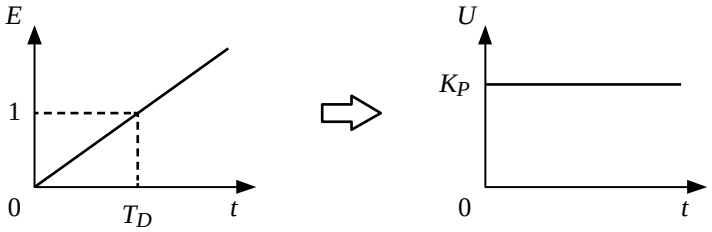
Fig.5-2 に，比例，積分，微分動作の入力と出力の関係を示す．



(a) Proportional action



(b) Integral action



(c) Derivative control action

Fig.5-2 Proportional, Integral, and Derivative control action.

この PID 制御の操作量を決定する式は，操作量をU，偏差をEとすると

$$U(t) = K_P E(t) + K_I \int_0^t E(\tau)\, d\tau + K_D \frac{dE(t)}{dt} \qquad (5\text{-}1)$$

となる．K_P，K_I，K_Dは比例係数である．また慣習により(5-1)を以下のように表現することが多い.

$$U(t) = K_P \left\{ E(t) + \frac{1}{T_I} \int_0^t E(\tau) d\tau + T_D \frac{dE(t)}{dt} \right\} \qquad (5\text{-}2)$$

$(K_I \equiv K_P/T_I,\ K_D \equiv K_P T_D)$

(5-2)式から PID 調節器の伝達関数$G_c(s)$は,

$$G_c(s) = K_p\left(1 + \frac{1}{T_I s} + T_D s\right) \tag{5-3}$$

と求まる．K_Pは比例ゲイン，T_Iは積分時間，T_Dは微分時間である．Fig.5-2 から分かるように，比例ゲインは比例動作における偏差と操作量の比である．積分時間は，同じステップ状の入力に対する比例動作と積分動作の出力が等しくなるまでの時間である．微分時間は同じランプ（直線）状の入力に対する比例動作と微分動作の出力が等しくなるまでの時間である．PID 制御の制御系の設計には，これら比例ゲイン，積分時間，微分時間の 3 つのパラメータの最適な値を決定することが必要である．

5.1.2 PID 制御の調整法[51][52][53]

PID 制御の調整，すなわち比例ゲイン，積分時間，微分時間の適切な値を選ぶための方法が PID 制御の調整法である．ここでは，そのパラメータを決定するための初期設定値の決め方について述べる．実際の PID 制御ではこの初期設定を再調整して制御が行われる．

この PID 制御器の初期パラメータを決定する代表的な方法に, Ziegler と Nichols によって提案された限界感度法と過度応答法（ステップ応答法）がある．以下にそれらを説明する．

1) 限界感度法

限界感度法は，閉ループの応答特性に基づいて初期設定を決定する代表的な方法である．比例制御だけで制御を行い，比例ゲインを徐々に大きくしていくと，目標値あるいは外乱のステップ状変化に対する制御量の応答はしだいに振動的になり，ついには安定限界を超えて発振状態となる．この発振状態となる比例ゲインと，その発振信号の振動周期から PID の制御パラメータを決定する方法が限界感度法である．Table 5-1 に限界感度法による制御パラメータの決め方を示す．発振状態となる比例ゲインをK_c，発振信号の振動周期をT_cとすれば, 調節器の各パラメータは, Table 5-1 に示されているように決められる. これらは Ziegler と Nichols が実験例を通じて決定したものである．

Table 5-1 限界感度法による制御パラメータの決め方

	比例ゲイン	積分時間	微分時間
P 調節器	$0.5K_c$		
PI 調節器	$0.45K_c$	$0.833T_c$	
PID 調節器	$0.6K_c$	$0.5T_c$	$0.125T_c$

限界感度法には，いくつかの問題点がある．1 つは制御系を一旦安定限界まで持っていく必要があるため，制御系が完成している必要があること（PID 調節器の実装前にパラメータを

決定することができない.)，また操作量に飽和があると比例ゲインを大きくしても正確に安定限界を求めることができないことなどである.

2) ステップ応答法 過度応答法

ステップ応答法は，開ループの応答特性に基づいて初期設定を決定する代表的な方法である．フィードバック制御を行わず開ループの状態で，制御対象に単位ステップ関数状の入力を加えて，制御対象のステップ応答を求める．Fig.5-3 に制御対象への単位ステップ応答の入力と制御対象からのステップ応答の出力が示されている．多くの制御対象では，ステップ応答は，Fig.5-3 (b)のような曲線（シグモイド型曲線）となる．この曲線の勾配が最も急なところに接線を引き，その勾配を R とする．またステップ応答の入力された時刻からこの接線が横軸（時間軸）と交わる時刻までの時間を L とする．ステップ応答法は，この R，L から調節器の初期設定を決定する．Table 5-2 にその決定法を示す.

なお，限界感度法およびステップ応答法のどちらの方法で制御パラメータを決定したとしても，出来上がった制御系は目標値のステップ変化に対する応答に 25%程度のオーバーシュートが生じる．制御対象によっては問題になる場合もあるため制御対象ごとに微調整をする必要がある.

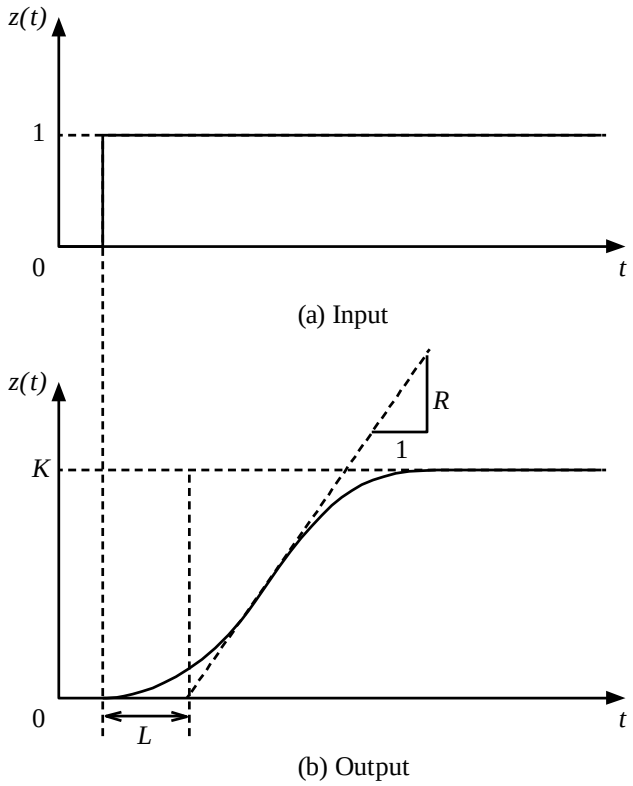


Fig.5-3 Step response waveform.

Table 5-2 ステップ応答法による制御パラメータの決め方

	比例ゲイン	積分時間	微分時間
P 調節器	$1/RL$		
PI 調節器	$0.9/RL$	$3.33L$	
PID 調節器	$1.2/RL$	$2L$	$0.5L$

5.1.3 PID 制御回路[51][54]

本研究では PID 調節器を，オペアンプを用いた簡単な電子回路で構築する．PID 制御回路は，オペアンプを用いた反転増幅回路，積分回路，微分回路，加算回路の 4 種類のオペアンプ回路を組み合わせることで簡単に構築することができる．Fig.5-4 にその PID 制御回路の例を示す．また PID 制御回路について説明する．

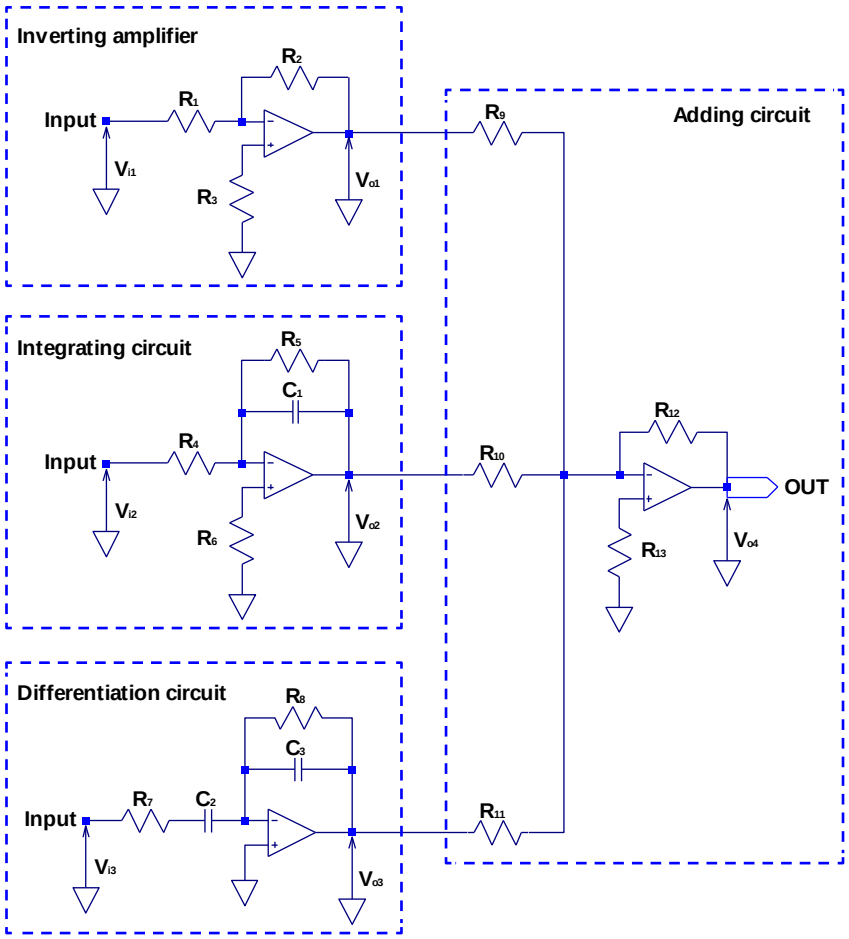


Fig.5-4 PID circuit.

PID 制御回路では，入力信号はそれぞれ反転増幅回路，積分回路，微分回路に入力され，それらの出力信号が加算回路で加算される．反転増幅回路，積分回路，微分回路，加算回路の出力電圧は，それぞれ

$$V_{o1} = -\frac{R_2}{R_1}V_{i1} \tag{5-4}$$

$$V_{o2} = -\frac{1}{C_1R_4}\int V_{i2}dt$$

$$V_{o4} = -R_{12}\left(\frac{V_{o1}}{R_9} + \frac{V_{o2}}{R_{10}} + \frac{V_{o3}}{R_{11}}\right) \tag{5-7}$$

となる．PID 制御回路では，$R_1 = R_2$とし反転増幅回路のゲインは 1 倍とする．また加算回路のゲインは，各入力電圧V_{o1}，V_{o2}，V_{o3}に対して一定にするため$R_9 = R_{10} = R_{11}$とする．式(5-4)，(5-5)，(5-6)，(5-7)より PID 制御回路の出力電圧V_{out}は，反転増幅回路，積分回路，微分回路の入力電圧が$V_{in} = V_{i1} = V_{i2} = V_{i3}$であるならば，

$$\begin{aligned} V_{out} &= -R_{12}\left\{\frac{1}{R_9}\left(-\frac{R_2}{R_1}V_{in}\right) + \frac{1}{R_{10}}\left(-\frac{1}{C_1R_4}\int V_{in}dt\right) + \frac{1}{R_{11}}\left(-C_2R_8\frac{dV_{in}}{dt}\right)\right\} \\ &= -\frac{R_{12}}{R_9}\left(-V_{in} - \frac{1}{C_1R_4}\int V_{in}dt - C_2R_8\frac{dV_{in}}{dt}\right) \\ &= \frac{R_{12}}{R_9}\left(V_{in} + \frac{1}{C_1R_4}\int V_{in}dt + C_2R_8\frac{dV_{in}}{dt}\right) \end{aligned} \tag{5-8}$$

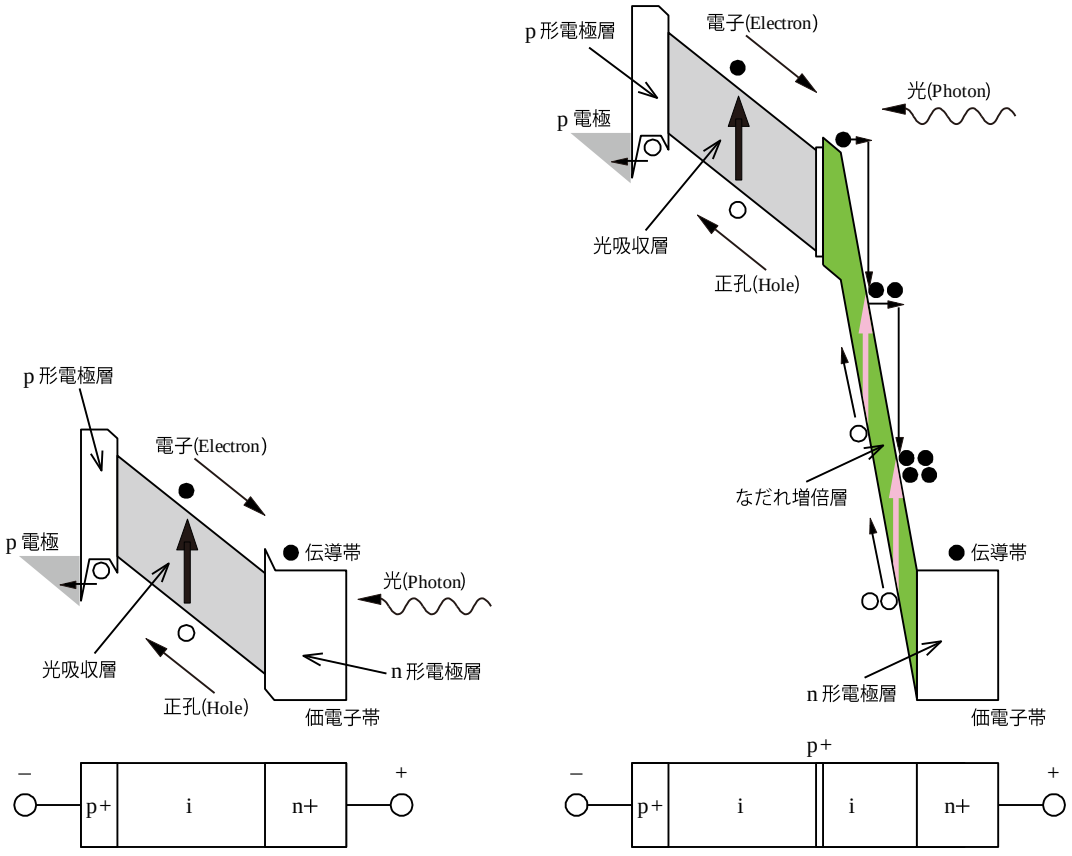
となる．この式と式(5-2)を比較するとわかるように，PID 制御回路における比例ゲイン，積分時間，微分時間は，それぞれ$K_P = R_{12}/R_9$，$T_I = C_1R_4$，$T_D = C_2R_8$となる．

5.1.4 アバランシェフォトダイオード[17][55]

民生機器や光通信などにおいては，小型で信頼性が高く経済的な，半導体接合型素子（光起電力型素子）の光検出器が多用されている．光起電力型素子は，キャリヤ励起によって発生する電流や電位を信号として取り出すものであり，代表例であるフォトダイオード(PD)はさまざまな分野で用いられている．以下にフォトダイオードの一種であるアバランシェダイオード（Avalanche photodiode：APD）について説明する．

内部光電効果型光検出器の代表的なものは，pin 接合型フォトダイオード(pin-PD)である．この pin-PD の感度（信号対雑音比）を向上させるため素子に利得を持たせたのが APD である．Fig.5-5(a)，(b)にそれぞれ pin-PD と APD のバンド図と層構成を示す．Fig.5-5(a)に示す

ように，pin-PD はアンドープの光吸収層を p 形および n 形の半導体層（電極層）ではさんだ構造をしている．動作時には pin 接合を逆バイアスし，空乏化した光吸収層に高電界を印加しておくと，光信号の入力により光吸収層で発生した電子･正孔対が，電界によりそれぞれの電極に掃引され電流として取り出される．一方 APD は，Fig.5-5(b)に示すように，空乏層内に高電界が印加された増倍層を設けている．増倍層中では，加速された高エネルギーのキャリヤが格子原子と衝突して 2 次的な電子-正孔対を生成する「衝突イオン化」が生じる．そして生成されたキャリヤは再び電界に掃引されイオン化を起こすという現象を繰り返すことで，キャリヤ数がなだれ的に増大し，光電流を増幅する．



(a) Pin photo diode　　(b) Avalanche photo diode

Fig.5-5 Band diagram and layer structure.

APD の出力から入射光パワーを計算する方法を説明する．Fig.5-6 に実験に使用する APD を用いた光検出回路を示す．

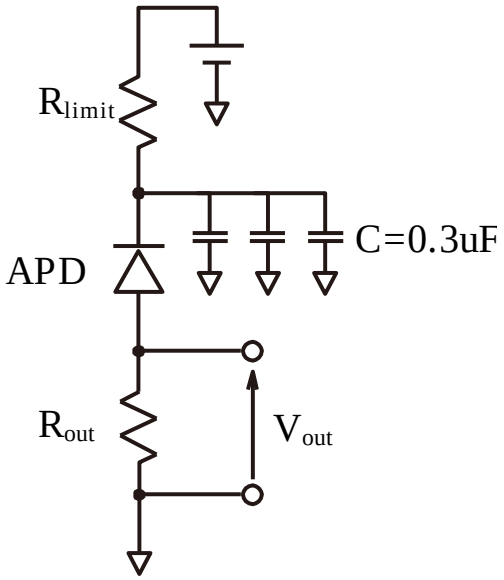


Fig.5-6 Light detect circuit.

APD を電流I_{APD}を出力する電流源と見なし，出力端子に接続する機器の入力インピーダンスが無限大であると仮定する．APD 回路出力電圧がV_{out}[V]のとき，終端抵抗R_{out}[Ω]に流れる電流は，APD の暗電流を無視すると，

$$I_{APD} = \frac{V_{out}}{R_{out}}[\mathrm{A}] \tag{5-9}$$

となる．バイアス電圧をV_{bias}[V]とし，電流制限抵抗をR_{limit}としたとき APD の両端電圧V_{APD}[V]は，

$$V_{APD} = V_{bias} - I_{APD}(R_{limit} + R_{out}) = V_{bias} - \frac{V_{out}}{R_{out}}(R_{limit} + R_{out})[\mathrm{V}] \tag{5-10}$$

となる．実験に使用した APD は，入力光の波長が 800nm 付近において，バイアス電圧が 100[V]以下である場合，増倍率 M が，実測値から，

$$M \cong 10^{\frac{V_{APD}}{80}} \tag{5-11}$$

と仮定できる．APD の入射光パワーは，分光感度をCとおくと，

$$P_{input} = \frac{I_{APD}}{C} = \frac{2I_{APD}}{M} = \frac{2V_{out}}{R_{out}\left(10^{\frac{V_{APD}}{80}}\right)}$$

$$= \frac{2V_{out}}{R_{out}\left[10^{\frac{\left\{V_{bias}-\frac{V_{out}}{R_{out}}(R_{limit}+R_{out})\right\}}{80}}\right]} [\mathrm{W}] \qquad (5\text{-}12)$$

となる．実験に使用した APD の分光感度 C は，$C = M/2$である．以上より，APD 回路出力電圧V_{out}と回路パラメータから，入射光パワー[W]を求めることができる．式(5-12)より計算した，APD の出力電圧特性を以下の Fig.5-7 に示す．計算の条件は，バイアス電圧 $V_{bias} = 90[V]$，出力電圧$V_{out} = 10\mathrm{k}[\Omega]$，電流制限抵抗$R_{limit} = 10\mathrm{k}[\Omega]$である．

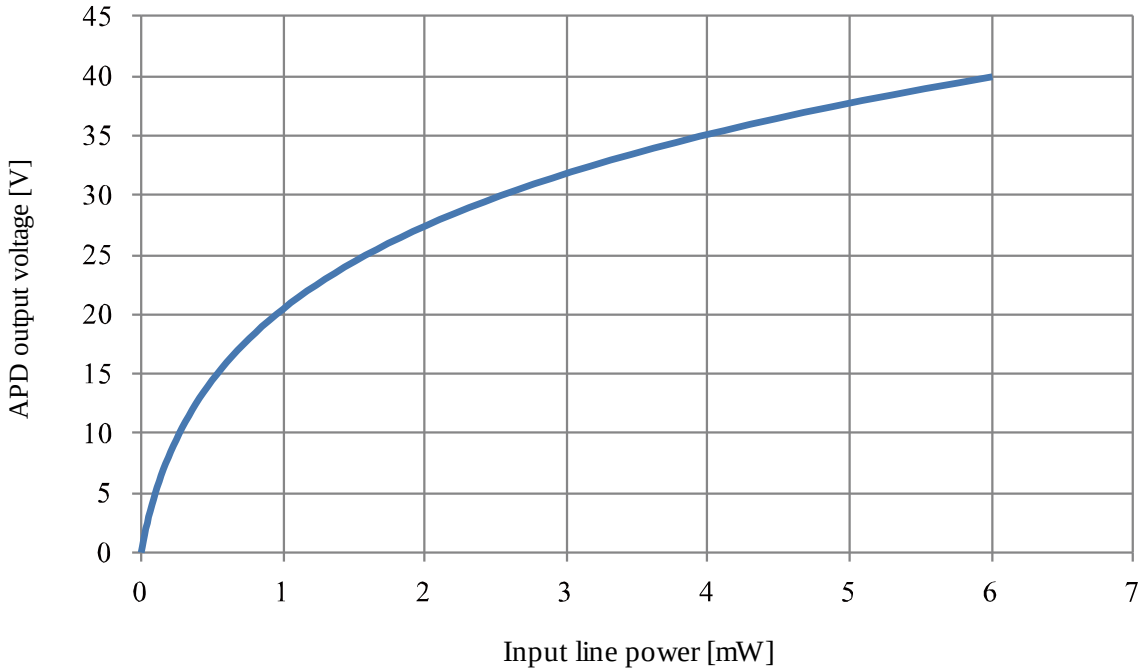


Fig.5-7 APD output voltage characteristic.

5.1.5 飽和吸収分光[17][56]

赤外・可視域のレーザを用いた原子や分子のレーザ分光において分解能の上限を決めるのは，前々章で述べたスペクト線のドップラー幅である．その影響を軽減することができる方法に，吸収の飽和効果を用いた飽和吸収分光法がある．飽和効果とは，電磁波が強く原子の吸収が盛んに起こると，緩和が追いつかなくなり，エネルギー準位の上下で原子数が同じ程度になることで誘導吸収と誘導放出が釣り合って正味の吸収がゼロに近づく現象

である．飽和吸収分光では，ある速度成分を持つ原子群によるスペクトル（ホール）を観測することができ，ドップラー幅より遥かに狭い幅の吸収スペクトルを得ることができる．Fig.5-8 にそのための基本的な光学系を示す．

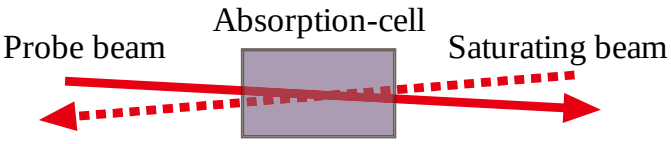
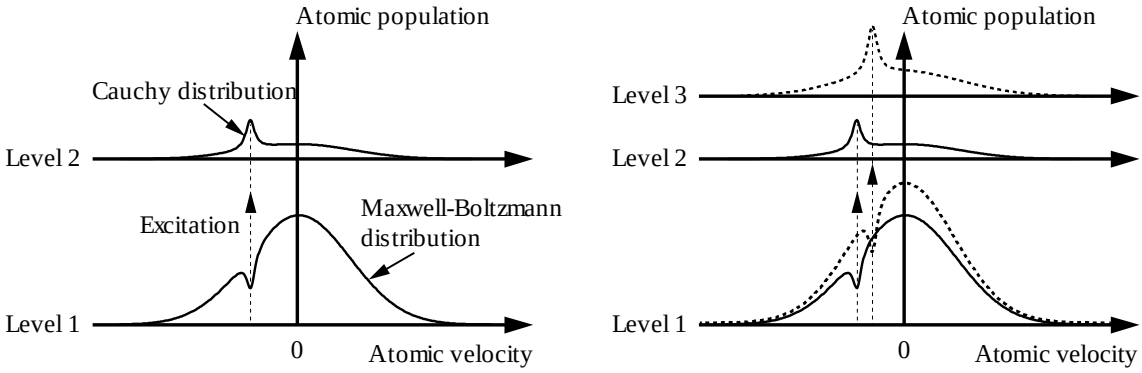


Fig.5-8 Fundamental optical setup for the saturated absorption spectroscopy.

飽和吸収分光の光学系は，検出光（Probe beam)と飽和光（Saturating beam）を逆向きに吸収セル（Absorption cell）に入射し，その光軸が吸収セル内で一致するようにする．このときある同じ速度成分を持つ原子群が，飽和光と検出光で同時に励起されることで飽和効果が起こり，Fig.5-9 に示すようにドップラーシフトによる速度分布の中にローレンツ形の穴（ホール）ができる．この現象はホールバーニングと呼ばれる．以下に入射光の周波数とホールの現れる位置の関係について説明する．



(a) Two-level system　　(b) Three-level system

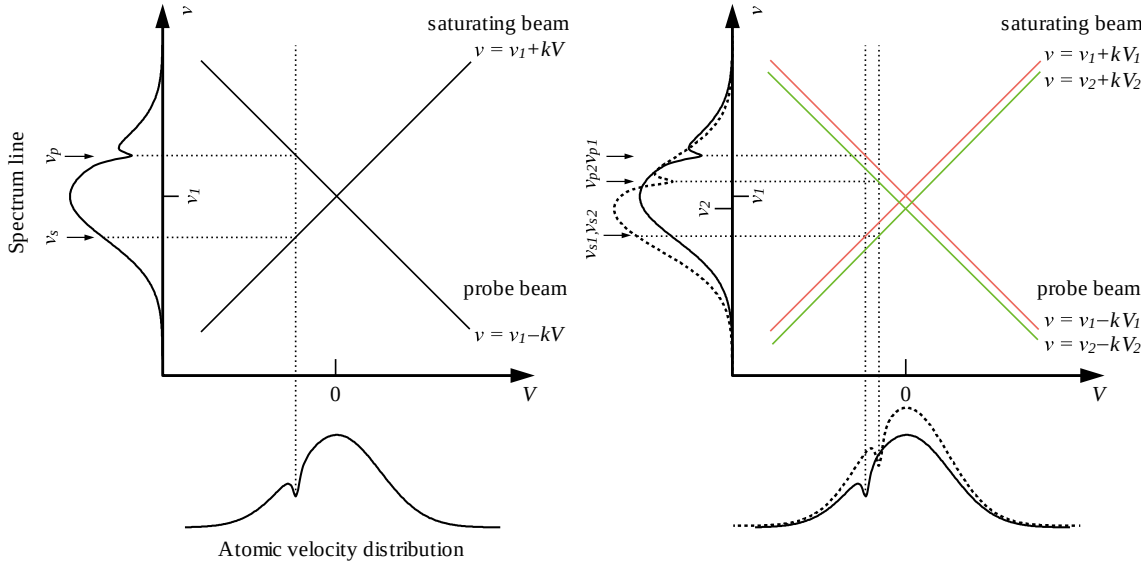
Fig.5-9 Energy level and velocity distribution of atoms.

簡単のためまず 2 準位系について考える．進行方向を正として，ある速度成分 V を持つ原子群が，飽和光と検出光によって励起される場合，飽和光と検出光の周波数は，それぞれ$\nu_1 + kV$，$\nu_1 - kV$と表すことができる．ただしν_1は吸収スペクトルの中心周波数，kは波数である．($k = \nu/c = 1/\lambda$で表される．νは入射光の発振周波数, λは吸収線の波長である．) Fig.5-10 はそのときの入射光の周波数とホールのできる位置の関係を示している．飽和光と検出光の周波数をν_s，ν_pとしたとき，Fig.5-10 (a)から分かるように飽和光と検出光の周波数が，吸収スペクトルの中心に対して対象の周波数であるときホールが観測される．これは飽和光と検出光が，吸収セルに対して逆向きに入射されているため，ドップラーシフトが

両入射光で逆向きになるためである．この関係は Fig.5-10 (b)より 3 準位系でも同じであることが分かる．3 準位系では，ドップラー幅の中に重なった 2 つのスペクトル線が存在するが，Fig.5-10 (b)のように鋭いホールによってスペクトルが分離されて観測される．ただし，2 つのホールの間隔は，2 つのスペクトル線の中心の間隔の 2 倍となる．すなわち，

$$\nu_{p1} - \nu_{p2} = 2(\nu_1 - \nu_2) \qquad (5\text{-}13)$$

の関係が成り立つ．ν_{p1}，ν_{p2}は 2 つのホールが検出される位置での検出光の周波数である．またν_1，ν_2は 2 つの吸収スペクトルの中心周波数である．このようにしてホールを観測する飽和吸収分光は，他の方法と区別してホールバーニング分光と呼ばれる場合がある．



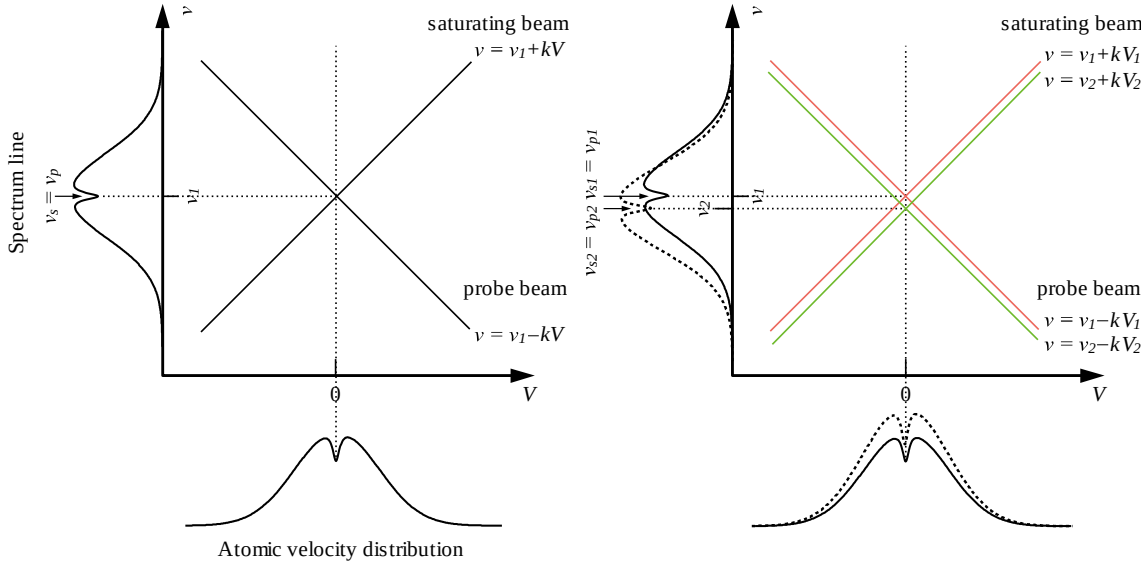
(a) Two-level system　　(b) Three-level system

Fig.5-10 Relations between input beams frequencies and positions of holes for the hole-burning spectroscopy.

ホールバーニング分光では，飽和光と検出光を同一のレーザ光源から作る必要はないが，敢えて同一のレーザ光源から飽和光と検出光を作ることもできる．この場合，逆方向に進む飽和光および検出光の周波数ν_sとν_pに，$\nu_s = \nu_p$の関係が成り立つためレーザ光源の発振周波数を吸収スペクトル付近で掃引していくと，Fig.5-11 に示すようにホールが丁度吸収スペクトルの中心の位置で観測される．このような飽和吸収分光は，特にラムくぼみ分光と呼ばれる．ラムくぼみ分光では，飽和光と検出光の周波数が一致しているためホールが観測される位置が，直線$\nu = \nu_1 + kV$（saturating beam）と$\nu = \nu_1 - kV$（probe beam）の交点と一致する（Fig.5-11 (a)）．また 3 準位系の場合も同様で，2 つのホールが観測される位置が，そ

れぞれ直線$\nu = \nu_1 + kV_1$（saturating beam）と$\nu = \nu_1 - kV_1$（probe beam）の交点の位置と直線$\nu = \nu_2 + kV_2$ (saturating beam) と$\nu = \nu_2 - kV_2$ (probe beam) の交点の位置に一致する (Fig.5-11 (b))．

3 準位系では，さらに直線$\nu = \nu_1 + kV_1$と$\nu = \nu_2 - kV_2$，直線$\nu = \nu_2 + kV_2$と$\nu = \nu_1 - kV_1$にそれぞれ交点が存在し，その位置でもホールが観測される．この現象はクロスオーバー共鳴と呼ばれる．クロスオーバー共鳴は，2 つの吸収スペクトルの速度分布が重なっているとき，飽和光と検出光が別々の吸収スペクトルにおけるある速度成分を持つ原子群を同一の周波数で同時に励起することで起こる．Fig.5-12 はクロスオーバー共鳴における入射光とホールの関係を示している．Fig.5-12 から分かるようにクロスオーバー共鳴の現れる位置は，2 つの吸収スペクトルの中心周波数ν_1とν_2の中間の位置である．



(a) Two-level system　　(b) Three-level system

Fig.5-11 Relations between input beams frequencies and positions of holes for the Lamb dip spectroscopy.

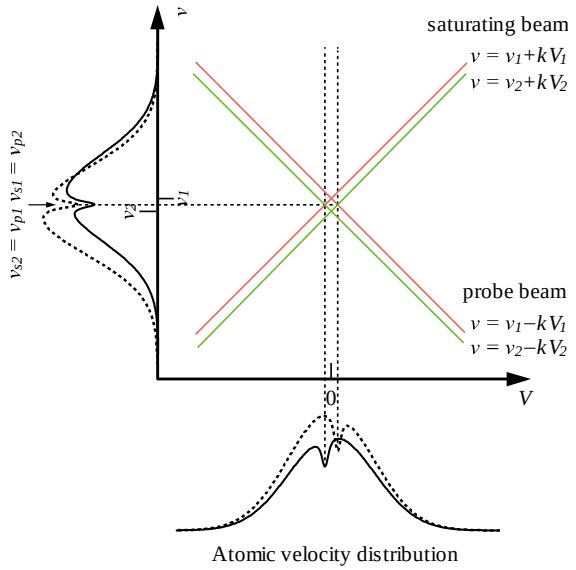


Fig.5-12 Relations between input beams frequencies and positions of holes for the cross over resonance.

実際のラムくぼみ分光のための光学系は，Fig.5-13 に示すように 1 つの半導体レーザ（Laser diode）から放出されたレーザ光を，ビームスプリッタ（Beam splitter）やハーフミラーなどを用いて飽和光と検出光に分け，その 2 つのレーザ光を吸収セルに対して互いに反対方向から光軸を一致させるように入射することで構築する．またより大きなラムくぼみを観測するために，テクニックとして 1/2 波長板と偏光ビームスプリッタ（Polarized beam splitter）によって飽和光の光強度を検出光より大きくなるように調整する．

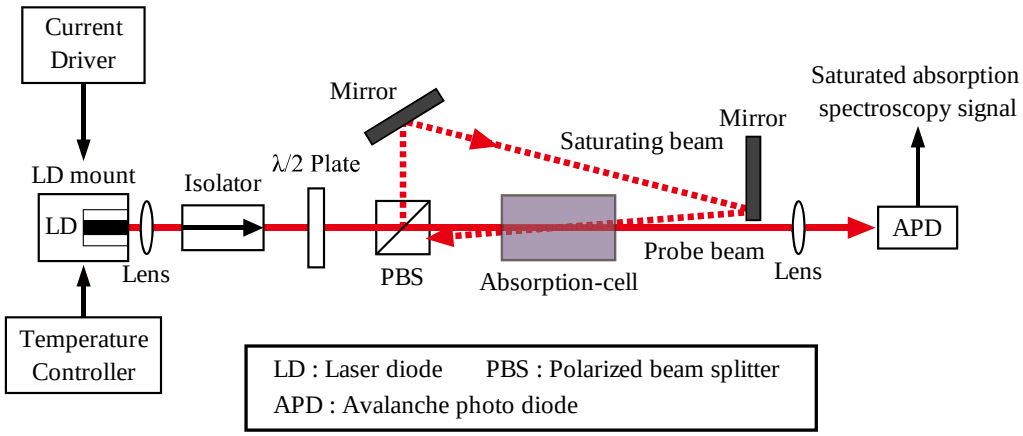


Fig.5-13 Optical setup of Saturated absorption spectroscopy.

Fig.5-13 の光学系を使用して実際に Rb 原子の D_2 吸収線を観測した結果が Fig.5-14 である．Rb-D_2 吸収線の場合 4 準位系であるため，1 つの谷に 3 つのラムくぼみと 3 つのクロスオー

バ共鳴が現れる．しかし Fig.5-14 から分かるようにこれらの位置は非常に近接しているため実際には区別することができず，100MHz 程度の幅を持つくぼみとして観測される．

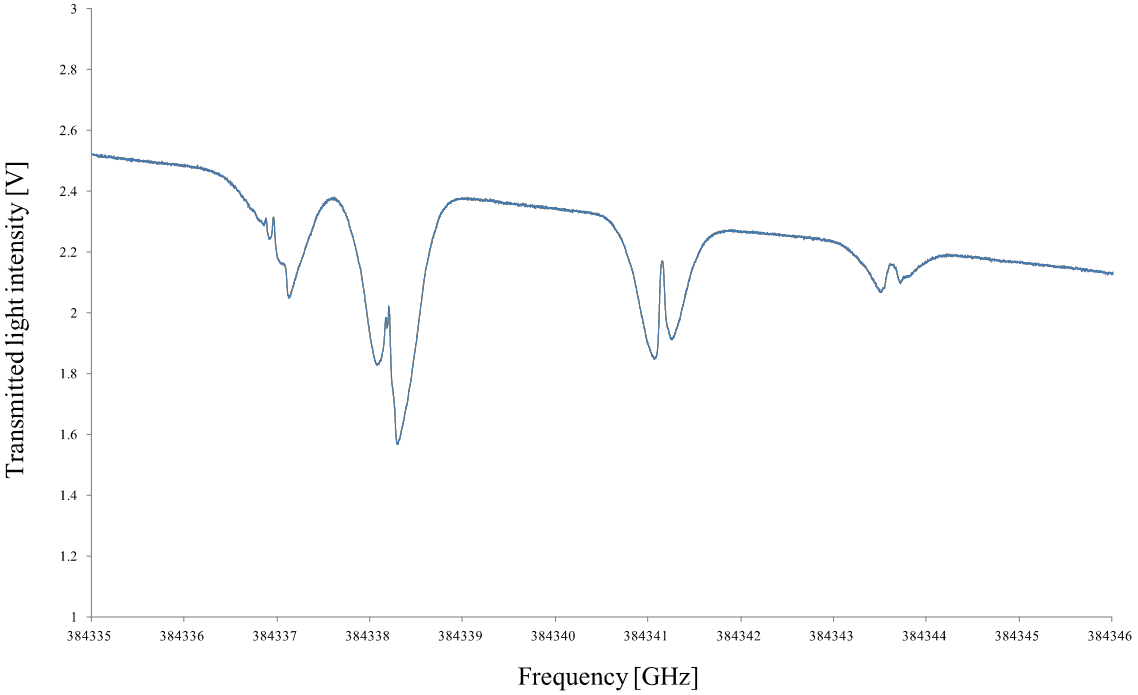


Fig.5-14 Observed profile of the Rb-D_2 absorption line using the saturated absorption spectroscopy.

5.1.6 偏光分光[50]

本研究では，基準レーザ（半導体レーザ）の発振周波数を安定化するために，Rb原子吸収線の偏光分光信号を偏差信号に利用する．ここではRb原子吸収線の偏光分光信号を得るための方法を説明する．Fig.5-15は，偏光信号を得るための光学系である．

ここで紹介する偏光信号を得る方法は，従来の方法より大きな偏光信号を得られる方法である．純粋な偏光信号を得るための従来の方法は，分析される媒質を含んでいるセルの前と後ろのそれぞれの検出光（probe beam）を，方向が交差した偏光子に通し，検出光の信号を光検出器で検出することで，偏光信号を観測する．このときポンプ光（pump beam）の存在は，検出光の偏光面が微小な角度Φだけ回転する原因になり，光検出器で角度Φに対応した透過強度が検出される．その時の透過強度は，マリュスの法則から

$$I = I_0 cos^2\Phi \cong I_0\Phi^2 \qquad (5\text{-}14)$$

と予測することができる．

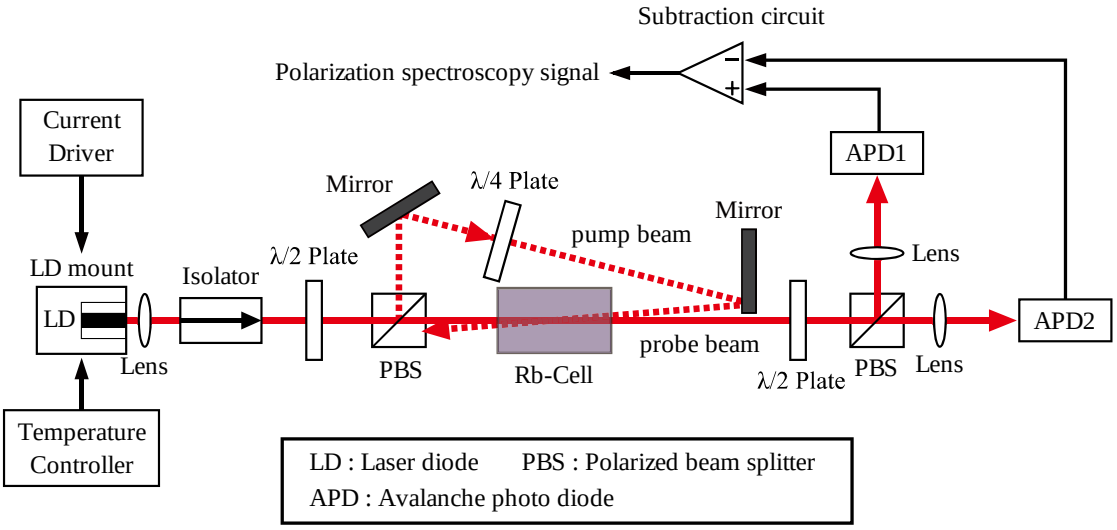


Fig.5-15 Optical setup of Polarization spectroscopy.

我々がここで使用する方法は，Fig.5-15に示すように偏光ビームスプリッタ（PBS）を使用する．この方法ではPBSに対してプローブ光の偏光面が，$\pi/4$傾いている必要がある．ポンプ光がない場合，PBSの一方の光強度は，

$$I_x = I_0 cos^2 \pi/4 = I_0/2 \tag{5-15}$$

となる．また，もう一方の光強度は，

$$I_y = I_0 sin^2 \pi/4 = I_0/2 \tag{5-16}$$

となる．これらを引くと信号はゼロとなる．一方ポンプ光が存在するときは，プローブ光の偏光面の微小角度Φの回転は，信号$I_y - I_x = 2I_0\Phi$の結果につながる．

ここで，2つの方法から得られる振幅の式と偏光信号の外形の式を導き出す．まず，プローブ光の進む方向をz軸と定める．そしてx軸に関して角度φの傾きを持つ面の直線偏光を

$$E = \begin{bmatrix} E_x \\ E_y \end{bmatrix} = E_0 \begin{bmatrix} cos\varphi \\ sin\varphi \end{bmatrix} \tag{5-17}$$

とする．また円偏光の基底ベクトルに関して式(5-17)を以下のように書き換える．

$$E = E_0 \begin{bmatrix} cos\varphi \\ sin\varphi \end{bmatrix} = E_0 \left\{ \frac{e^{-i\varphi}}{2} \begin{bmatrix} 1 \\ i \end{bmatrix} + \frac{e^{i\varphi}}{2} \begin{bmatrix} 1 \\ -i \end{bmatrix} \right\} \tag{5-18}$$

長さLのセルを通って伝搬する際に，ビームはガスセルの窓によって示差吸収と分散の影響を受ける．そのセルの窓の複屈折は，製造プロセスや窓の外と中での圧力勾配に起因して起きる．よってセルを通過した後のプローブ光の電界は，以下のように表せる．

$$E = E_0\left\{\frac{e^{-i\varphi}}{2}\begin{bmatrix}1\\ i\end{bmatrix}e^{-ik_+L}e^{-\alpha_+L/2}e^{-ik_{\omega+}l} + \frac{e^{i\varphi}}{2}\begin{bmatrix}1\\ -i\end{bmatrix}e^{-ik_-L}e^{-\alpha_-L/2}e^{-ik_{\omega-}l}\right\} \quad (5\text{-}19)$$

ここで，$k_\pm = \frac{\omega}{c}n_\pm$ ；$n_\pm$は，$\sigma^\pm$遷移を引き起こす円偏光成分におけるガスの屈折率である．$\alpha_\pm$は付随する吸収係数である．そして$k_{\omega\pm} = \frac{\omega}{c}n_{\omega\pm}$の項は，幅$l$の窓を横切ることによっておこる位相変化を示す．窓の屈折率は複雑であるため，それらは以下のように表される．

$$n_{\omega\pm}l = b_{R\pm} - i\frac{c}{\omega}b_{I\pm} \quad (5\text{-}20)$$

また，以下のようにこの表現を書き直す．

$$E = E_0 exp\left\{-i\left[\frac{\omega}{c}(cL + b_R) - ib_I - i\frac{\alpha L}{2}\right]\right\}\left\{\frac{e^{-i\varphi}}{2}\begin{bmatrix}1\\ i\end{bmatrix}e^{+i\Omega} + \frac{e^{i\varphi}}{2}\begin{bmatrix}1\\ -i\end{bmatrix}e^{-i\Omega}\right\} \quad (5\text{-}21)$$

ここで，

$$\Omega = \frac{\omega}{2c}(\Delta nL + \Delta b_R) - i\left(\frac{L}{4}\Delta\alpha + \frac{1}{2}\Delta b_I\right) \quad (5\text{-}22)$$

また，$n = \frac{1}{2}(n_+ + n_-)$，$\alpha = \frac{1}{2}(\alpha_+ + \alpha_-)$，$b_R = \frac{1}{2}(b_{R+} + b_{R-})$，$b_I = \frac{1}{2}(b_{I+} + b_{I-})$，$\Delta n = n_+ - n_-$，$\Delta\alpha = \alpha_+ - \alpha_-$，$\Delta b_R = b_{R+} - b_{R-}$，$\Delta b_I = b_{I+} - b_{I-}$である．プローブ光はビームスプリッタによって水平$x$成分と垂直$y$成分に分解され，2つの成分の光強度$I \propto |E|^2$の違いは，以下に示す偏光分光信号を与える．

$$I_{signal} = I_y - I_x$$
$$I_{signal} = I_0 e^{-\alpha L - 2b_I} cos\left(2\varphi + L\Delta n\frac{\omega}{c} + \Delta b_R\frac{\omega}{c}\right) \quad (5\text{-}23)$$

I_0は，セルのない時のプローブ光の強度である．ここで，これらの結果を単純化するために近似モデルを作る．セルの複屈折率は，一般的に非常に小さく，また異方性の媒質によって誘発される偏光の回転角度$\Phi = 2\pi(n_+ - n_-)L/\lambda$も非常に小さい．レーザ周波数が単一共

振器を横切ることで解析されると仮定する．吸収のスペクトルの外形は，以下に示すように（大きく広げられた）ローレンツ分布である．

$$\Delta\alpha = \frac{\Delta\alpha_0}{1+x^2} \tag{5-24}$$

$\Delta\alpha_0$は線の中心における吸収の最大差である．また$x = (\omega_0 - \omega)/(\Gamma/2)$は，線幅$\Gamma$の半分で規格化し見積もられた周波数差である．吸収係数の変化は，媒質の屈折率の変化に付随する変化である．吸収係数と屈折率はKramers-Kronigの分散関係によって以下のような関係がある．

$$\Delta n = \frac{c}{\omega_0}\Delta\alpha_0 \frac{x}{1+x^2} \tag{5-25}$$

少ない媒質によって誘発される偏光の角度回転の場合，$\varphi = \pi/4$のとき，式(5-24)の信号は最大になる．ここで式(5-23)を近似すると信号は以下のように表せる．

$$I_{signal} = -I_0 e^{-\alpha L - 2b_I}\left(L\Delta\alpha_0 \frac{x}{1+x^2} + \Delta b_R \frac{\omega}{c}\right) \tag{5-26}$$

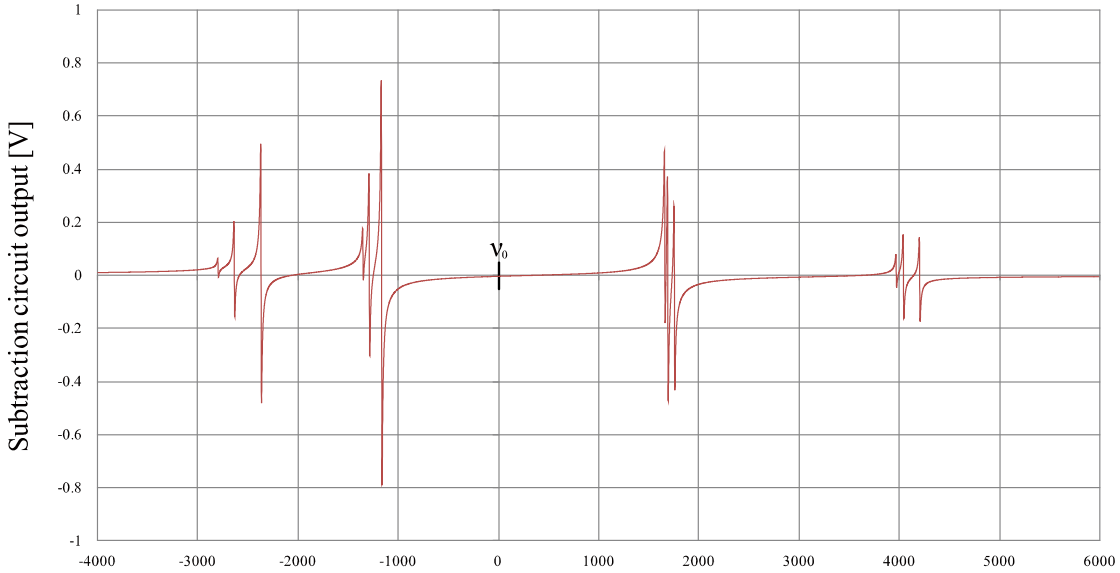
すなわち，サブドップラー線幅の微分係数によって形づくられる分散信号を得ることができる．これは，最大強度が得られる$\varphi = \pi/4$を中心に広範囲の角度において正確である．このテクニックは，背景雑音の少ない，分散による分布曲線を生じさせる．そしてその偏光スペクトルはレーザの周波数をロックするのに理想的である．PBSの軸のどちらかにプローブ光がほぼ一致している状態，すなわち角度φがゼロもしくは$\pi/2$付近であるとき，検出される信号は，

$$1 - \frac{1}{2}\left(L\Delta\alpha_0 \frac{x}{1+x^2}\right)^2 \tag{5-27}$$

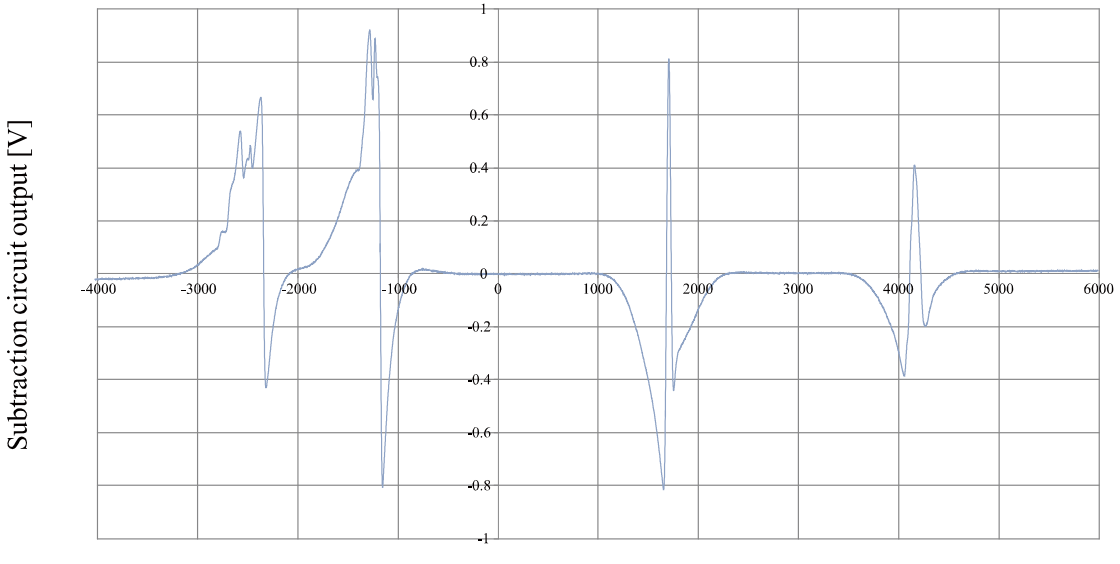
の形になる．こうした状況下で，偏角が非常に小さく検出される信号は，線幅が広い従来の吸収の波形になる．

Fig.5-16に$Rb\text{-}D_2$吸収線の偏光スペクトルの理論的な外形と実測された外形を示す. 偏光スペクトルは，$Rb\text{-}D_2$吸収線の場合，12本の吸収スペクトルが存在するため，Fig.5-16 (a)に示すように波長780.02nm近傍にその微分係数によって形づくられる分散信号が得られる．この分散信号は，各吸収スペクトルのピークの位置にゼロクロス点を持つため，半導体レー

ザの発振周波数を安定化するための偏差信号として使用することができる．一方実際に観測された偏光スペクトルの外形は，Fig.5-16 (b)から分かるように各スペクトルの分散信号がしっかり分解されず，安定化に使用できるゼロクロス点が6点だけである．これは$Rb\text{-}D_2$吸収線の場合12本ある吸収スペクトルが隣接している上，5.1.6節で説明したクロスオーバー共鳴が偏光スペクトルに影響して正確な観測を困難にしているためである．



(a) Theoretical profile



(b) Measured profile

Fig.5-16 Profile of $Rb\text{-}D_2$ polarization spectrum.

偏光スペクトルの理論外形は，式(5-26)から光強度を計算し，その結果を式(5-12)によってAPDの出力信号に変換して算出した．理論計算に使用したパラメータは，Table 5-3（各吸収スペクトルの名前は，Fig.3-を参照）に示す．計算を簡単にするため$b_I = \Delta b_R = 0$とし，セルの窓の複屈折の影響は無視した．また計算に必要な各吸収スペクトルの吸収係数αは，Fig.5-15の光学系から得た実測値から理論モデルを作った．吸収係数αは，APD1，APD2から検出された$\sigma^{\pm}$遷移を引き起こされた吸収スペクトの実測値からα_+，α_-を求めて，$\alpha = \frac{1}{2}(\alpha_+ + \alpha_-)$の関係から算出した．Fig.5-17は，その$\sigma^{\pm}$遷移を引き起こされた吸収スペクトの実測結果である．図から分かるように吸収スペクトルは，ドップラー幅の中にローレンツ型の反転くぼみとして観測される．実際作成した吸収係数αの理論モデルも，Fig.5-18に示すように線幅が50MHzのローレンツ分布になった．

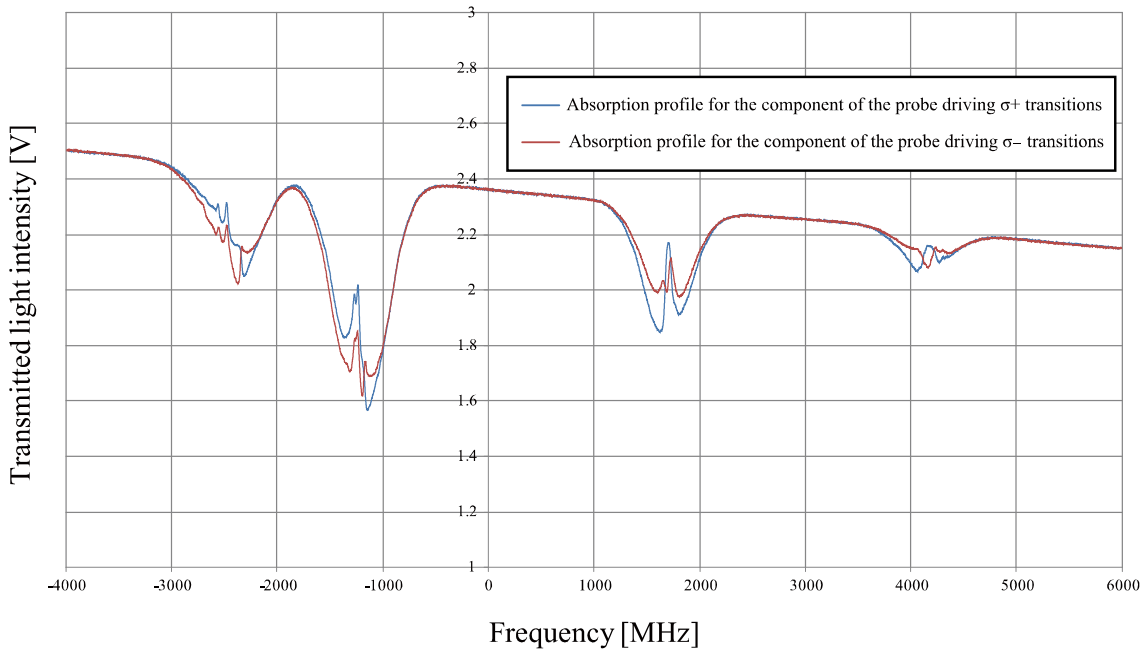


Fig.5-17 Observed Rb-D2 absorption profile for the component of the probe driving σ± transitions.

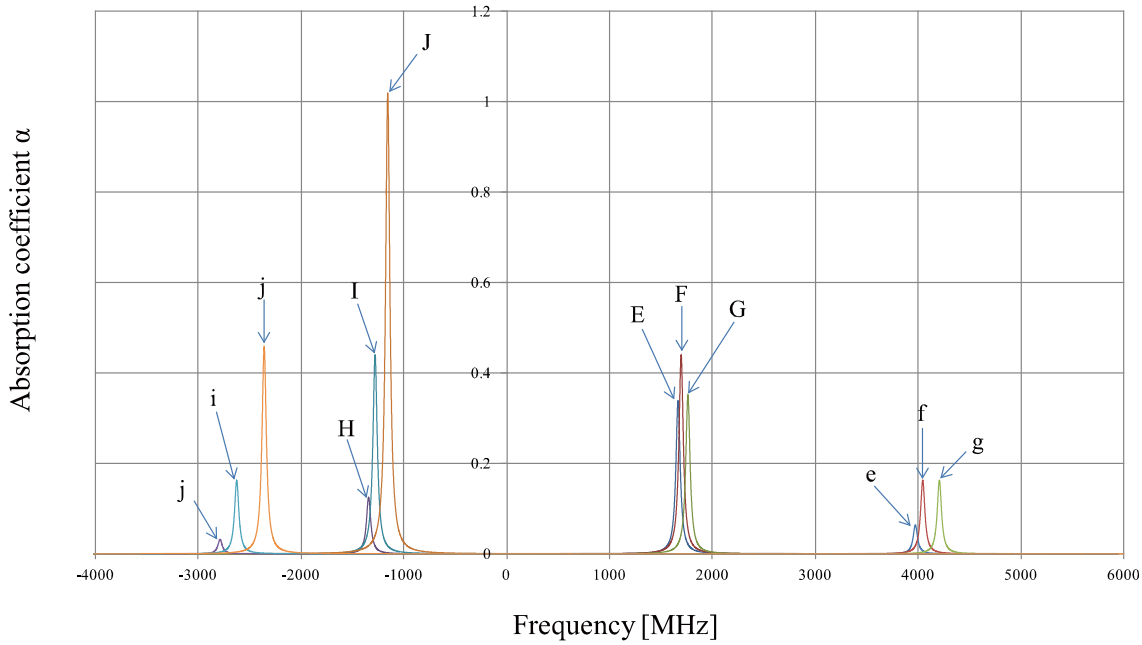


Fig.5-18 Absorption coefficient of each absorption spectrum.

Table 5-3 偏光スペクトルの理論値計算のためのパラメータ

吸収スペクトルの線幅 Γ	50 [MHz]
セルの長さ L	0.08 [m]
$b_I = \frac{1}{2}(b_{I+} + b_{I-})$	0
$\Delta b_R = b_{R+} - b_{R-}$	0
セルのない時のプローブ光の強度 I_0	≅ 0.045 [mW]
$\Delta\alpha_0$（スペクトル e）	0.668
$\Delta\alpha_0$（スペクトル f）	0.864
$\Delta\alpha_0$（スペクトル g）	0.692
$\Delta\alpha_0$（スペクトル h）	0.1845
$\Delta\alpha_0$（スペクトル i）	0.648
$\Delta\alpha_0$（スペクトル j）	1.5
$\Delta\alpha_0$（スペクトル E）	0.128
$\Delta\alpha_0$（スペクトル F）	0.322
$\Delta\alpha_0$（スペクトル G）	0.322
$\Delta\alpha_0$（スペクトル H）	0.064
$\Delta\alpha_0$（スペクトル I）	0.322
$\Delta\alpha_0$（スペクトル J）	0.9

5.1.7 PLL Optical Frequency Synthesize[57]

我々は Rb-D_2 吸収曲線の傾斜領域に，半導体レーザの発振周波数を安定化するために，PLL（Phase-Locked-Loop）の技術を用いた PLL 光周波数シンセサイザ（PLL Optical Frequency Synthesize）を構築した．Fig.5-19 は，その PLL の基本構成図である．PLL は，位相比較器（PC：Phase Comparator），ループフィルタ（Loop Filter）またはローパスフィルタ（LPF：Low-pass Filter），電圧制御発振器（VCO：Voltage Controlled Oscillator）及び，基準信号用外部クロック（EC：External Clock）から構成される周波数負帰還回路である．PLL の制御ループは，参照周波数f_{ref}と VCO の出力周波数$f_{out} = f_d$が常に一致するように動作する．位相比較器はf_{ref}とf_dの誤差に対応した誤差パルス信号を出力し，その信号を LPF が直流電圧の誤差信号に変換している．LPF はパルス信号を直流電圧に変換する役目のほか，積分回路として動作し，そのまま I 制御となる．この PLL も一種の周波数シンセサイザと呼べるが，基準信号の周波数をそのままコピーしているだけであり，実用的な PLL シンセサイザにするためには自由に周波数を可変できる仕組みが必要になる．

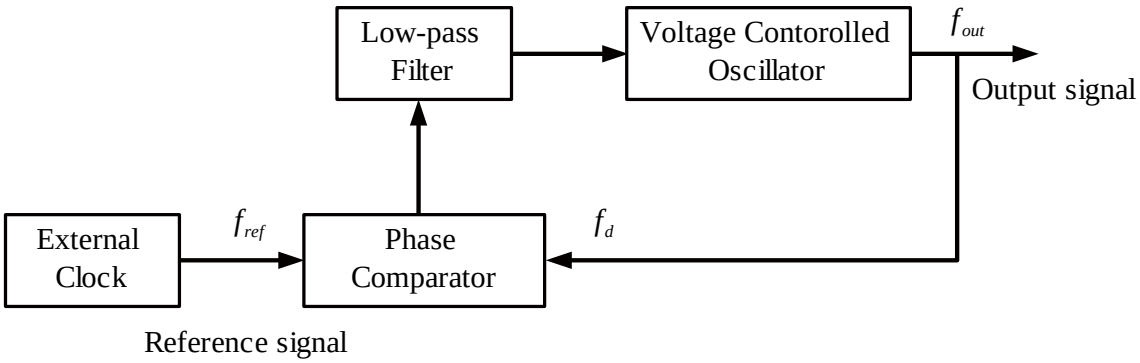


Fig.5-19 Base configuration of Phase-locked-Loop.

PLL を利用した実用的な周波数シンセサイザは，PLL の位相比較器と電圧制御発振器の間に分周器を挿入することで実現される．Fig.5-20 はその基本構成図を示している．PLL シンセサイザの出力周波数をf_{out}とおくと，Fig.5-20 から分かるよう以下のような関係が成り立つ．

$$f_d = f_{out}/N \tag{5-28}$$

ここで PLL が構成されることによって$f_d = f_{ref}$が成り立つため

$$f_{out} = f_{ref} \times N \tag{5-29}$$

となる．すなわち，出力周波数f_{out}は，参照周波数f_{ref}のN倍となり，f_{ref}と分周数 N によって PLL シンセサイザの出力周波数が，自由に選択できるようになる．この PLL シンセサイザは高いレベルで完成された技術であるため信頼性が非常に高く，今日では携帯電話や衛星通信などほとんどの無線機器に用いられている．PLL 光周波数シンセサイザは，この技術を応用したものである．

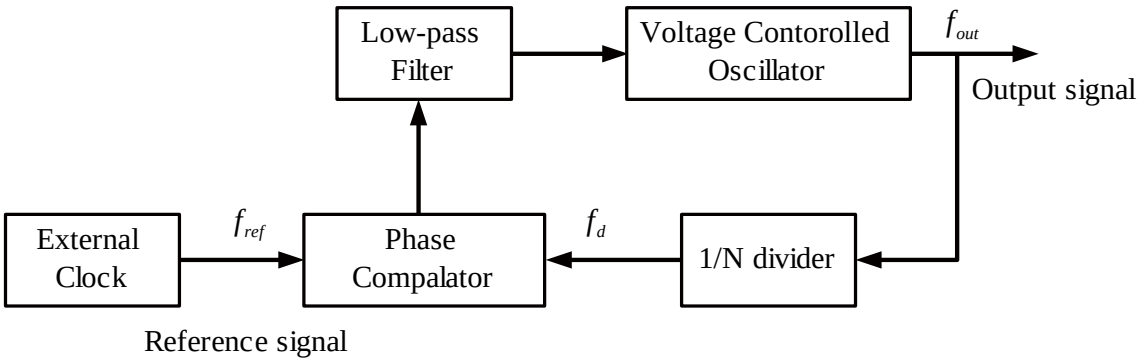


Fig.5-20 Base configuration of PLL frequency synthesizer.

Fig.5-21 に，構築した PLL 光周波数シンセサイザの基本構成を示す．PLL 光周波数シンセサイザは，8bit プログラマブル分周器，位相比較器，ループフィルタから成る PLL unit とビート信号を検出するための光学系から成る VCO Section，そして分周器から構成される．VCO Section では，発振周波数を Rb-D_2 吸収線の偏光信号の波長にロックした安定化レーザ（Stabilized Laser）と周波数可変レーザ（Tunable Laser）の光軸を一致させ，フォトディテクタで受光することでビート信号を検出している．検出されたビート信号は，2 つの半導体レーザの発振周波数の差周波の周波数を持つ．これを一種の VCO と見なし周波数可変レーザを PLL で制御することで絶対周波数がわかるレーザ光を実現している．

PLL 光周波数シンセサイザは，VCO の代わりに 2 つレーザ光のビート周波数を PLL で制御するため，その出力f_{out}は，以下の式のような関係が成りたつ．

$$f_{out} = |f_1 - f_2| = N_1 N_2 f_{ref},\ f_{out} = f_{beat} \qquad (5\text{-}30)$$

f_1 : 周波数可変レーザの発振周波数，f_2 : 安定化レーザの発振周波数，N_1 : 分周器の分周数，N_2 : プログラマブル分周器の分周数，f_{ref} : リファレンスの周波数である．

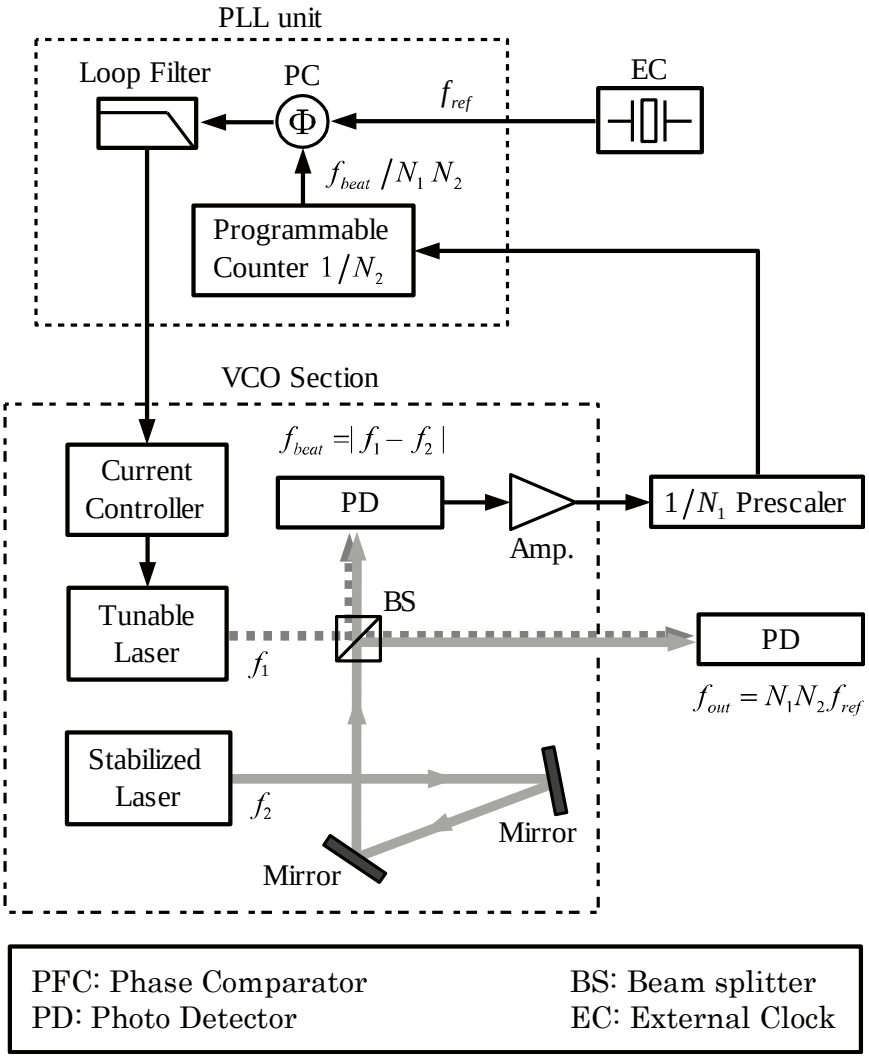


Fig.5-21 Optical Frequency Synthesizer Experiment system.

5.2 周波数安定度の評価方法

半導体レーザの発振周波数の安定度の評価には，中心周波数からの周波数揺らぎの瞬時値を中心周波数で規格化した相対的な周波数揺らぎの量を用いて，パワースペクトル密度やアラン分散などで安定度を評価する方法がある．本研究ではアラン分散により安定度の評価を行う．

本節では，まず 5.2.1 項でアラン分散について述べ，5.2.2 項でフリーランニング状態の半導体レーザの雑音について，5.2.3 項でビート信号によるレーザの発振周波数の測定方法についてそれぞれ述べる．

5.2.1 アラン分散[58][59]

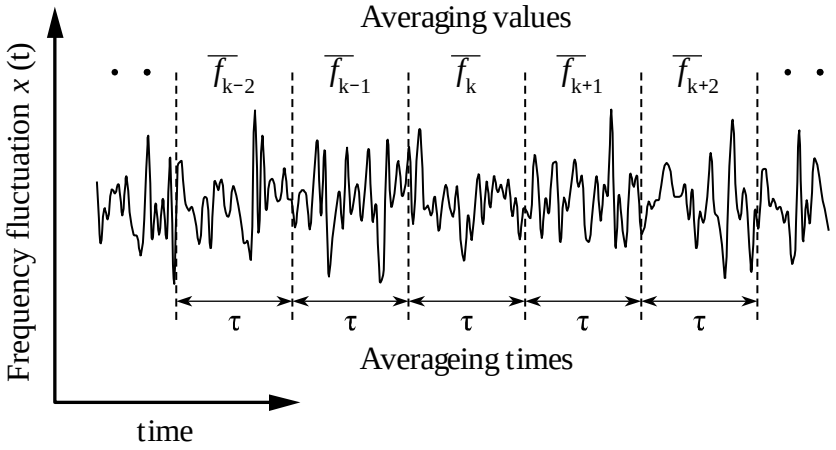


Fig.5-22 Definition of the Allan variance.

発振器などの発振周波数安定度を表す尺度として，アラン分散が用いられる．この評価方法は，一定期間の安定化で得られたデータ群を集計して高い周波数成分から低い周波数成分までの測定データのばらつき（分散）を計算するもので，様々な周波数成分に対する安定度を評価することができる. Fig.5-22 に示すように, まず信号源の周波数の時間変化$x(t)$を平均化時間τで平均し，平均値$\overline{f_k}$を得る．

$$\overline{f_k} = \frac{1}{\tau}\int_{k\tau}^{(k+1)\tau} x(t)\,dt \tag{5-31}$$

連続する 2 個の平均周波数$\overline{f_1}$と$\overline{f_2}$をレーザの中心周波数fで規格化した$\overline{f_1}/f$，$\overline{f_2}/f$についての標本標準偏差の 2 乗は,

$$\frac{1}{2-1}\sum_{i=1}^{2}\left(\frac{f_1+f_2}{2}-\bar{f}_i\right)\cdot\frac{1}{f^2}=\frac{(f_1-f_2)}{2}\cdot\frac{1}{f^2} \tag{5-32}$$

となるが，アラン分散はこれを m 個の$\bar{f}_k$に対して計算し，それを平均したもので，次式で表される．

$$\sigma^2(2,\tau)=\frac{1}{m-1}\sum_{k=1}^{m-1}\left(\frac{\overline{f_{k+1}}-\bar{f}_k}{2}\right)\cdot\frac{1}{f^2} \tag{5-33}$$

アラン分散$\sigma^2(2,\tau)$の変数部分にある 2 は“隣り合う 2 つの平均値$\bar{f}_k$と$\overline{f_{k+1}}$の差分をとる”ということを表し，平均化時間τが小さいほど短期安定度を，大きいほど長期安定度を表す．周波数安定度は(5-33)式の平方根値$\sigma(2,\tau)$が用いられ，アラン偏差（Allan deviation）と呼ばれる. また, $\sigma(2,\tau)$は平均化時間τにおける分散の期待値と見ることもできる. 従って, $\sigma(2,\tau)$にレーザの中心周波数を掛けることにより，時間τが経過した後に発振周波数が確率的に見てどの程度変動するかを知ることができる．なお，アラン分散はパワースペクトル密度から求めることもでき，パワースペクトル密度$S(f)$に対して，

$$\sigma^2(2,\tau)=2\int_0^{\infty}S(f)\frac{sin^4(\pi f\tau)}{(\pi f\tau)^2}df \tag{5-34}$$

の関係が成り立つ．Fig.5-23 にそのパワースペクトル密度とアラン偏差の関係を示す.

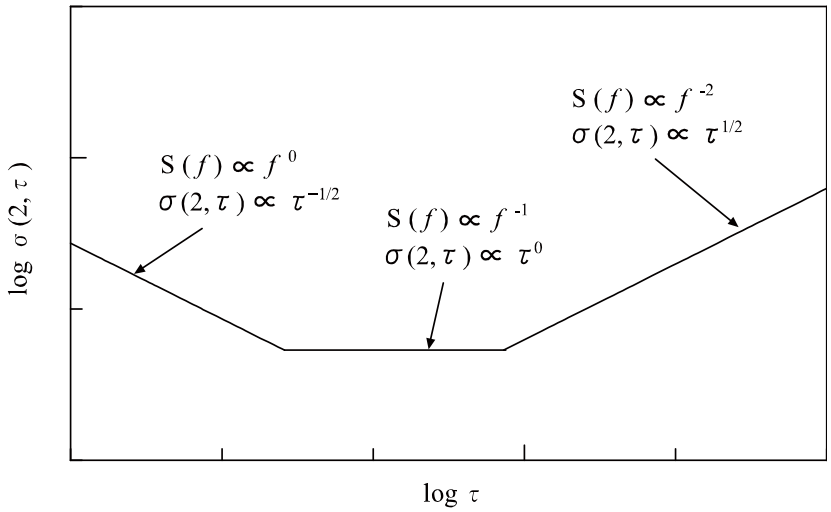


Fig.5-23 Relations of power spectrum density and the Allan deviation.

$S(f)\propto f^0$，$S(f)\propto f^{-1}$，$S(f)\propto f^{-2}$のような雑音は，それぞれ白色雑音（white noise），フリッカ雑音（flicker noise），ランダムウォーク（random walk）を示している．同図のように特

微的な雑音信号のパワースペクトル密度は，アラン偏差からも読み取ることができる．

5.2.2 フリーランニング状態の半導体レーザの雑音[17][20][60]

外部から何も制御を施さない状態，すなわちフリーランニング状態の半導体レーザの周波数雑音を与える各種雑音源のうち基本的なものは自然放出光である．これによる周波数雑音の大きさを半古典ランジュバン（Langevin）方程式によって求めアラン分散で表すと

$$\sigma^2(2,\tau) = \frac{h}{16\pi^2 \nu_0 P_0}\left(\frac{c}{nL}\right)^2 \left(\alpha_l L + ln\frac{1}{R}\right)\left(ln\frac{1}{R}\right) n_{sp}\tau^{-1} \qquad (5\text{-}35)$$

となる．この他に，この自然放出光を吸収し，伝導帯に励起されたキャリヤ数の変動により共振器の屈折率が変動して周波数が変動する．この大きさはαパラメータを使って表され，それは式(5-35)のα^2倍である．更にこのようにキャリア数が変動すると流れる電流も変化し自己発熱量も変化する．これにより共振器の縦モード周波数が温度ドリフトして周波数雑音を生ずる．以上がレーザ内部で発生する周波数雑音の要因である．

次に半導体レーザ外部に起因する雑音源としては，レーザ駆動用の電流源の電流変動がある．この電流源の雑音は，電流源に用いられるトランジスタやオペアンプなどの能動素子の雑音特性に依存したものである．また半導体レーザの雰囲気温度変動によっても雑音が発生する．これらは共にレーザを自己発熱させ共振器の縦モード周波数を変動させる要因である．これら内部・外部の雑音要因すべてを重ね合わせた結果が，実際に観測されるフリーランニング状態の半導体レーザの周波数雑音である．

以下に，これら雑音の理論計算値を示す．計算は 800nm 帯の AlGaAs レーザについて報告された論文[44]を参考にした．本研究で用いる半導体レーザは 780nm 帯のものであるが，材料や構造が同じであるため得られる結果は論文で示されたものと同程度であると考えられる．計算に用いたパラメータを Table 5-4 に示す．

Table 5-4 自然放出雑音のアラン分散の計算に用いたパラメータ

レーザ中心周波数 ν_0	375×10^{12} [Hz]
レーザ出力 P_0	3.0 [mW]
レーザ媒質の屈折率 n	3.5
共振器長 L	300 [μm]
共振器端面の反射率 R	0.3
モード損失係数α_l	80 [cm^{-1}]
自然放出因子n_{sp}	2
αパラメータ	2

- **内的要因**

＜自然放出雑音＞

$$\sigma(2,\tau) = 1.63 \times 10^{-12}\tau^{-1/2} \tag{5-36}$$

＜キャリア雑音＞

$$\sigma(2,\tau) = 3.25 \times 10^{-12}\tau^{-1/2} \tag{5-37}$$

＜電流雑音＞

$$\sigma(2,\tau) = \begin{cases} 1.38 \times 10^{-9}, & \tau < 1 \times 10^{-4}s \\ 8.31 \times 10^{-12}\tau^{-1/2}, & \tau \geq 1 \times 10^{-4}s \end{cases} \tag{5-38}$$

- **外的要因**

＜電流源雑音＞

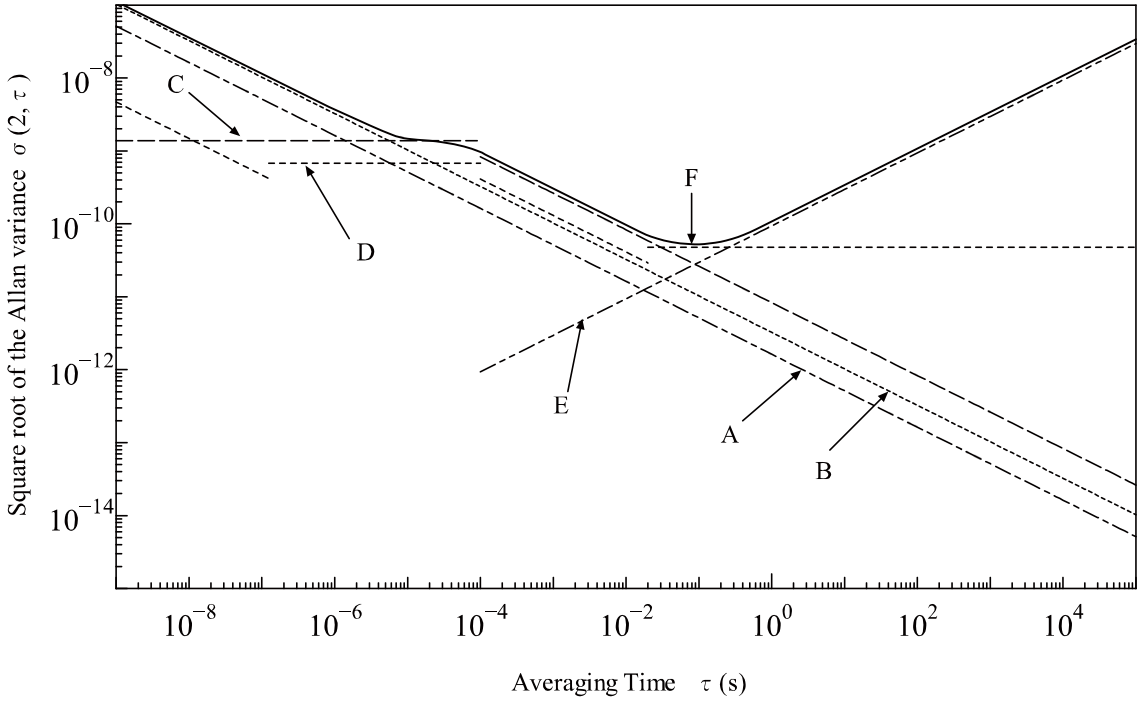
$$\sigma(2,\tau) = \begin{cases} 1.48 \times 10^{-13}\tau^{-1/2}, & \tau < 1.25 \times 10^{-7}s \\ 6.78 \times 10^{-10}, & 1.25 \times 10^{-7}s \leq \tau < 1 \times 10^{-4}s \\ 4.12 \times 10^{-12}\tau^{-1/2}, & 1 \times 10^{-4}s \leq \tau < 2 \times 10^{-2}s \\ 4.80 \times 10^{-11}, & \tau \geq 2 \times 10^{-2}s \end{cases} \tag{5-39}$$

＜温度雑音＞

半導体レーザの温度変動が，1×10^{-6}Kにまで抑えられるとして安定度を見積もると，以下のようになる．

$$\sigma(2,\tau) = 9.38 \times 10^{-11}\tau^{1/2}, \quad \tau \geq 1 \times 10^{-4}s \tag{5-40}$$

以上の結果をまとめたものが，Fig.5-23 である．曲線 A, B, C がそれぞれ内的要因である自然放出雑音，キャリア雑音，電流雑音であり，曲線 D, E が外的要因である電流源雑音と温度雑音である．そして，内的・外的要因のすべてを重ね合わせた結果が曲線 F である．すなわち，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，曲線 F 以上になることが分かる．



A : spontaneous emission noise (eq.5-36). B : carrier noise (eq.5-37).

C : current noise (eq.5-38). D : current source noise (eq.5-39).

E : temperature noise (eq.5-40). F : limit value of the frequency noise of the free running.

Fig.5-24 Calculated results of the square root of the Allan variance of the frequency fluctuations for AlGaAs lasers.

5.2.3 ビート信号によるレーザの発振周波数の測定

安定度を評価するためには，半導体レーザの発振周波数を直接観測することが好ましいが，発振周波数は数百 THz にも達するため直接観測することは困難である．そこで独立した 2 つの系の各レーザ間のビート周波数の変動を観測することで安定度を評価する．ここでいうビートとは, 極近接した光の周波数差であり音の現象でいう“うなり”と同じものである．この現象はレーザ光を電波と同様に電場の正弦波的な振動と考えることで議論できる．周波数がわずかに異なる 2 つの波を重ね合わせると，合成波のエネルギー密度に 2 つの波の周波数差を持つゆっくりとした波動が現れる．光のエネルギー密度は普通，光の強度と呼ばれ，短時間に単位面積を通過するエネルギーを表し，自由空間を伝わる光，すなわち横波電磁波では電場の複素振幅の絶対値の 2 乗で与えられる．

点P_0での 2 つの光の各々の複素振幅を$E_1(P_0,t)$，$E_2(P_0,t)$とすると，2 つの光を重ね合わせた時の強度$I(P_0,t)$は，

$$\begin{aligned} I(P_0,t) &= |E_1(P_0,t)+E_2(P_0,t)|^2 \\ &= |E_1(P_0,t)|^2+|E_2(P_0,t)|^2+2Re\{E_1(P_0,t)+E_2(P_0,t)\} \end{aligned} \tag{5-41}$$

となる．ただし，$Re\{Z\}$は複素量Zの実部を表す.

一般に，距離rだけ離れた点Pに伝わったときの電場の複素振幅$E(P,t)$は

$$E(P,t)=A_0 exp\{i(\omega t-\kappa r)\} \tag{5-42}$$

と表され, A_0は振幅，ωは光の角振動数（angular frequency），κは角波数（angular wave number）と呼ばれる量である．光速をc，波長をλ，振動数をνとすると，これらの間には次式の関係がある．

$$\omega=2\pi\nu=\frac{2\pi}{\lambda}\cdot c=\kappa c \tag{5-43}$$

可視領域の光では，νは 10^{14}Hz 程度であり，このように速い振動に追従する検出器も計測器もなく，光波の振動を直接計数することはできない．通常検出器として使われているものは光の強度を検出し，これに比例した数の光電子を生じるものである．光電子を生じる検出器より得られる光電流$i(t)$は単位時間に光電面の各点に生じた光電子電荷の少量に等しく，

$$i(t)=\int \eta(P_0)I(P_0,t)dA \tag{5-44}$$

となる．ここで，$\eta(P_0)$は光電面上P_0点での光強度－電荷の変換係数であり，以後簡単のために光電面は半径R_0の円形とし，この上でηは一定と仮定する．また，dAはP_0の周りの微小面積であり，積分は光電面上の前面に渡って行われる．座標原点を光電面中心にとり，2 つの光波の干渉距離をr_1，r_2としてそれぞれの光波の角周波数をω_1，ω_2としたときの光電流$i(t)$は，

$$\begin{aligned} i(t) &= 2\pi R_0^2\eta(A_1^2 + A_2^2) + 2\eta A_1 A_2 cos\{(\omega_1 - \omega_2)t\} \cdot \int exp\{-i(\kappa_1 r_1 - \kappa_2 r_2)\}\, dA \\ &= i_{dc} + i_{ac} \end{aligned} \tag{5-45}$$

となる．右辺の最初の項i_{dc}は各々の点光源からの光強度の和から生じる電流であり，光源強度が時間的に変化しなければ一定であるが，積分を含む項i_{ac}は，

$$\Delta\omega = \omega_1 - \omega_2 \tag{5-46}$$

の角周波数$\Delta\omega$で振動する交流電流を与える．この比較的低い周波数の振動は 2 つの光波のビートによって作り出されたもので，光電検出器の高域応答周波数より$\Delta\omega$が低い場合は，この光電流の交流周波数を測定することから光波のビート周波数が決定できる．これにより，半導体レーザの発振周波数の変動をビート周波数の変動として周波数カウンタで測定し，前項で述べたアラン分散の平方根値を算出することにより正確な安定度の評価を行うことができる．

また，独立した 2 つの系を両方とも同じ設計にすれば，安定度の評価によってその系の再現性を調べることができる．さらに，一方が他方よりも明らかに安定度が低い場合は，安定度の低い方の安定度についてより高い精度で評価できるとされている．

第 6 章 物理乱数を生成するための XOR 演算に関する実験

本研究では，半導体レーザの周波数雑音から物理乱数を生成する実験を行った．第 4 章で説明したように，我々の物理乱数の生成方法では，2 つの独立した異なる 2 進数データ間の XOR 演算が必要である. そのため, 物理乱数を生成するための XOR 演算に使用する Delay Data の遅延時間は, 生成される物理乱数の品質に大きく影響する. そこで, 我々は Delay Data に必要とされる遅延時間について調査することとした.

6.1 実験方法

実験方法は，実際に異なる遅延時間の 2 進数データを使って物理乱数列を生成し，それらの生成された物理乱数列の品質を比較することで，最適な遅延時間の条件を調べる．品質の比較実験には，最も無秩序性が劣る 2 進数データの最上位ビット（MSB）から生成した物理乱数列を使用する（すなわち，並列生成方式における r7 bit から生成される物理乱数列を使用する）. Fig.6-1 は, その 2 進数データの r7 bit を使った XOR 演算を示している. Fig.6-1 に示すように XOR 演算に使用する Delay Data は, 4.1.1 項で説明した方法と同様に Base Data の遅延を施して減った先頭のデータを遅延によって余った末尾のデータで補うことで生成する.

実験では，物理乱数列を，遅延時間 0.02 μs～0.2 ms の間で生成する．また各桁を 20 等分する間隔（すなわち，80 通り）で物理乱数列を生成する．A/D コンバータのサンプリング速度は，500 MS/s を使用することとする．生成された物理乱数列の品質は，4.2.1 項で説明した乱数検定 SP800-22 を使用して評価する．SP800-22 のパラメータは，Table 6-1 に示した通りである.

以下本節では，6.1.1 項と 6.1.2 項でそれぞれ実験に使用した周波数雑音検出器の実験系と Reference Laser の実験系について説明する.

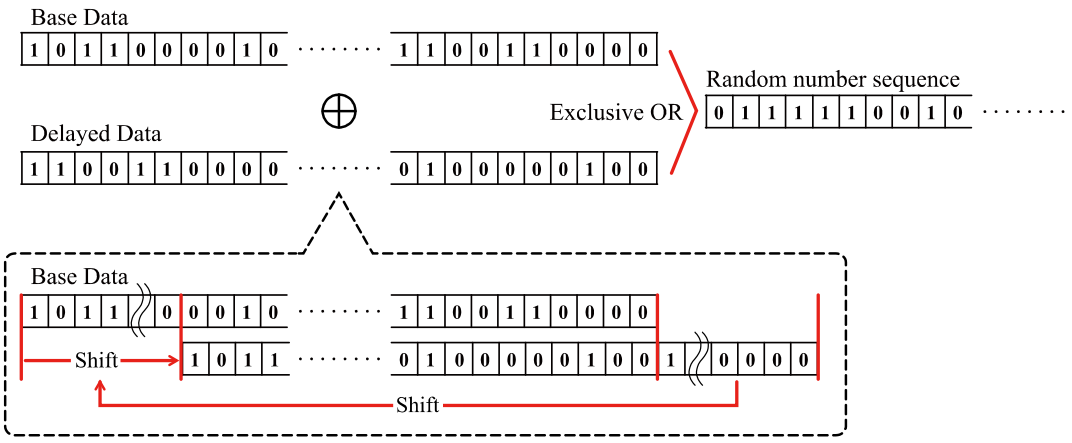


Fig.6-1 Exclusive-OR operation by r7 bit binary sequence.

Table 6-1 Parameters used for NIST SP800-22 test suite.

Test Name	Block Length
Block Frequency Test	128
Non-overlapping Template Test	9
Overlapping Template Test	9
Approximate Entropy Test	10
Serial Test	16
Linear Complexity Test	500

6.1.1 周波数雑音検出器の実験系

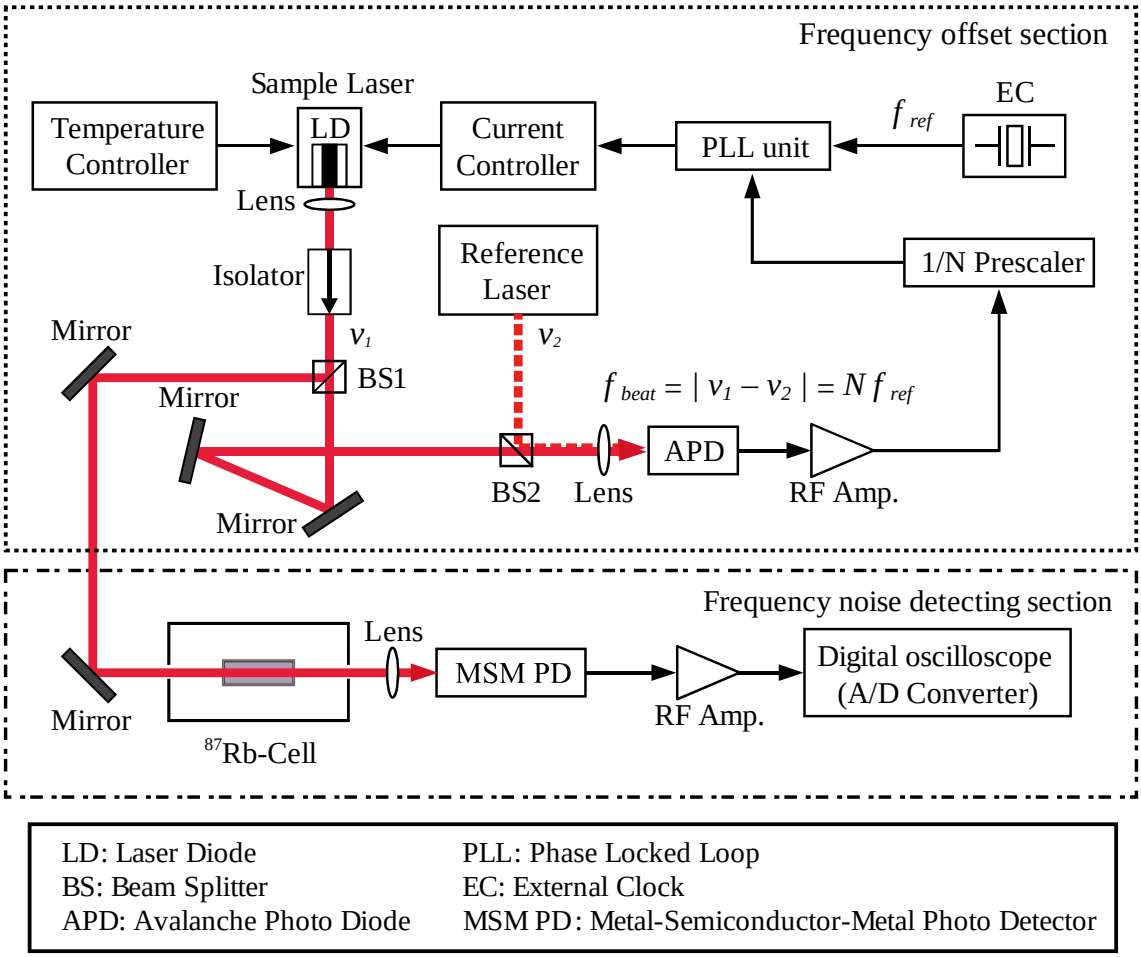


Fig.6-2 Experiment setup to detect a frequency noise.

我々は，半導体レーザの発振周波数の中心周波数を，PLL を使用した周波数シンセサイザ[61]の技術によって制御する．Fig.6-2 に，実際の半導体レーザの周波数雑音検出システム

の実験系を示す．このシステムは，半導体レーザの中心周波数を制御するためのシステムと半導体レーザの周波数雑音を実際に検出するためのシステムの 2 つのシステムから構成されている．Fig.6-1 に示された Sample Laser（Sanyo, DL7140-201）が周波数雑音を検出するための半導体レーザである．この Sample Laser は，発振波長 785 nm，光出力 70 mW，閾値電流 30 mA（ケース温度 25℃）の Fabry-Perot type AlGaAs Diode Laser である．実験では，注入電流は 58 mA に設定した．また雰囲気温度は，±1/100 K の精度の温度コントローラ（Yamaki, KLT-2）を用いて 17.00 ℃に制御した．

Sample Laser の中心周波数は，Frequency offset section で制御される．Reference Laser は，Sample Laser の中心周波数を制御するために必要となる周波数基準である．Reference Laser は，Rb 原子吸収線の偏光分光法[48][49][50]によって得られた周波数誤差信号を用いて発振周波数が安定化された半導体レーザ（Sanyo, DL-7140-201）である．ここでの誤差信号とは，半導体レーザの中心周波数と相対周波数の間の差を示した信号である．

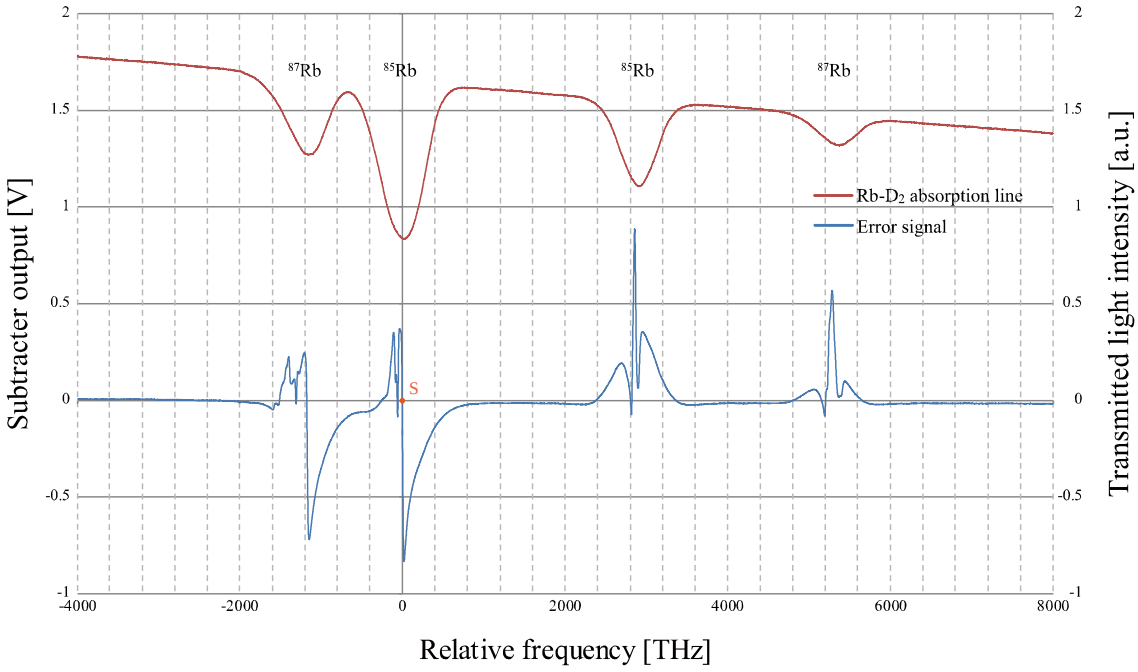


Fig. 6-3 Observed profiles of the Rb-D_2 absorption line and the error signals obtained using polarization spectroscopy.

Fig.6-3 に実際に観測された Rb 原子の D_2 吸収線とそれの偏光分光から得られた信号を示す．Reference Laser の発振周波数は，この信号のゼロクロス点の 1 つである S 点に安定化される．我々は，Sample Laser の中心周波数を制御するために，Sample Laser と Reference Laser との間で生成されたビート信号を一種の Voltage Controlled Oscillator（VCO）と見なす．そしてビート信号の周波数が一定になるように，Sample Laser の注入電流を PLL で制御する[61]．Sample Laser の中心周波数は，Reference Laser の発振周波数の中心周波数から周波数オフセ

ットされた周波数になる．（すなわち，Sample Laser の中心周波数は S 点の周波数から周波数オフセットされた周波数になる．）オフセット周波数は，External Clock の周波数と分周器の分周数を変えることで自由に変更することができる．我々は，Sample Laser の中心周波数を S 点から低周波側に周波数オフセットすることで，^{87}Rb の $5S_{1/2}$ F=2 準位から $5P_{3/2}$ F=1,2,3 準位への遷移に対応する吸収曲線を周波数弁別器として使用する．^{87}Rb 原子を封入した ^{87}Rb-Cell が本システムにおける周波数弁別器である．^{87}Rb-Cell を透過した光を観測するための受光素子は，Metal-Semiconductor-Metal Photo Detector（MSM PD, HAMAMATSU, G4176-03）を使用する．MSM PD の応答速度は，上昇時間，下降時間がともに 30 ps である．また，応答速度を遮断周波数に換算すると，約 11.7GHz になる．遮断周波数f_cは以下の式から求めた．

$$t_r = \frac{0.35}{f_c} \tag{6-1}$$

ここで，t_rは上昇時間である．MSM PD から得られた透過光強度信号は，2 台の Low Noise RF Amplifier（Mini-Circuits, ZFL-1000LN+：Bandwidth 0.1～1,000 MHz）を用いて 2 段で増幅される．増幅された透過光強度信号の交流成分を観測することで周波数雑音と比例関係にある電気信号を得ることができる．透過光強度信号の直流成分は，High pass filter としても働く RF Amplifier によって除去される．RF Amp.で増幅された信号は，デジタルオシロスコープ（LeCroy, WaveRunner Zi64：Bandwidth 4.0 GHz）に内蔵された垂直分解能 8 ビットの A/D コンバータによって，2 進数のデータに変換される．このデータから物理乱数を生成する．

6.1.2 Reference Laser の実験系

Fig.6-4 に Rb 原子吸収線の偏光分光信号を用いた半導体レーザの発振周波数安定化のための光学系を示す．半導体レーザの動作温度は，±1/100 K の精度の温度コントローラ(Yamaki KLT-2)によって制御する．半導体レーザの出力光は戻り光を抑制するファラデーアイソレータ（Isolator）を通過し，BS によって分けられる．一方の光をレーザの出力光とし，もう一方の光を Rb 原子吸収線の偏光分光信号を得るために用いる．偏光信号は，PBS の S 偏光の光を 1/4 波長版（λ/4 Plate）によって円偏光に変換したポンプ光（pump beam）を，Rb セルを通過する P 偏光のプローブ光（probe beam）に逆向きに入射することで得られる．PBS の前の 1/2 波長版（λ/2 Plate）は，直線偏光の偏光方向を調整することで S 偏光と P 偏光の光量を調整している．ポンプ光は＋σ 遷移と－σ 遷移をそれぞれ Rb 原子吸収線に誘発し，プローブ光の偏光面の回転に寄与する．プローブ光は 1/2 波長版を透過し，PBS で偏光方向の変化が逆の強度変化になる 2 つの光に分けられ，それぞれ APD1，APD2 に受光される．この得られた信号は偏光波形と通常吸収波形の合成波形であり，減算器に入力して差を取る

ことで通常吸収波形が相殺された偏光分光波形を得ることができる．この信号は零クロス点を持つため半導体レーザの発振周波数安定化のための誤差信号として使用することができる．この誤差信号から生成した比例，積分，微分制御信号（PID 制御信号）を，半導体レーザの注入電流にフィードバックすることで安定化が行われる．

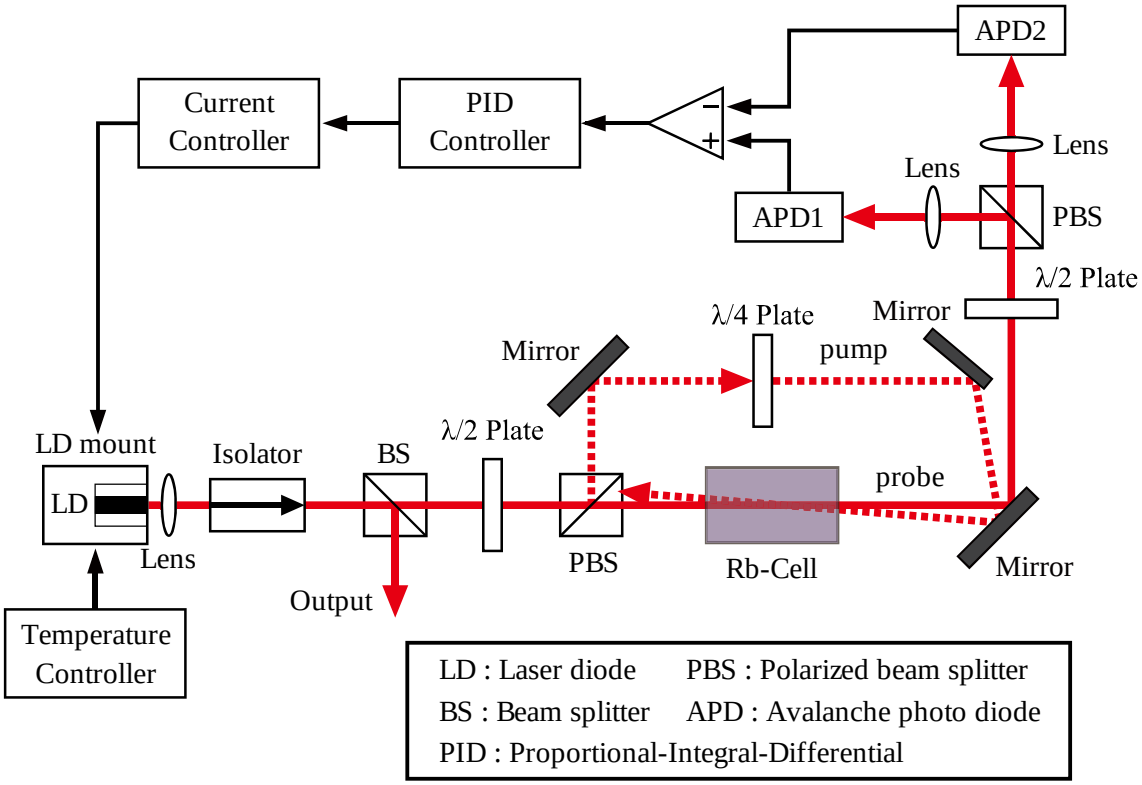


Fig.6-4 Experiment setup of Polarization spectroscopy.

6.2 実験結果と考察

6.2.1 実験結果

Fig.6-5 に XOR 演算のための 2 進数データの遅延時間とその生成された物理乱数の SP800-22 における合格率の関係を示す．Fig.6-5 では，横軸の遅延時間は，遅延ビットに換算している．遅延ビットは以下の式で求まる．

$$n_{bit} = t_{delay} \cdot f_S \tag{6-2}$$

ここで，n_{bit}は遅延ビット，t_{delay}は遅延時間，f_Sは，A/D コンバータのサンプリング速度である．これより遅延時間 0.02 μs～0.2 ms は，A/D コンバータのサンプリング速度 500 MS/s の場合，遅延ビット 10 ビット～10^5 ビットに変換できる．また図上の赤い線は，SP800-22 の理論合格率を示している．各遅延時間における合格率は，乱数検定の試行回数 100 回における検定合格率である．そのため我々は，各遅延時間ごとに 1 Gbit の長さの 2 進数列（物理乱数列）を 100 セット生成した．

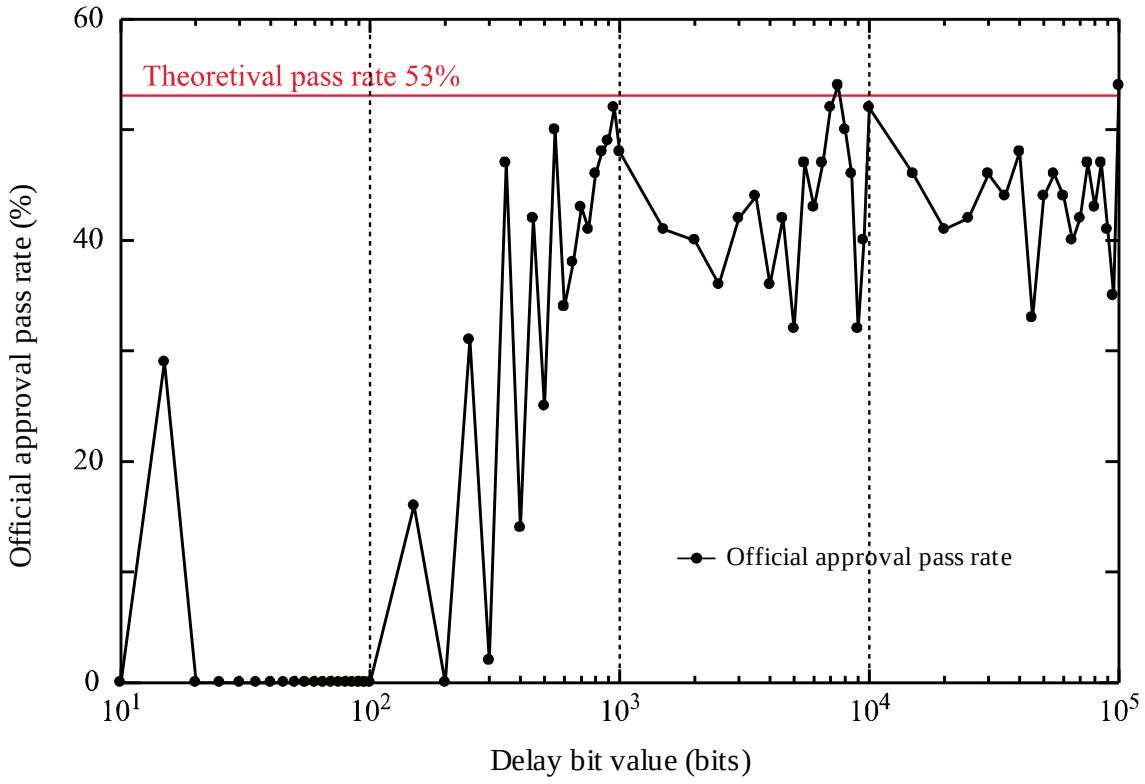


Fig.6-5 Delay times for XOR

横軸（遅延じっと）の分解能が低いため，正確さに問題があるが，図から 10 ビット～10^3 ビットあたりまでは，遅延ビットの値が大きくなるにつれて，検定合格率も共に上昇していることが分かる. また, 検定合格率の上昇は 9×10^2 ビットを超えたあたりで頭打ちになり，およそ 43±10 %くらいの範囲でほぼ安定することが分かった.

6.2.2 考察

我々は，実験のサンプリング速度（500 MS/s）が遅いことやサンプリング速度に対して RF-Amp.の増幅帯域や A/D コンバータのアナログ帯域が十分に広いことから，検出した周波数雑音が十分に白色雑音に近い性質を有していると考えた．そのため周波数雑音（白色雑音）から得られた 2 進数列データは，1 ビットの遅延を与えるだけで，素の 2 進数データと十分異なる 2 進数データが得られると予想した．すなわち，1 ビットの遅延を与えたデータと素のデータとの間で排他的論理和を行い生成された 2 進数列は，乱数になると予想した．しかし，実際には 10 ビット～10^2 ビット程度の遅延では，ほとんど品質の高い物理乱数列は生成されなかった．このような結果になった理由として，半導体レーザの周波数雑音が，理想的な白色雑音でなかった可能性や観測系の予期せぬ雑音が影響した可能性が考えられる.

単一縦モード半導体レーザの周波数雑音は，自然放出光およびそれによって誘発された屈折率揺らぎ（キャリア密度揺らぎ）や，温度揺らぎ，1/f 揺らぎなどによる光位相の変動が原因になっている．そして Fig.6-6[62]に示すように半導体レーザの周波数雑音は，DC～1 MHz 付近までの低域では, 温度揺らぎや 1/f 揺らぎが支配的で, 1 MHz 以上の周波数域では, 自然放出光揺らぎをベースとした屈折率揺らぎが支配的である．この屈折率揺らぎはほぼ白色雑音の特性を有しているが，それ以外の雑音は白色雑音ではないため，このことが実験において遅延時間に影響したことは十分考えられる．また観測系の特性を決定する電気信号を増幅するための RF-Amp.の周波数特性や雑音，A/D コンバータ自身の雑音などが，観測される 2 進数列データに非常に大きな影響を与えたと考えられ，今後はこれらの特性についても考慮する必要があると考える.

最後に，今回の実験結果はあくまでも我々の構築したシステムにおいて必要とされる遅延時間であり，使用する半導体レーザや観測機器によって結果が異なるであろうことが予想される．そのため異なる条件下による更なる実験が必要性である．また Fig.6-5 の実験から良質な物理乱数列を生成するために必要な遅延ビットは，およそ 1,000 ビット以上，すなわち 1,000 bit / 500 MS/s = 0.000002 sec = 2 μs 以上の遅延時間が必要であることが分かるが，この条件は 500 MS/s 以上の速度でサンプリングした場合には当てはまらないため，今後サンプリング速度を上げた実験も必要である.

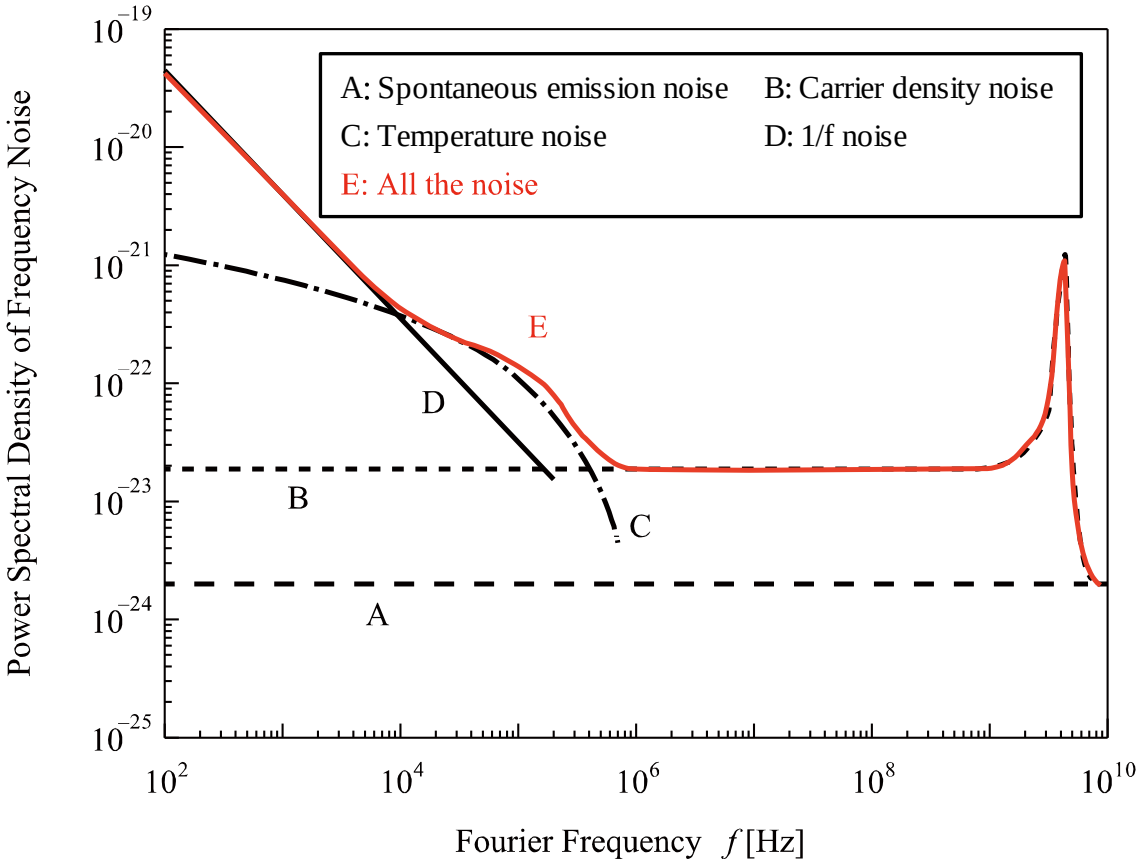


Fig.6-6 Power spectral density of LD's frequency noise.

第 7 章 周波数弁別器の最適な使用条件に関する実験

本研究で，我々は半導体レーザの周波数雑音を周波数弁別器を使用する方法で検出する．そのため，我々の方法で生成される物理乱数列の品質は，周波数弁別器と半導体レーザの発振周波数の間の関係によって大きく影響を受ける．これは半導体レーザの発振スペクトルの中心周波数を周波数弁別器のどの位置に設定するかによって，検出される雑音信号の周波数特性が変化してしまうからである．そこで我々は半導体レーザの発振スペクトルの中心周波数と周波数弁別器の関係について調査することとした．

7.1 実験方法

実験方法は，Rb 原子の吸収曲線の各位置（周波数）で物理乱数列を生成し，その生成された物理乱数列の品質を比較することで，良質な物理乱数列を生成するための最適な吸収曲線上の位置を調べる．生成する物理乱数列は，第 6 章の実験と同様に 2 進数データの最上位ビットから生成する. 実験のターゲットにする吸収線は, ^{87}Rb の $5S_{1/2}$ F=2 準位から $5P_{3/2}$ F=1,2,3 準位への遷移に対応した吸収線である．調査範囲は，吸収線のピークを中心に±1 GHz の範囲を調べる．また調査間隔は 20 MHz である．生成された物理乱数列の品質は，SP800-22 の結果を統計的に評価することで調べる（4.2.2 項を参照）．SP800-22 のパラメータは，Table 6-1 に示した通りである．また A/D コンバータのサンプリング速度は，500 MS/s と 1 GS/s の 2 通りについて調べる．

さらに，実験結果を考察するために，吸収曲線の各位置における透過光強度雑音信号のパワースペクトルを観測する．実験に使用する実験系は，第 6 章で XOR 演算に関する実験に使用したものと同じものを使用する（Fig.6-2 を参照）．

7.2 実験結果

7.2.1 乱数検定の合格率

Fig.7-1 に ^{87}Rb-D_2吸収曲線の輪郭とその吸収曲線の各位置で生成された乱数の検定合格率を示す．また図には吸収線の超微細構造も示す．我々は，この実験で XOR 演算のための 2 進数データの遅延時間を 2 μs に設定した. 遅延時間 2 μs はサンプリング速度が 500 MS/s と 1 GS/s である場合，それぞれ 2 進数のデータを 1,000 ビットと 2,000 ビット取得する時間に相当する．吸収曲線の各位置の検定合格率は，吸収曲線のそれぞれの位置で，100 セットの乱数列を取得し，100 回の SP800-22 の検定結果から算出した．算出された検定合格率は，有意水準を 1 %（$\alpha = 0.01$）に設定し，2 項検定によって評価した．有意水準 1 %の場合の信頼区間（Confidence interval）は，40 %～65 %の区間になる（4.2.2 項を参照）.

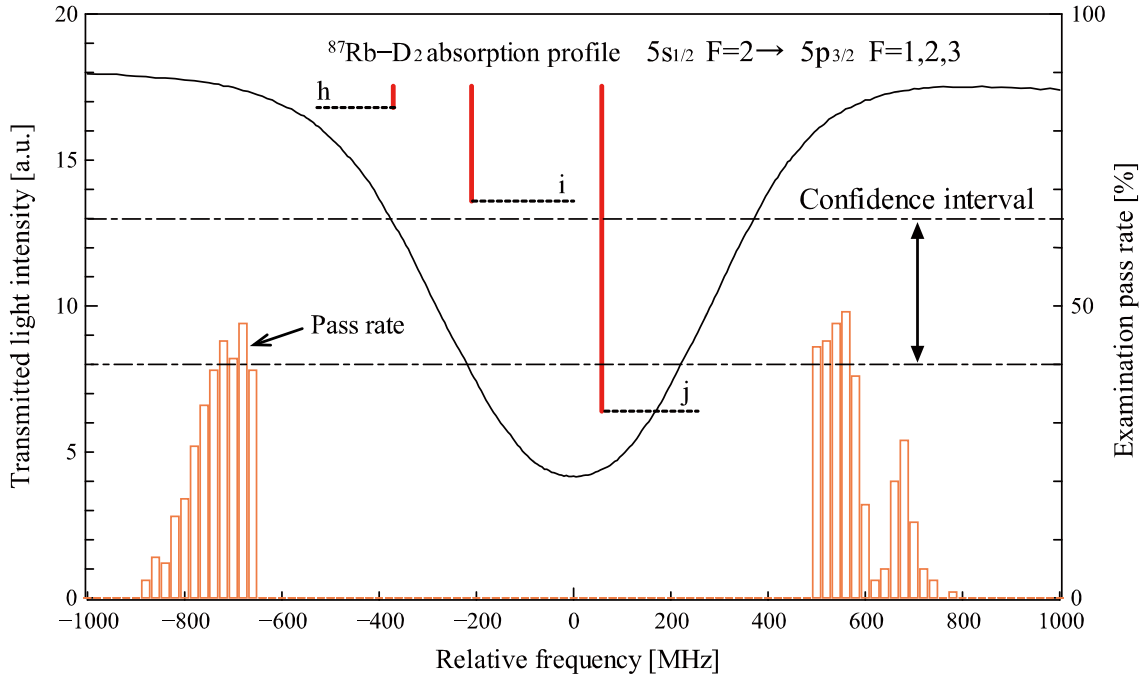


Fig.7-1 Pass rate of SP800-22 test in each position of the Rb-D_2 absorption curve.

Fig.7-1 によると，サンプリング速度が 500 MS/s の場合，吸収曲線の傾斜部分で信頼区間に含まれる乱数が生成できる位置は, 吸収曲線のピークから+500 MHz～+560 MHz の範囲と -720 MHz～-680 MHz の範囲であることが分かった．またこれらの領域は吸収線の低周波数側と高周波数側の両方で吸収線のピークから 500 MHz 以上離れた位置である．Rb 吸収線の FWHM がおよそ 500 MHz であることからも分かるように，この位置は吸収曲線の端に近い位置である．その領域の幅は Fig.7-1 から吸収線の低周波数側において 40 MHz（相対周波数 -720 MHz～-680 MHz），高周波数側において 60 MHz（相対周波数+500 MHz～+560 MHz）である（分解能が 20 MHz であるため正確さに欠けることに留意する必要がある）．吸収線の高周波数側と低周波数側で，良質な物理乱数が生成された領域の位置やその幅が異なるが，それらは Rb 原子の超微細構造によって吸収曲線が理想的なガウス分布の形から逸脱しているためと考えられる．

また我々はサンプリング速度 1 GS/s の場合の実験も行ったが，吸収曲線の傾斜部分において生成された全ての乱数列が，乱数検定を合格しないことを確認した．

7.2.2 透過光強度雑音信号のパワースペクトル

Fig.7-2 には，吸収曲線の傾斜部分の異なる位置で観測された透過光強度雑音信号のパワースペクトルが示されている．Fig.7-2 の上の図は，3D の等高線図でパワースペクトルの変

化を示している．また下の図は，3D の折れ線グラフによってパワースペクトルの変化を示している．パワースペクトルはデジタルオシロスコープの Fast Fourier transform（FFT）の演算機能を使用することによって取得している．A/D コンバータのサンプリング速度は，1 GS/s である．パワースペクトルの観測位置は，吸収線のピークを 0 Hz とした時の相対周波数によって表す．観測範囲は，相対周波数 0 Hz から±1000 MHz の範囲である．また観測間隔は，20 MHz 間隔である．この Fig.7-2 は，吸収曲線の各観測位置で，半導体レーザの周波数雑音が，どのように透過光強度雑音信号として観測されるかを説明する助けとなる．図から，変化する透過光強度雑音のレベルは，吸収スペクトルに沿って各々の位置で異なることが分かる．また，吸収スペクトルの急な傾斜では増加し，ピーク付近とほとんど勾配が観察されなかった吸収線の浅い傾斜では減少していることが分かる．半導体レーザの周波数雑音は，通常広い帯域において強く白色雑音の特性を有しているが，実際には，観察された雑音信号のパワースペクトルの強度は, Noise frequency に沿って変化している. また，ピーク付近と吸収曲線に沿った急傾斜の部分で観察された雑音信号は, Noise frequency に沿って，少しずつ減少している．これらの事実は，これらの領域で周波数弁別器が，ローパスフィルタのような振る舞いをすることを示している．一方，浅い斜面のあたりで観察された雑音信号は，Noise frequency に沿って，徐々に増加していることが分かる．これは浅い斜面の領域で周波数弁別器が，ハイパスフィルタ，正確にはバンドパスフィルタのように振る舞うことを示している．観測位置ごとのこれらの特徴や形状の違いは，周波数弁別器に依存する周波数雑音によって生じた左右のサイドバンドのバランスの崩れ方が，観測位置ごとに，異なることが原因である．このサイドバンドのバランスの崩れ方は，吸収線の輪郭（ガウス分布）の形とその帯域幅に依存している．

良質な物理乱数が生成された Rb 吸収曲線上の位置における透過光強度雑音信号と Background noise のパワースペクトルが，Fig.7-3 に示されている．図より，良質な物理乱数列が生成された位置では，およそ 250 MHz の広帯域にわたって，ほぼ白色雑音が観測されることが分かる．また Background noise は，半導体レーザの強度雑音，RF Amp.の雑音，MSM PD の雑音，デジタルオシロスコープ（A/D コンバータ）の雑音などによって構成されていることが分かる．特に A/D コンバータ由来と考えられる特定の周波数における非常に大きな雑音が，Background noise として観測されている．

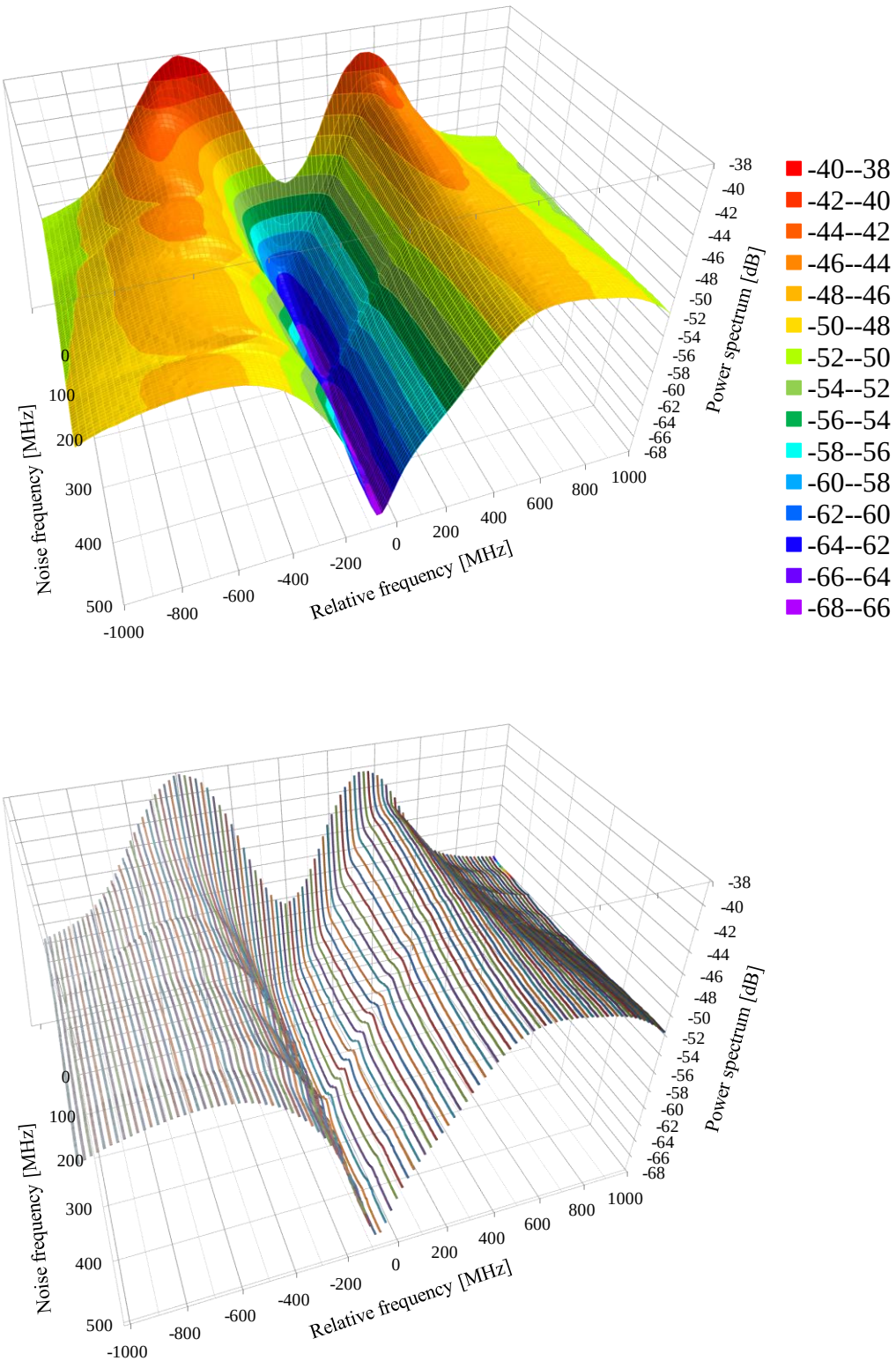


Fig.7-2 Power spectrum of the transmitted light-intensity signal observed at different positions (relative frequencies) along the Rb absorption curve.

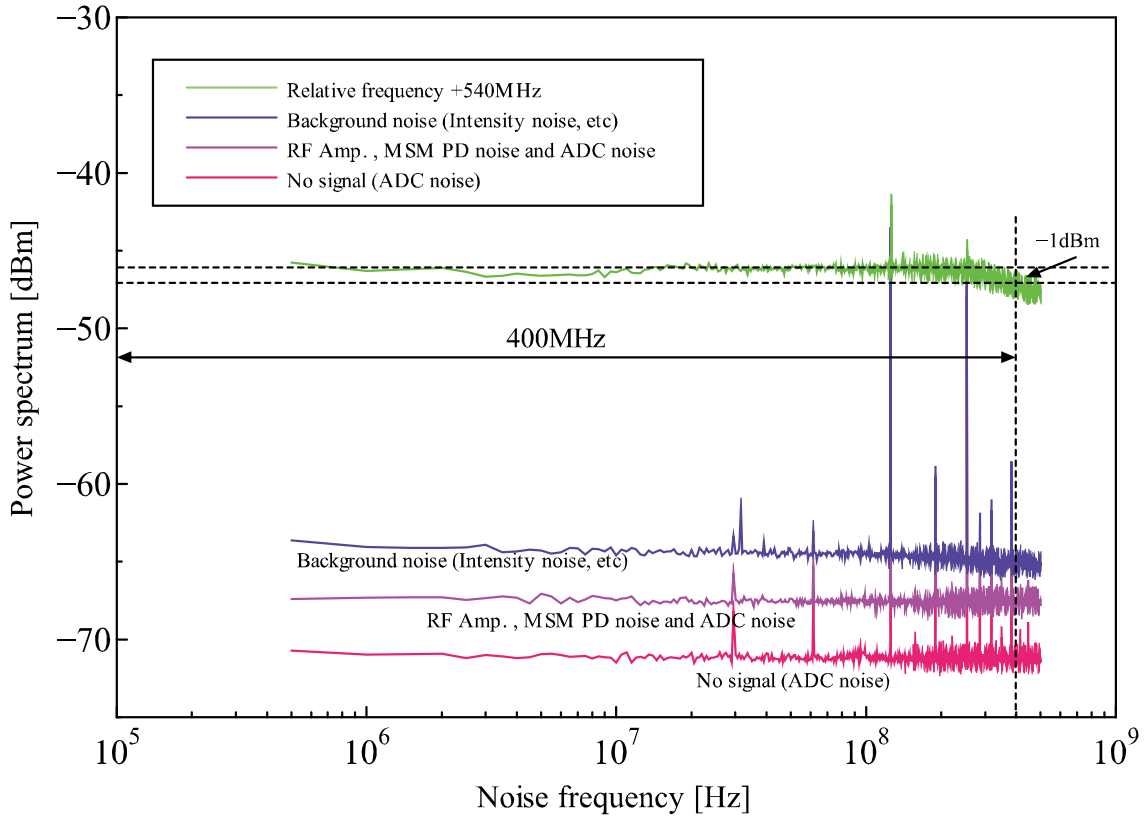


Fig.7-3 Power spectrum of the transmitted light-intensity signal observed at point where a good physical-random number was generated, along the Rb absorption curve, and that of background noise.

7.3 考察

7.3.1 良質な物理乱数が生成される周波数弁別器の領域

我々の周波数雑音の検出原理が，スロープ検波と同様の仕組みであるとするなら，半導体レーザの発振周波数は，スロープの傾きが最も急峻な位置に設定することが望ましいと予想できる．しかし実際の実験結果は，この考えと異なる結果となった．これはスロープの傾きが最も急峻な位置で，500 MS/s の速度において白色雑音の性質を持つ雑音が検出されなかったためであると考えらる．

3.2 節で説明した理論から，周波数弁別器における FM 信号の周波数ごとの検出効率は，周波数弁別器のピークと FM 信号のキャリア信号の間の位置関係（周波数差）によって変化することが予想される．具体的には，Fig.7-2 に示されたパワースペクトルのグラフから分かるように Rb 吸収線は，そのピークとキャリア信号の間の周波数差が小さい場合，片側サイドバンドの信号を検出する窓，そしてローパスフィルタのように動作する．周波数弁別器のスロープの傾きが急峻な位置は，ローパスフィルタ（周波数弁別器）の帯域が狭いため，低い周波数の信号が大きく検出されている（Fig.7-2）．よって，500 MS/s の速度でサンプリングした場合，良質な物理乱数を生成できなかった．一方良質な物理乱数列が高速に生成された吸収曲線上の領域の位置は，ローパスフィルタ（周波数弁別器）のカットオフ周波数が最大になった位置である．すなわち，この位置は半導体レーザの周波数雑音が，最も広帯域において白色雑音として検出される．よって，500 MS/s の速度でサンプリングした場合でも良質な物理乱数を生成することができた．

他の原子や分子の吸収線を周波数弁別器として使用する場合，基本的にはその外形がガウス分布によって近似できるため，その最適な領域の位置を見つけるための目安として今回の実験結果が使用できる．しかし最適な領域の厳密な位置は，RF-Amp.などの伝達特性，原子や分子の超微細構造の影響を受けるため個々に調べる必要がある．またファブリ・ペロー共振器やエタロンなどの場合は，その節の外形がガウス分布でないため，今回の実験結果から最適な領域の位置を予測することができないことに注意する必要がある．

7.3.2 乱数の生成速度

本研究では物理乱数の実時間生成を行っていないが，以後，実時間生成を行ったと仮定して生成速度について議論していく．そのため物理乱数の生成速度は，A/D コンバータのサンプリング速度と等しいと考えることとする．本実験では，サンプリング速度 500 MS/s で得られたデータから良質な物理乱数列を生成することに成功している．また 1 Gb/s（1 GS/s）の速度で良質な物理乱数を生成することができなかったことから，本方法における物理乱数の生成速度の限界は，500 Mb/s（500 MS/s）と 1 Gb/s（1 GS/s）の間に存在することが予

想される．本方法における物理乱数の生成速度の限界は，乱数源である半導体レーザの周波数雑音の帯域，周波数弁別器の復調帯域，増幅器（RF-Amp.）やケーブルを始めとした電気信号の伝達経路の帯域，そして観測機器の A/D コンバータのアナログ帯域によって複合的に決定される．本研究において，最も周波数特性が劣っていた要素は周波数弁別器であり，Fig.7-3 よりその復調帯域は，1 dBm ダウンにおいておよそ 400 MHz，0 dBm ダウンにおいておよそ 250 MHz 程度であった．このことから周波数弁別器の帯域 250 MHz（0 dBm ダウン）～400 MHz（1 dBm ダウン）の 2 倍の周期の速度（サンプリング定理より），すなわち 500 MS/s～800 MS/s でのサンプリングが，良質な物理乱数を生成するためのサンプリング速度の限界であると考えられる．これは我々の実験結果と一致する．

研究に使用した半導体レーザは，実測した結果，およそ 2 GHz 程度の帯域にわたって周波数雑音を持つことが分かっている．そして緩和振動周波数における共鳴ピーク[23]~[27]を考慮すると，白色雑音としての特性を持つ周波数雑音の帯域は，およそ 1 GHz 程度であった．このことから，さらに物理乱数の生成速度を向上させる為には，周波数弁別器の復調帯域を今の帯域よりも大きく広げる必要があると考えられる．そこで，今後は復調帯域を自由に設定できるエタロンなどを周波数弁別器に使用する必要があると考えられる．ただ周波数弁別器の復調利得と復調帯域はトレードオフの関係にあるため，帯域を不必要に広げることは利得の減少を引き起こすことに注意する必要がある．

第 8 章 物理乱数の安定的な生成に関する実験

次世代の通信用暗号技術には，非常に大量の乱数が必要とされる．そのため乱数生成器には，高い生成速度の他に，長時間安定的に乱数を生成できる高い安定性も要求される．そこで我々は構築した物理乱数生成器（周波数雑音検出器）の長期的な安定性について調べることとした．

本章では，半導体レーザの発振周波数の安定度と，実際に生成した物理乱数列の品質の点から物理乱数生成器の安定性について述べる．

8.1 実験方法

8.1.1 半導体レーザの発振周波数

第 7 章で述べたように，周波数弁別器を用いて半導体レーザの周波数雑音を検出する方法では，周波数弁別器のどの位置で，周波数雑音を検出するかが非常に重要である．（半導体レーザの発振周波数と周波数弁別器の関係が重要である．）そのため，物理乱数生成器の安定性は，半導体レーザの発振周波数と周波数弁別器の安定性に強く依存する．よって物理乱数生成器の安定性を評価するために，我々は半導体レーザの発振周波数の安定度を調べることとした．

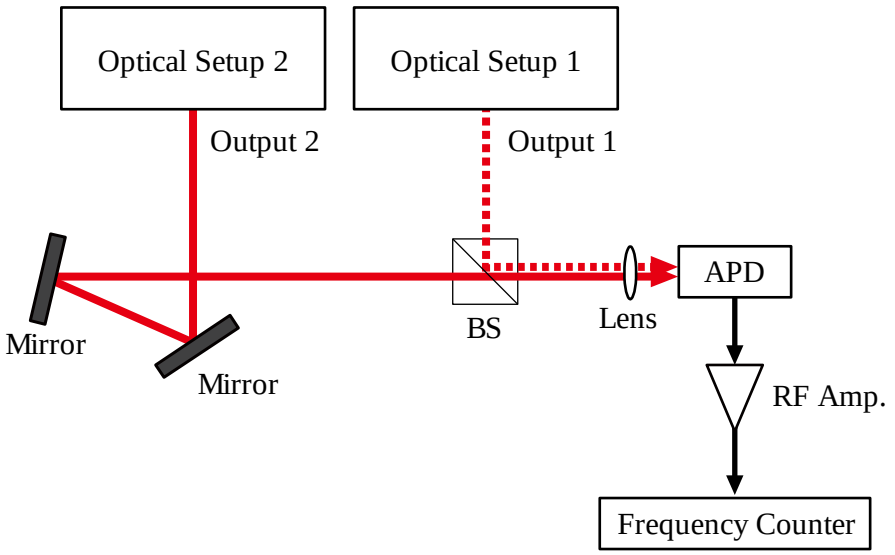


Fig.8-1 Experimental setup for beat signal measurement.

半導体レーザ（Sample Laser）の発振周波数の安定度は，偏光分光信号によって発振周波数が安定化された半導体レーザ（Reference Laser）の周波数安定度から知ることができる．

（周波数雑音を検出するために使用する Sample Laser の発振周波数は，PLL によって Reference Laser（Fig.6-2 参照）の発振周波数に安定化されているため，PLL の安定度が十分高い場合，Sample Laser の発振周波数の安定度は，Reference Laser の発振周波数の安定度とほぼ一致する.）半導体レーザの発振周波数は，およそ 384 THz（波長 780 nm）と非常に高く，直接観測することは困難である．そのためヘテロダインを行って観測可能な周波数に変換して観測する．Fig.8-1 にそのための実験系を示す．Fig.8-1 の Optical Setup 1 と Optical Setup 2 は, それぞれ Rb 原子吸収線の偏光分光信号を使用して発振周波数が安定化された相互に独立した半導体レーザ（Fig.6-4）である．また Fig.8-2 に，その実際に観測された Rb-D_2 吸収線とその偏光分光信号を示す．Optical Setup 1 と Optical Setup 2 の半導体レーザは，それぞれ Fig.8-2 に示された安定化点 S1 と S2 に周波数を安定化する．半導体レーザの発振周波数は，この 2 つの安定化された半導体レーザの光軸を重ねることで得られるビート信号（5.2.3 項を参照）の周波数を計測することで間接的に観測する．ビート信号の周波数は，周波数カウンタを用いて 0.01 s 間隔で，一定期間取得する．ビート信号の周波数安定度は，5.2.1 項で説明したアラン分散の平方根値を算出して評価する．

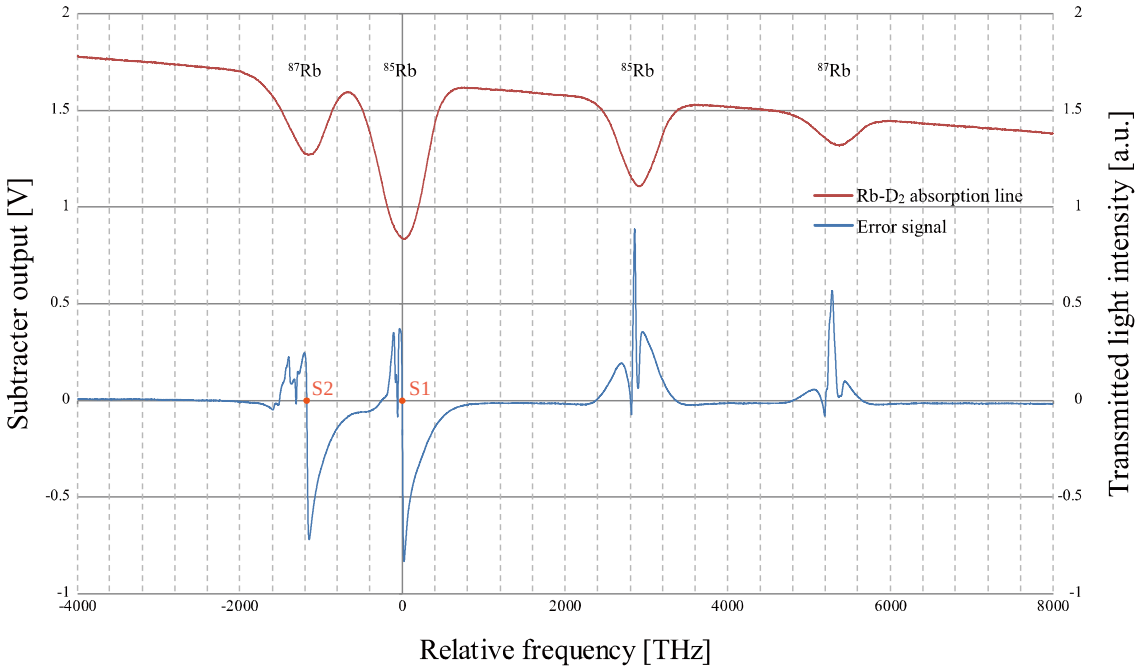


Fig. 8-2 Observed profiles of the Rb-D_2 absorption line and the error signals obtained using polarization spectroscopy.

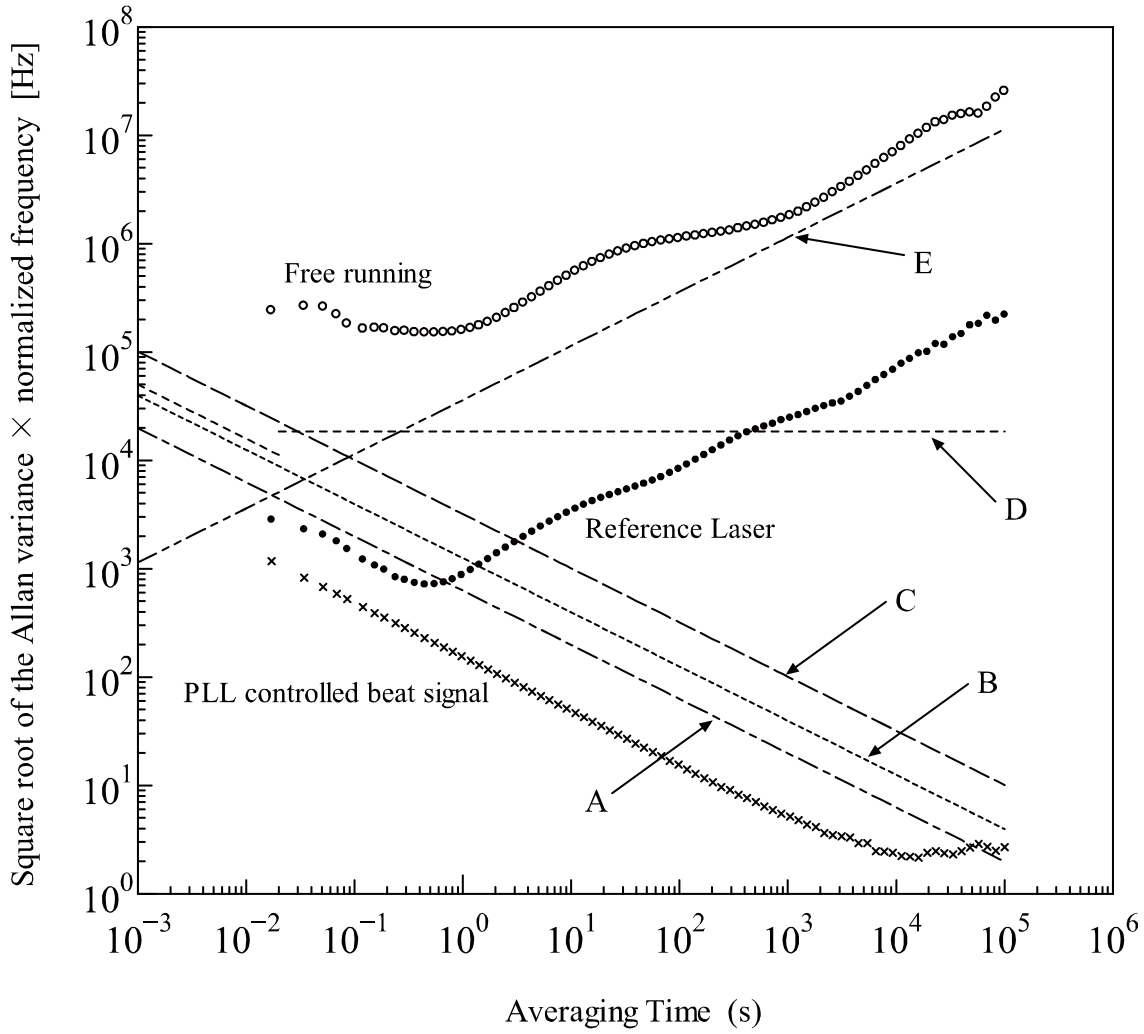
8.1.2 物理乱数の長時間生成

我々は，構築した半導体レーザの周波数雑音検出システムを使って実際に長時間の周波数雑音検出を行い，それで取得された 2 進数データから生成した物理乱数列の時間的な品

質の変化を調べることで本システムの物理乱数生成器としての安定性を評価する．物理乱数列は, 第 6 章, 第 7 章同様に 2 進数データの最上位ビットから生成する. 2 進数データは，デジタルオシロスコープで容量が 10^7 点（10 Mega Sample）のデータを一定の時間間隔（およそ 3.6 秒間隔）でゆっくり取得し，100 時間で合計 1,000 個のデータ（全容量が 10^{12} 点（1 Terra Sample）のデータ）を取得する．これらのデータから 1 Gbit の長さの 2 進数列（物理乱数列）を 1,000 個生成し，さらに生成した時系列準に 100 個単位で SP800-22 の合格率を算出し，その時間的な変化を見る．SP800-22 の合格率は，統計検定によって評価する（4.2.2 項を参照）．SP800-22 のテストパラメータは，Table 6-1 に示した通りである．A/D コンバータのサンプリング速度は，500 MS/s を使用することとする．また XOR 演算のための 2 進数データの遅延時間は 2 μs とする．

8.2 実験結果

8.2 1 半導体レーザの発振周波数安定度



A : spontaneous emission noise (eq.5-36). B : carrier noise (eq.5-37).

C : current noise (eq.5-38). D : current source noise (eq.5-39).

E : temperature noise (eq.5-40).

Fig.8-3 Oscillation frequency stability.

5.2.1 項で説明したようにアラン分散は，一定期間に得られたデータ群を集計して，一定時間内（平均化時間）の平均周波数のばらつき（分散）を計算するもので，平均化時間ごとの周波数安定度を評価することができる．Fig.8-3 に周波数安定度の結果を示す．横軸は平均化時間，縦軸はアラン分散の平方根値に規格化周波数を掛けた値である．●記号（Reference Laser）は，偏光分光信号で周波数安定化された半導体レーザの安定度を示して

いる．○記号（Free running）は周波数が安定化されていないときの半導体レーザの安定度を示している．（Free Running の半導体レーザは，温度制御だけを施した状態である．）また×記号は PLL で制御されたビート信号の周波数安定度を示している．

実験結果から，Free running の最大安定度は，平均化時間 1×10^{-1}s～1×10^{0}s 付近においておよそ 100 kHz，最低安定度は，平均化時間 1×10^{5} s（約 28 時間）付近において 20 kHz 程度であることが分かる．また実験結果から Reference Laser が，Free running よりも定常的に 1 桁以上安定度がよいことが分かる．Reference Laser の最大安定度は，平均化時間 4×10^{-1}s 付近でおよそ 700 Hz 程度の変動幅である．また平均化時間 4×10^{-1} s 以上においてランダムウォークの特徴を示し，徐々に安定度が劣化している．最低安定度は，平均化時間 1×10^{5}s（約 28 時間）でおよそ 200 kHz である．また Reference Laser は，平均化時間 6×10^{-1} s 以下において，白色雑音の特性を有しほぼ理論限界に近い周波数安定度を達成している．

高いレベルで Reference Laser の発振周波数の安定度に Sample Laser の発振周波数を追随させるためには，PLL で制御されたビート信号の周波数安定度が Reference Laser の発振周波数安定度より高くなければならない．実験結果から PLL で制御されたビート信号の周波数安定度は，Reference Laser の周波数安定度に比べ，安定度が高いことが分かる．よって PLL 制御を用いた周波数オフセットのシステムは十分な安定度を達成している．

8.2.2 物理乱数の検定合格率

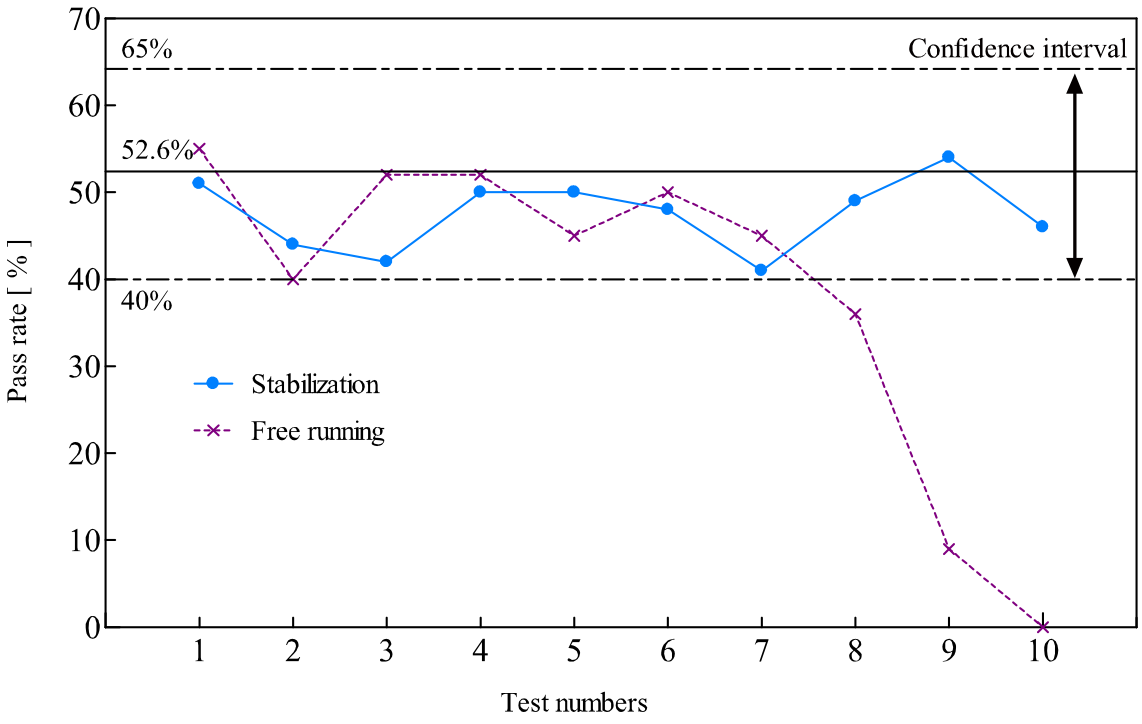


Fig.8-4 Change of the pass rate.

Fig.8-4 は，物理乱数生成器で生成される物理乱数列の品質（SP800-22 の合格率）の時間的変化を示している．縦軸は SP800-22 の合格率を示し，横軸は生成した時系列準に振り分けた物理乱数列の番号を示している．また dot dash 線で囲まれた区間は，SP800-22 の合格率を統計的に評価した場合の信頼区間（4.2.2 項を参照）を示している．実験は，半導体レーザの発振周波数を制御した状態と無制御の状態の 2 条件について比較する．

図から半導体レーザの発振周波数が安定化されている時は，物理乱数列の SP800-22 の合格率がすべて信頼区間内にあり，物理乱数列が安定的に生成されていることが分かる．一方フリーランニング時は，8 番目～10 番目の物理乱数列の合格率が急激に悪くなり，その合格率が信頼区間外になっていいることが分かる．

8.3 考察

Fig.8-4 から半導体レーザの発振周波数が安定化されている場合は，物理乱数列が長時間安定的に生成されていることが分かる．このことは我々が予想した通り物理乱数生成器の安定性が，半導体レーザの発振周波数の安定度に依存することを示している．一方，フリーランニング時は，8 番目～10 番目の物理乱数列の合格率が急激に悪くなり，物理乱数列が安定的に生成されていないことが分かる．これは半導体レーザの発振周波数が変化して周波数弁別器の最適な位置からずれてしまったことが原因であると考えられる．第 7 章の結果から分かるように周波数弁別器において物理乱数を高い品質で生成できる領域の幅は，最大でも 60 MHz 程度である．よってフリーランニング状態の半導体レーザの発振周波数は，80 時間～100 時間（8 番目～10 番目の物理乱数列を生成するための 2 進数データが周波数雑音検出器から検出されている時間）で 60 MHz 以上発振周波数が変動したと考えられる．

また，Fig.8-3 の結果からフリーランニング時の半導体レーザの発振周波数の安定度は，平均化時間 1×10^5 s（約 28 時間）において，およそ 20 MHz の変動をしている．この結果はフリーランニング時の半導体レーザの発振周波数が，約 112 時間でおよそ 80 MHz ほど変動する可能性を示している．また，この予想は Fig8-4 の結果と整合性がある．

第 9 章 並列生成と結合生成における物理乱数の生成速度

第 6 章，7 章，8 章では，8 ビットの 2 進数データの最上位ビットを用いた物理乱数の生成方法を用いて物理乱数を生成した．しかしその生成速度は，半導体レーザの周波数雑音の帯域や周波数弁別器の帯域に依存するため，それぞれファブリ・ペロータイプの半導体レーザや Rb 吸収線を使用した場合，その生成速度は数百 Mb/s 程度が限界であった．そこで我々は第 4 章で説明した 2 進数データの複数ビットを使用した物理乱数のマルチビット生成方式を用いて，超高速な物理乱数生成を試みることとした．

9.1 実験方法

Fig.9-1 に実験の概要が示されている．実験では，1 台の Frequency noise detecting system から取得された Binary Data を用いて物理乱数が生成される．Binary Data は，各生成方式の生成速度を比較するために, A/D コンバータからサンプリングレート 500 MS/s, 1 GS/s, 2 GS/s, 5 GS/s，10 GS/s，20 GS/s と 40 GS/s の 7 通りの速度で取得される．サンプリングレートが 500 MS/s，1 GS/s，2 GS/s である時，RF-Amp.2 と 3 に Bandwidth 0.1～1,000 MHz の RF-Amp.（Mini-Circuits, Low Noise Amplifier ZFL-1000LN+）が使用される．またサンプリングレートが 5 GS/s, 10 GS/s, 20 GS/s, 40 GS/s である時, RF-Amp.2 と 3 に Bandwidth 0.3～14,000 MHz の RF Amp.（Mini-Circuits, Ultra Wide Bandwidth Amplifier ZX60-14012L+）が使用される．XOR 演算と RXOR 演算の計算と各乱数生成の処理は，パーソナルコンピュータによって行われる．我々は，XOR method と RXOR method の性能を比較するために，これらの方法に使用される Original Data1 に共通の Binary Data を使用する．また RXOR method のための Original Data2 には，1 台の Frequency noise detecting system から別々の時間に取得された Binary Data が使用される．（すなわち，乱数の生成速度は，サンプリング速度の 1/2 になる．）また本実験では，XOR method のための XOR Data は，1k Bytes（2 進数の各桁においては 1k bits）の遅延によって構築された Delay Data から生成されている．我々は，XOR method と RXOR method にそれぞれ並列生成方式（Parallel generation method）と結合生成方式（Coupling generation method）を適用した全 4 種類の方法から生成された物理乱数の品質を，統計検定 SP 800-22 によって評価する．

我々は，SP800-22 による乱数の品質評価を厳密に行うため SP800-22 を 100 回実行して，その合格率を二項検定によって統計的に評価することとした．この二項検定の帰無仮説は，「生成された物理乱数列が，理想的な乱数列である．」である．我々は有意水準 1 %と 0.1 %の 2 段階の水準について二項検定を行うこととした．これらの有意水準から統計的に有意でない範囲（信頼区間）を計算すると，99 %信頼区間は，40≦X≦65，99.9 %信頼区間は，36≦X≦69 である．確率変数 X は，物理乱数が SP800-22 を合格した回数である．これらの信頼区間が，生成された物理乱数の品質の目安である．また本研究で我々は，乱数の生成

速度を決定するために，合格率が 99.9 %信頼区間内である場合を理想的な乱数生成の成功と判断することとした．

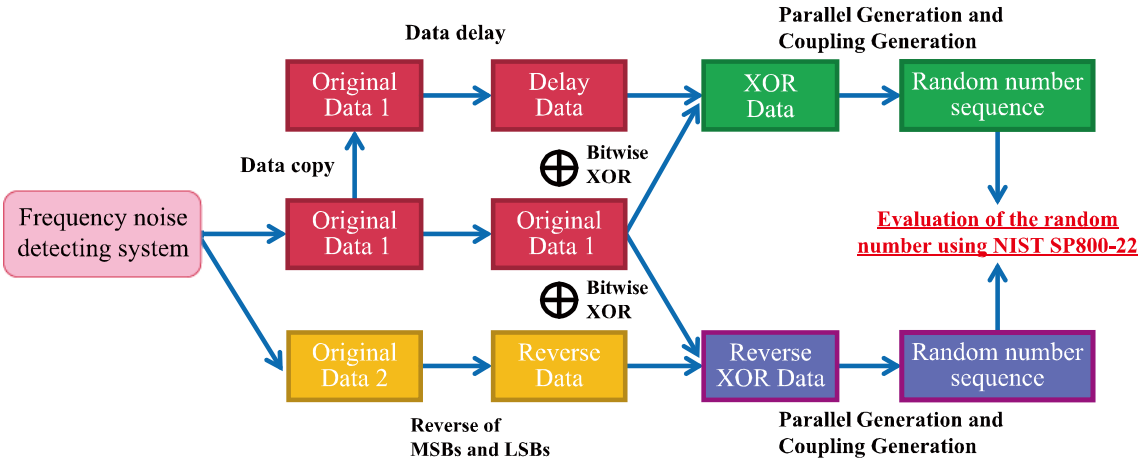


Fig.9-1 Flow of the experiment.

9.2 実験結果

9.2.1 XOR method の実験結果

Table 9-1 は，XOR method によって生成された物理乱数の SP800-22 の合格率を示している．そして Table 9-1(a)と(b)は，それぞれ Parallel generation method と Coupling generation method の結果を示している．合格率がレベル 1 %で有意な場合，合格率の右横に*の印が記されている．また合格率がレベル 0.1 %で有意な場合、合格率の右横に**の印が記されている．（すなわち，合格率が 99 %信頼区間内であれば，実験結果の合格率の右横に印が記されない．合格率が 99 %信頼区間外で 99.9 %信頼区間内であれば，合格率の右横に*の印が記される．合格率が 99.9 %信頼区間外であれば，合格率の右横に**の印が記される．）Parallel generation method の実験結果は，XOR Data の $r0_{xor}$bit から $r7_{xor}$bit までの各桁から生成された乱数列の合格率が示されている．$r7_{xor}$ と $r0_{xor}$ は，XOR Data の MSB と LSB である．Table 9-1(a)よりサンプリングレート 500 MS/s における 8LSBs, 1 GS/s と 2 GS/s と 5 GS/s における 6LSBs, 10 GS/s と 20 GS/s における 5LSBs，40 GS/s における 3LSBs からそれぞれ並列生成された乱数列の合格率が，おおむね 99 %信頼区間に含まれていることが分かる．ただし，サンプリングレート 1 GS/s における $r1_{xor}$bit，2 GS/s における $r1_{xor}$bit と $r2_{xor}$bit と $r4_{xor}$bit，5 GS/s における $r5_{xor}$bit からそれぞれ生成された乱数列の合格率は，レベル 1 %で有意である．よって，これらの桁から生成された乱数列の品質は，ばらつきを持つが，我々はおおむね理想的な乱数列が生成されていると判断した．一方，サンプリングレーザ 1 GS/s，2 GS/s，5 GS/s における 2MSBs，10 GS/s，20 GS/s における 3MSBs，40 GS/s における 5MSBs からそれぞれ並列生成された乱数列の合格率は，0 %であった．合格率 0 %は，99.9 %信頼区間の外（すなわり，合格率はレベル 0.1 %で有意である．）であるため，この場合の乱数列は，統計的には理想的な乱数列である可能性が低いと判断される．この実験結果は，サンプリングレートが速くなるにつれて MSBs を source として生成された乱数列の品質が，低下することを示していることが分かる．

Coupling generation method の実験結果は，2LSBs から 8LSBs までの各 LSBs から生成された乱数列の検定合格率が示されている．Table 9-1(b)よりサンプリングレーザ 500 MS/s，1 GS/s，2 GS/s における 2LSBs から 6LSBs までの各 LSBs，5 GS/s における 2LSBs と 4LSBs から 5LSBs までの各 LSBs，10 GS/s における 2LSBs から 4LSBs までの各 LSBs と 6LSBs，20 GS/s における 3LSBs と 4LSBs，40 GS/s における 2LSBs からそれぞれ結合生成された乱数列の合格率が，99 %信頼区間に含まれていることが分かる．ただし，サンプリングレート 5 GS/s における 3LSBs，10 GS/s における 5LSBs，20 GS/s における 2LSBs から結合生成された乱数列の合格率は，レベル 1 %で有意である．一方，サンプリングレート 500 MS/s, 1 GS/s, 2 GS/s, 5 GS/s, 10 GS/s における 8LSBs と 7LSBs, 20 GS/s における 8LSBs から 5LSBs までの各 LSBs，40 GS/s における 8LSBs から 3LSBs までの各 LSBs からそれぞれ結合生成

された乱数列の合格率は，0 %である．この結果は，サンプリングレートが速くなるにつれて, より多くの MSBs が生成に使用された乱数の品質が低下していることを意味している．この特徴は，Parallel generation method の結果の特徴と一致する．

Table 9-2 は，XOR method から生成された物理乱数の品質評価の結果から算出された各サンプリングレートにおける理想的な乱数の生成速度を示している．Parallel generation method における生成速度は，合格率が 99.9 %信頼区間に含まれた乱数（桁）の個数×サンプリングレートから算出される．また Coupling generation method における生成速度は，合格率が 99.9 %信頼区間に含まれた乱数（各 LSBs）の中で最も大きな LSBs の値×サンプリングレート×1/2 から算出される．Table 9-2 より Parallel generation method における乱数の最大生成速度は，サンプリングレート 40 GS/s の時の 120 Gb/s（40 Gb/s×3LSBs）であることが分かる．また Coupling generation method における乱数の最大生成速度は，サンプリングレート 20 GS/s と 40 GS/s の時の 80 Gb/s（20 Gb/s×4LSBs and 40 Gb/s×2LSBs）であることが分かる．これらの乱数の最大生成速度は，単ビット乱数生成における乱数の最大生成速度（500 Mb/s）と比較して，Parallel generation method の場合で 240 倍，Coupling generation method の場合で 160 倍の速度である．

Table 9-1. The number of the passes of the random number generated by XOR method. (a) Parallel generation method in the XOR method of 1k delay.

	Sampling Rate (GS/s)						
Binary Digit	0.5	1	2	5	10	20	40
$r7_{xor}$	47	0**	0**	0**	0**	0**	0**
$r6_{xor}$	44	0**	0**	0**	0**	0**	0**
$r5_{xor}$	45	41	58	39*	0**	0**	0**
$r4_{xor}$	47	45	39*	44	41	41	0**
$r3_{xor}$	52	52	47	46	50	44	0**
$r2_{xor}$	54	50	38*	51	46	47	45
$r1_{xor}$	46	39*	37*	49	46	54	51
$r0_{xor}$	54	47	53	48	53	50	50

(b) Coupling generation method in the XOR method of 1k delay.

	Sampling Rate (GS/s)						
LSBs	0.5	1	2	5	10	20	40
8	0**	0**	0**	0**	0**	0**	0**
7	0**	0**	0**	0**	0**	0**	0**
6	43	46	44	50	47	0**	0**
5	51	49	44	53	39*	0**	0**
4	57	51	44	43	54	41	0**
3	41	51	55	36*	49	48	0**
2	42	50	49	54	50	39*	52

Table 9-2. The generation speed (Gbits/s) of the random number generated by XOR method.

	Sampling Rate (GS/s)						
Generation method	0.5	1	2	5	10	20	40
Parallel generation	4	6	12	30	50	100	120
Coupling generation	3	6	12	30	60	80	80

9.2.2 RXOR method の実験結果

Table 9-3 は，RXOR method によって生成された物理乱数の SP800-22 における合格数を示している．Table 9-3(a)は Parallel generation method の結果を示している．また Table 9-3(b)は Coupling generation method の結果を示している．Parallel generation method の実験結果は，RXOR Data の $r0_1$ xor $r7_2$bit から $r7_1$ xor $r0_2$bit までの各桁から生成された乱数列の合格率が示されている．$r7_1$ xor $r0_2$ と $r0_1$ xor $r7_2$ は，RXOR method の MSB と LSB である．Table 9-3(a)より 40 GS/s 以外のサンプリングレートにおける 8LSBs からそれぞれ並列生成された乱数列の合格率が，おおむね 99 %信頼区間に含まれていることが分かる．すなわち，500 MS/s から 20 GS/s までのサンプリングレートにおいて，すべての桁から並列生成された乱数列が，理想的な乱数列であると判断される．ただし，サンプリングレート 500 MS/s，1 GS/s における $r6_1$ xor $r1_2$bit から生成された乱数列の合格率は，レベル 1 %で有意である．一方，サンプリングレート 40 GS/s では，2MSBs と 2LSBs からそれぞれ並列生成された乱数列の合格率が，99.9 %信頼区間に含まれているが，それら以外の桁から並列生成された乱数列の合格

率は，0 %であることが分かる．このような結果になった理由は，高速なサンプリングレートにおいては，MSBs に加え中間ビットの無秩序性も劣化するため，中間ビット間の XOR 演算で，中間ビットの劣る無秩序性を相殺することができなかったためと予想される．この現象は，XOR method では起こらない RXOR method の特有の現象である．

Coupling generation method の実験結果は，2LSBs から 8LSBs までの各 LSBs から生成された乱数列の合格率が示されている．Table 9-3(b)より 40 GS/s 以外のサンプリングレートにおける 2LSBs から 8LSBs までの各 LSBs からそれぞれ結合生成された乱数列の合格率が，おおむね 99 %信頼区間に含まれていることが分かる．すなわち，500 MS/s から 20 GS/s までのサンプリングレートにおいて，すべての桁から結合生成された乱数列が，理想的な乱数列であると判断される．500 MS/s から 20 GS/s までのサンプリングレートで生成されたすべての乱数列の品質が良好である Coupling generation method の特徴は，Parallel generation method の結果の特徴と一致する．ただし，サンプリングレート 2 GS/s における 8LSBs，10 GS/s における 2LSBs から結合生成された乱数列の合格率は，レベル 1 %で有意である．一方，サンプリングレート 40 GS/s では，2LSBs から結合生成された乱数列の合格率が，99 %信頼区間に含まれているが, それ以外の各 LSBs から結合生成された乱数列の合格率は, 0 %であることが分かる．

Table 9-4 は，RXOR method の実験結果から算出された物理乱数の生成速度を示している．Table 9-4 より Parallel generation method の乱数の最大生成速度は，サンプリングレート 20 GS/s と 40 GS/s の時の 80 Gb/s（20 Gb/s×1/2×8LSBs and 40 Gb/s×1/2×(2MSBs+2LSBs)）であることが分かる．また Coupling generation method の乱数の最大生成速度は，サンプリングレート 20 GS/s の時の 80 Gb/s（20 Gb/s×1/2×8LSBs）であることが分かる．これらの乱数の最大生成速度は，単ビット乱数生成の 160 倍の速度である．

Table 9-3. The number of the passes of the random number generated by RXOR method. (a) Parallel generation method in the RXOR method.

	Sampling Rate (GS/s)						
Binary Digit	0.5	1	2	5	10	20	40
$r7_{1xor}r0_2$	41	44	40	48	56	45	39*
$r6_{1xor}r1_2$	38*	38*	54	48	44	42	39*
$r5_{1xor}r2_2$	51	42	51	46	44	52	0**
$r4_{1xor}r3_2$	44	52	55	48	48	47	0**
$r3_{1xor}r4_2$	58	48	51	49	40	46	0**
$r2_{1xor}r5_2$	49	45	43	42	44	47	0**
$r1_{1xor}r6_2$	47	56	42	49	55	55	54
$r0_{1xor}r7_2$	43	47	46	40	49	51	46

(b) Coupling generation method in the RXOR.

	Sampling Rate (GS/s)						
LSBs	0.5	1	2	5	10	20	40
8	52	51	37*	52	47	45	0**
7	40	59	46	40	51	53	0**
6	42	46	49	43	41	45	0**
5	43	54	40	42	45	47	0**
4	54	51	48	47	47	45	0**
3	46	43	54	42	47	40	0**
2	45	49	42	53	41	47	40

Table 9-4. The generation speed (Gbits/s) of the random number generated by RXOR method.

	Sampling Rate (GS/s)						
Generation method	0.5	1	2	5	10	20	40
Parallel generation	2	4	8	20	40	80	80
Coupling generation	2	4	8	20	40	80	40

9.2.3 パワースペクトル

Fig.9-2 に、physical-random number を生成するための source である半導体レーザの周波数雑音（透過光強度雑音）のパワースペクトルが示されている．パワースペクトルは，サンプリングレート 40 GS/s で取得した Data から，FFT によって算出された．図に示されている Intensity noise は，半導体レーザの Intensity noise を示している．また図に示されている No signal は, Background noise を示している. パワースペクトルは, A/D コンバータの Analog bandwidth が 4 GHz であるため，Frequency noise と Intensity noise，No signal も 4 GHz 付近から急激にそのパワーを減少させる．図から Frequency noise は，およそ 300 MHz 付近まで，ほぼ白色雑音の性質を有し，そこから急激にパワーが小さくなっていることが分かる．これは今回使用した周波数弁別器の帯域による制限である．また，およそ 3 GHz 付近に，緩和振動周波数の共鳴ピークが観測されている．

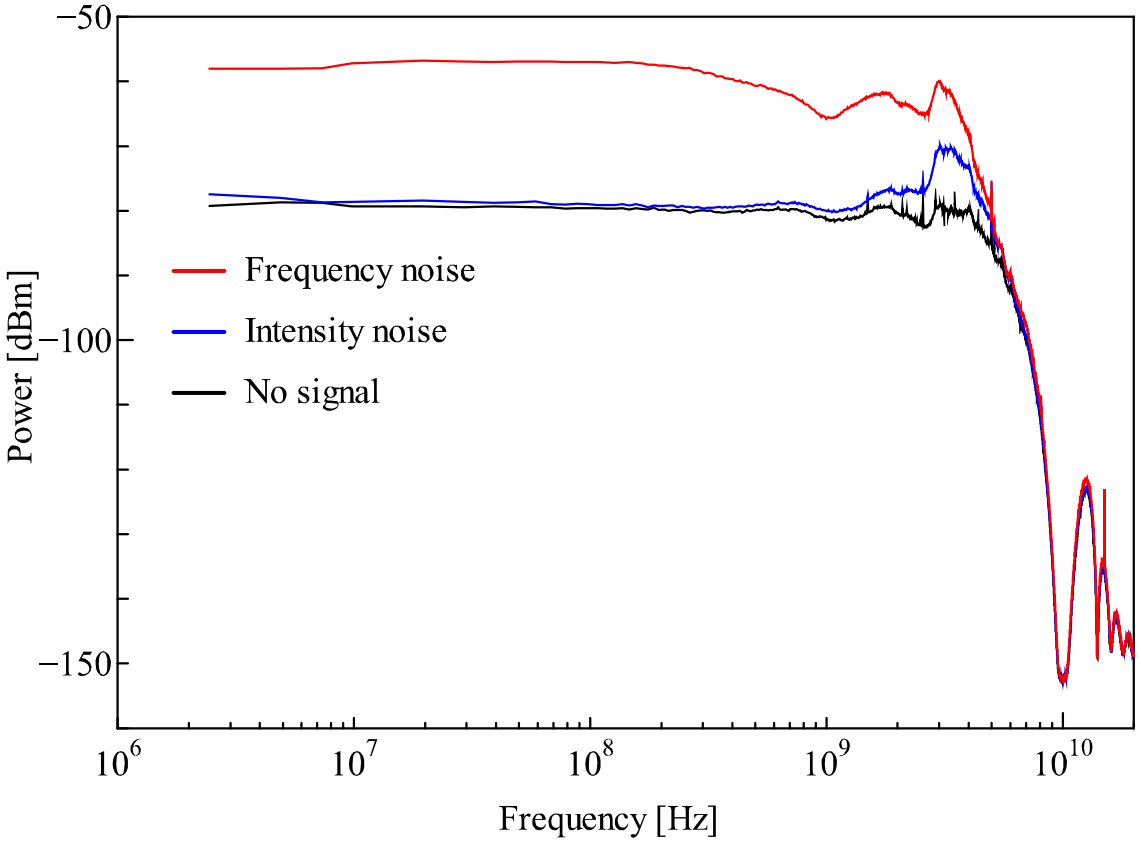


Fig.9-2 Power spectrum of DL's FM noise.

9.3 考察

ここで，9.2 節で得られた実験結果に対する考察を行う．

9.3.1 XOR method と RXOR method の比較

実験結果から半導体レーザの周波数雑音を源にして XOR method と RXOR method を実行することで，理想的な乱数が高速に生成できることが確認された．一方これらの実験結果の間には，明らかな違いも確認された．XOR method では，サンプリングレートが速くなるにつれて MSBs（上位の桁）を源として生成された乱数列（Parallel generation method）やより多くの LSBs が生成に使用された乱数列（Coupling generation method）の品質が徐々に低下した．それに対して RXOR method では，サンプリングレート 40 GS/s 以外の速度において各方式から生成されたすべての乱数列の品質が，低下しなかった．この結果は，RXOR method の MSBs の劣る無秩序性を相殺する効果が発揮されたことを示している．したがって，2 進数のすべての桁を理想的な乱数の生成に利用できる点で，XOR method に対して RXOR method の方が優れている．一方，物理乱数の最大生成速度は，RXOR method と比べて XOR method の方が高速であった．この結果は，RXOR method の乱数の生成速度が，AD コンバータのサンプリングレートの 1/2 になってしまうことが原因である．したがって，基本的に乱数の生成速度に関しては，XOR method に対して RXOR method の方が優れているわけではない．そのため，本研究の条件下で最も高速に物理乱数を生成できる方法は，XOR method であると，我々は結論付ける．

9.3.2 並列生成方式と結合生成方式の比較

本実験結果から Parallel generation method と Coupling generation method が，ともに乱数の生成速度を飛躍的に向上させることが確認された．しかし XOR method における Parallel generation method と Coupling generation method の実験結果を比較すると，これらの生成方式は, その生成速度に差があることが分かる.（具体的には, サンプリングレートが, 500 MS/s, 20 GS/s，40 GS/s である時，Parallel generation method と Coupling generation method のそれぞれの最大の乱数生成速度に差が確認された.）特に注目すべきポイントは，サンプリングレート 500MS/s における実験結果である．Parallel generation method では，2 進数のすべての桁から高い品質の乱数が並列生成されるのに対し，Coupling generation method では，8LSBs（2 進数のすべての桁)から高い品質の乱数が結合生成されない. 我々は, この原因を Binary Data の各桁の独立性が低いためであると考えた．Fig.8-3 はサンプリングレート 500 MS/s によって取得された Binary Data の各桁から生成された 2 進数列の間の相関係数の絶対値を示している．Fig.8-3 の r7 と r0 は，Binary Data の MSB と LSB を示している．図から r7 は，他の

桁に対して高い相関を示していることが分かる．具体的には r7 は，r6，r5，r4 に対して高い相関を示している．この結果は，r7 が他の桁に対して独立性が低いことを示している．よって Parallel generation method と Coupling generation method の生成速度の差は，この r7 の独立性の低さが原因であると考えられる．また r7 の独立性が低いことは，Parallel generation method によって各桁から生成された乱数列の間の独立性も低いことを意味している．この事実は乱数の用途によっては，大きな問題になる．

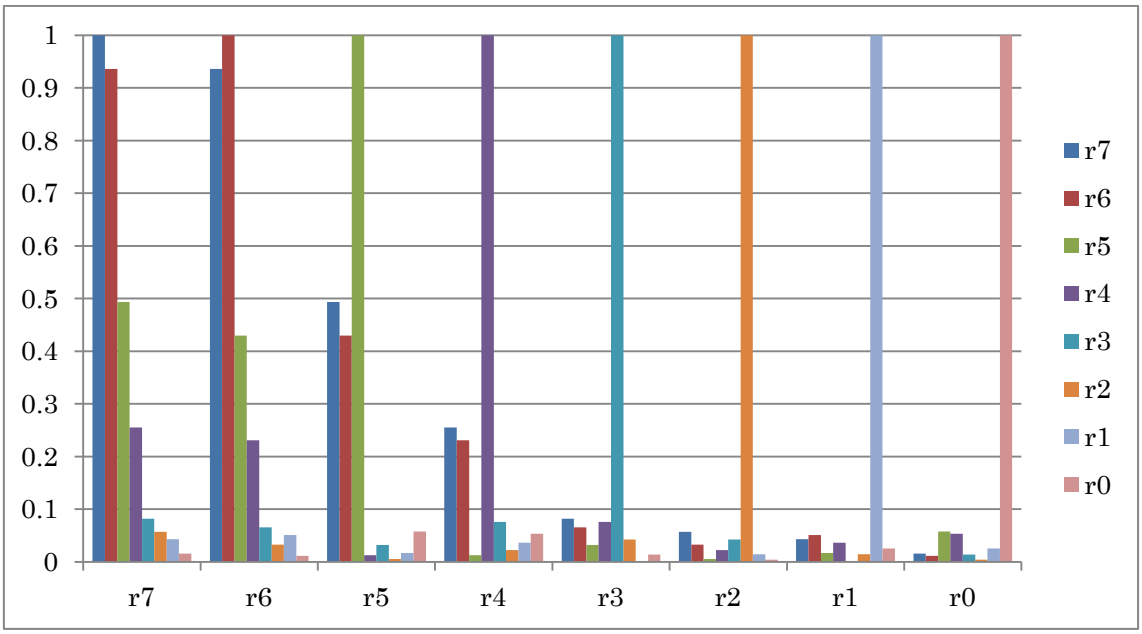


Fig.9-3 The comparison of the correlation coefficient between each digit.

9.3.3 Improved XOR method と Improved RXOR method

我々は，r7 の他の桁に対する低い独立性が，生成される乱数の品質に影響することを解消するために Binary Data の各桁に異なる Delay を施す方法を試してみた．Fig.8-4 は，Binary Data の具体的な操作の方法を示している．Original Data の遅延は 2 進数の各桁に対して 1bit 単位で行われ，Delay Data は，遅延を施して減った先頭の Data を遅延によって余った末尾の Data で補うことで生成される．Data の遅延量は，2 進数の各桁に異なる Delay が与えられている．また上位ビットであるほど大きな Delay が与えられている．Fig.8-4 では，各桁の Data の遅延量に 1 ビットずつの差が与えられているが，本研究では 1,000 ビットずつの差を与えて Delay Data を生成した．我々は，この Delay Data と Original Data との間で XOR 演算や RXOR 演算を行い，物理乱数列の源となる Binary Data を生成する．我々は，これらの生成方式を通常の XOR method，RXOR method と区別するために，前者を Improved XOR method，後者を Improved RXOR method と呼ぶこととした．我々は，これらの方式を用いて

Coupling generation method を試してみた．一方，2 進数の各桁から物理乱数を並列生成する Parallel generation method は，Improved XOR method と Improved RXOR method の効果が期待できない（影響を受けない）ため，我々はそれを試す必要がないと判断した．

Table 9-5 は，Improved XOR method と Improved RXOR method によって生成された物理乱数の各サンプリングレートにおける SP800-22 の合格率を示している．また Table 9-6 は，XOR method，RXOR method，Improved XOR method と Improved RXOR method の合格率の結果から算出された物理乱数の生成速度を示している．Table 9-5(a)より Improved XOR method の各サンプリングレートにおける結果が，XOR method における Coupling generation method の結果と比較して向上していることが分かる．具体的には，XOR method における Coupling generation method において 99 %信頼区間に含まれなかったサンプリングレート 500 MS/s，1 GS/s における 8LSBs，2 GS/s における 7LSBs，20 GS/s における 5LSBs，40 GS/s における 3LSBs から結合生成された乱数列が，99 %信頼区間に含まれるようになった．（すなわち，理想的な乱数列が生成されるようになった．）このように，乱数の生成速度もサンプリングレート 500 MS/s，1 GS/s，2 GS/s，20 GS/s，40 GS/s において向上した．また乱数の最大生成速度は，80 Gb/s（20 Gb/s×4LSBs and 40 Gb/s×2LSBs）から 160 Gb/s（40 Gb/s×4LSBs）に向上している．一方，Improved XOR method の各サンプリングレートにおける乱数の生成速度と XOR method における Parallel generation method のそれを比較すると，Table 9-6 (a)より各サンプリングレートにおける生成速度が，大きく向上していることが分かる．具体的には，サンプリングレート 1 GS/s，2 GS/s，10 GS/s，40 GS/s において乱数の生成速度が向上した．この結果は，Improved XOR method が，r7 の低い独立性によって生成される乱数へ与えられる影響を解消したためと考えられる．

Table 9-5 (b)は，Improved RXOR method の各サンプリングレートにおける物理乱数の SP800-22 の合格率を示している．Table 9-5 (b)より Improved RXOR method のサンプリングレート 40 GS/s における結果が，RXOR method の 40 GS/s における結果と比較して大きく向上していることが分かる．具体的には，8LSBs，7LSBs と 6LSBs から結合生成された乱数列が，99 %信頼区間に含まれている．（すなわち，理想的な乱数列が生成されている．）このように，Improved RXOR method の最大生成速度は，160 Gb/s（40 Gb/s×1/2×8LSBs）に向上した．

Improved XOR method と Improved RXOR method の最大生成速度は，本研究で最速の乱数の生成速度である．

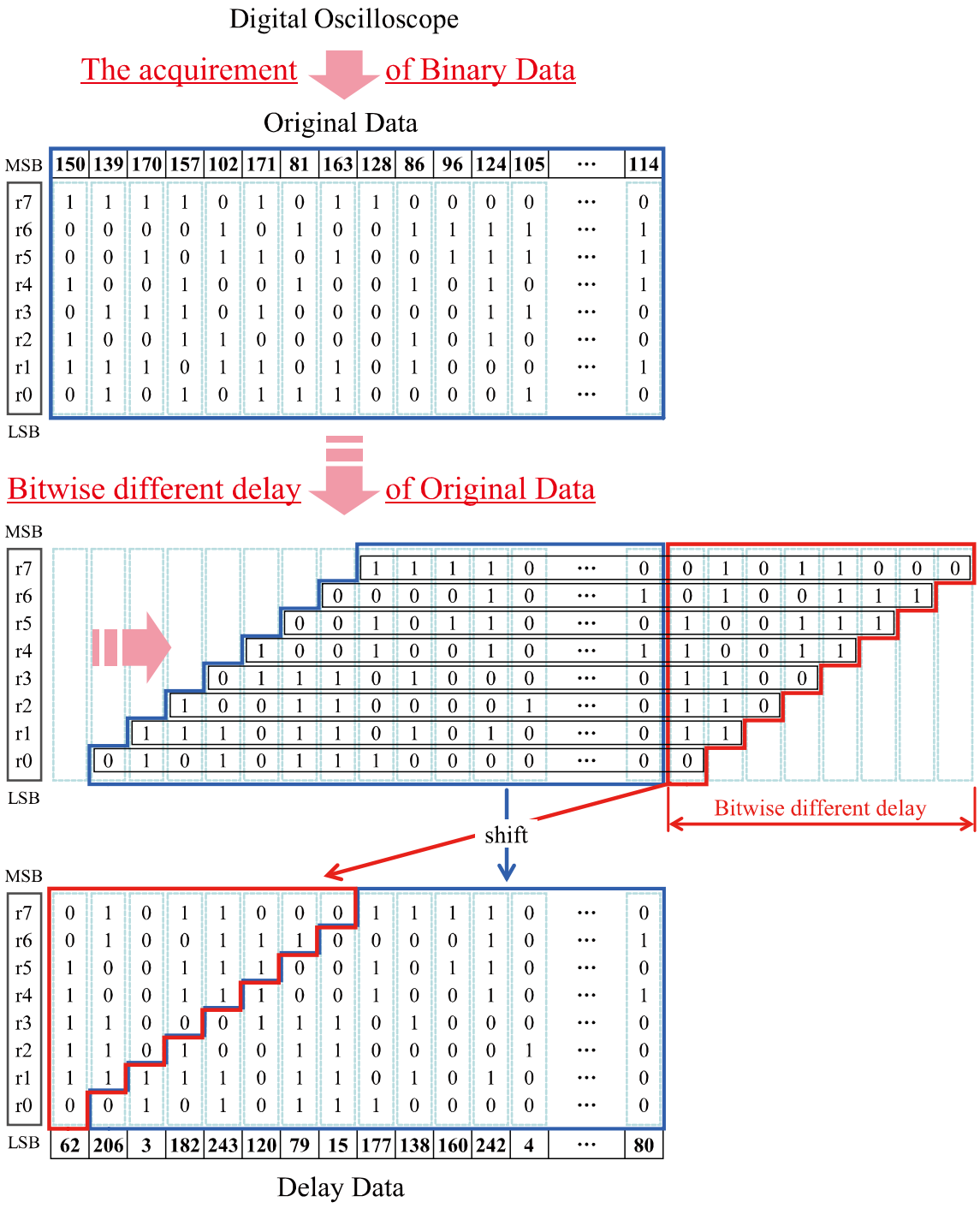


Fig.9-4 Bitwise different delay of Original Data.

Table 9-5. Pass number of random number test in the improved XOR method and improved RXOR method. (a) Coupling generation method in the improved XOR method of 8k～1k delay.

	Sampling Rate (GS/s)						
LSBs	0.5	1	2	5	10	20	40
8	44	53	0**	0**	0**	0**	0**
7	45	41	44	0**	0**	0**	0**
6	45	47	53	47	50	0**	0**
5	54	40	44	39*	49	48	0**
4	36*	54	48	46	42	46	55
3	49	37*	51	49	49	40	55
2	46	52	51	44	39*	47	45

(b) Coupling generation method in the improved RXOR method of 7k～0 delay.

	Sampling Rate (GS/s)						
LSBs	0.5	1	2	5	10	20	40
8	47	40	49	47	58	50	42
7	45	44	39*	55	53	46	43
6	41	42	47	44	44	50	44
5	49	38*	50	41	43	52	0**
4	44	43	43	50	45	50	0**
3	41	40	48	41	49	45	0**
2	50	46	46	49	44	52	47

Table 9-6. The generation speed (Gbits/s) of the random number generated by improved XOR method and improved RXOR method. (a) The generation speed of the random number generated by XOR method and improved XOR method.

	Sampling Rate (GS/s)						
Generation method	0.5	1	2	5	10	20	40
Parallel generation	4	6	12	30	50	100	120
Coupling generation	3	6	12	30	50	80	80
Improved XOR	4	8	14	30	60	100	160

(b) The generation speed of the random number generated by RXOR method and improved RXOR method.

	Sampling Rate (GS/s)						
Generation method	0.5	1	2	5	10	20	40
Parallel generation	2	4	8	20	40	80	80
Coupling generation	2	4	8	20	40	80	40
Improved RXOR	2	4	8	20	40	80	160

9.3.4 パワースペクトルと生成速度の比較

物理乱数の生成速度は，源の速度に依存する．また一般的な単ビットを用いた物理乱数の生成方法（XOR method における Parallel generation method による $r7_{xor}$）では，源となる雑音信号が白色雑音の性質を有している必要がある．本研究で使用した半導体レーザは，およそ 3 GHz（Fig.9-2）の帯域（緩和振動周波数の共鳴ピークが 3 GHz）において周波数雑音を持ち，周波数弁別器の帯域の制限によって，およそ 300 MHz（Fig.9-2）の帯域において白色雑音の性質を有していた．この事実から本研究では，単ビットを用いた物理乱数の生成方式において，最大 600 Mb/s（300 MHz×2）の速度で物理乱数が，生成可能であると予想される．実際に，我々は 500 Mb/s の生成速度を達成した．この速度は，ほぼ予想と一致する結果である．この単ビットによる物理乱数の生成方法で，更に生成速度を向上させるためには，源となる雑音信号の白色雑音の性質を有する帯域を伸ばす必要がある．そのためには，より高速な源を使用することと，帯域の広い周波数弁別器を使用することが必要である．高速な源としては，本研究で使用した Fabry-Perot type の半導体レーザ（一般的に数 GHz の帯域において周波数雑音を持つ）の数倍の帯域の周波数雑音を持つ半導体レーザの

一種である Vertical cavity surface emitting laser（VCSEL）が候補としてあげられる．また周波数弁別器は，帯域を自由に選択できるファブリペロー共振器やエタロンが使用可能である．ただし，半導体レーザの周波数雑音には，緩和振動周波数において共鳴ピークが存在するため，白色雑音の性質を持つ帯域は，周波数雑音の全体の帯域を超えることができない．よってこの生成方式では，物理乱数の生成速度も周波数雑音の帯域を超えることができない．

一方，多ビットを用いた物理乱数の生成方式は，単ビットを用いたそれの生成方式と比べ，源となる雑音信号に厳密な白色雑音としての性質を要求しない．また源の速度を超えた速度で物理乱数を生成することが可能である．実際に実験で，我々は 160 Gb/s の生成速度を達成した．この生成速度は，源の速度と比べて，極めて高速である．また，源として VCSEL を使用することで，単ビット用いた物理乱数の生成方式では，最大で 10 Gb/s 程度の生成速度が限界と考えられるが，この生成方式では，最大で 160 Gb/s の数倍の速度が期待できる，これは非常に大きなメリットである．

第 10 章 まとめ

今回，我々は高速に物理乱数を生成するために，半導体レーザの発振周波数を周波数弁別器によって検出し，得られた 2 進数データから高速に物理乱数列を生成することに成功した．また生成された物理乱数列は，統計検定 SP800-22 に合格する高い品質を確保することができた．

我々は，物理乱数を高速かつ安定的に生成するために，良質な物理乱数を生成するための条件について調べる実験を行った．その結果，半導体レーザの周波数雑音から良質な物理乱数を生成するためには，半導体レーザの中心周波数が $Rb\text{-}D_2$ 吸収線の限られた周波数領域内に存在する必要があることが分かった．本実験で，我々はこの最適な領域に半導体レーザの中心周波数を設定することによって A/D コンバータから得られた 2 進数データの最上ビットから 500 Mb/s の速度で良質な物理乱数を生成することに成功した．

また我々は，本研究で物理乱数を安定的に生成するために半導体レーザの発振周波数を安定化した．半導体レーザの発振周波数は，$Rb\text{-}D_2$ 吸収線の偏光分光信号に安定化された Reference Laser を周波数基準として PLL によって周波数弁別器の周波数に安定化した．半導体レーザの発振周波数の安定度は，安定的に物理乱数を生成するために十分な安定性を達成することができた． その結果，我々は 100 時間に及ぶ長時間において安定的に物理乱数を生成することに成功した．

また我々は本研究で XOR method と RXOR method に，それぞれ Parallel generation method と Coupling generation method を適用した 4 種類の方法から半導体レーザの周波数雑音を源として物理乱数列を生成した．我々は XOR method において Parallel generation method によって乱数生成速度 120 Gb/s を達成した．また RXOR method において Parallel generation method によって生成速度 80 Gb/s を達成した．本研究においては，RXOR method と比べて，XOR method が，乱数を高速生成するのに適していることが分かった．また Coupling generation method と比べて，Parallel generation method の方が，乱数を高速生成するのに適していることが分かった．一方，この Parallel generation method と Coupling generation method の生成速度の差は，2 進数の r7bit の他の桁に対する低い独立性が原因であった．この問題を解決した Improved XOR method と Improved RXOR method によって生成された乱数の生成速度は，XOR method における Parallel generation method や Coupling generation method，RXOR method におけるそれらの生成速度を上回る結果だった．最終的に，本研究の乱数の最大生成速度は，Improved XOR method と Improved RXOR method における Coupling generation method によって 160Gbits/s を達成した．この結果は，2 進数データの最上位ビットだけから乱数を生成する場合と比較して, 320 倍の速度である．したがって, Improved XOR method と Improved RXOR method は, 他の方式と比較して, 最も高速に物理乱数を生成できることが分かった．

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．

參考文獻

1. William C. Barker, Elaine Barker, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher" NIST Special Publication 800-67 Revision 1, 2012.
2. Calderbank, Michael. "The RSA Cryptosystem: History, Algorithm, Primes." (2007).
3. Lekitsch, B., et al. "Blueprint for a microwave trapped-ion quantum computer." *arXiv preprint arXiv:1508.00420* (2015).
4. N. Gisin , G. Robordy , W. Tittel and H. Zbinden "Quantum cryptography", *Rev. Modern Phys.*, vol. 74, pp.145 -195 2002.
5. Lo, Hoi-Kwong, Marcos Curty, and Kiyoshi Tamaki. "Secure quantum key distribution." *Nature Photonics* 8.8 (2014): 595-604.
6. Takesue, H., et al. "Differential phase shift quantum key distribution experiment over 105 km fibre." *New Journal of Physics* 7.1 (2005): 232.
7. Honjo, Toshimori, et al. "Differential-phase-shift quantum key distribution experiment using fast physical random bit generator with chaotic semiconductor lasers." *Optics express* 17.11 (2009): 9053-9061.
8. Nakazawa, Masataka, et al. "Real-time 70 Gbit/s, 128 QAM Quantum Noise Stream Cipher Transmission over 100 km with Secret Keys Delivered by Continuous Variable Quantum Key." *ECOC 2016; 42nd European Conference on Optical Communication; Proceedings of*. VDE, 2016.
9. Guo, Hong, et al. "Truly random number generation based on measurement of phase noise of laser." *arXiv preprint arXiv:0908.2893* (2009).
10. Atsushi Uchida et al., “Fast physical random bit generation with chaotic semiconductor laser”, Nat. Photon. 2(12) (2008) 728.
11. Reidler, I., et al. "Ultrahigh-speed random number generation based on a chaotic semiconductor laser." *Physical review letters* 103.2 (2009): 024102.
12. Uehara, Tomoyuki, and Takashi Sato. "Physical-random number generation using white frequency-modulation noise of frequency-stabilized semiconductor lasers." *Optical Engineering* 48.4 (2009): 044301.
13. Maehara, Shinya, et al. "Frequency noise characteristics of a diode laser and its application to physical random number generation." *Optical Engineering* 52.1 (2013): 014302.
14. Yabuzaki, T., T. Mitsui, and U. Tanaka. "New type of high-resolution spectroscopy with a diode laser." *Physical review letters* 67.18 (1991): 2453.
15. Sakuraba, Ryohsuke, et al. "Tb/s physical random bit generation with bandwidth-enhanced chaos in three-cascaded semiconductor lasers." *Optics express* 23.2 (2015): 1470-1490.
16. A. Rukhim, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D.

Banks, A. Heckert, J. Dray, S. Vo, NIST Special Publication 800-22 Revision 1, (2008).
17. レーザー学会: レーザーハンドブック(第2版), オーム社 (2005).
18. 稲場文男: 新版レーザ入門, コロナ社 (1979).
19. 久保亮五, 長倉三郎, 井口洋夫, 江沢洋: 岩波 理化学辞典 第4版, 岩波書店 (1987).
20. 応用物理学会編, 半導体レーザの基礎, オーム社 (1987).
21. 大津元一: コヒーレント光量子工学, 朝倉書店 (1990).
22. 霜田光一: レーザー物理入門, 岩波書店 (1994).
23. YAMADA, Minoru, and Koichi IIYAMA. "Noise Measurement of Semiconductor Lasers." *The Review of Laser Engineering* 19.8 (1991): 756-766.
24. M. Ohtsu and K. Nakagawa, "Spectroscopy by Semiconductor Lasers", Chapter5 of Coherence, Amplification and Quantum Effects in Semiconductor Lasers, Edited by Y. Yamamoto, John Wiley & Sons, Inc., New York, 1991, pp.137-190.
25. Vahala, Kerry, and Amnon Yariv. "Semiclassical theory of noise in semiconductor lasers-Part II." *IEEE Journal of quantum electronics* 19.6 (1983): 1102-1109.
26. Spano, Paolo, S. A. L. V. A. T. O. R. E. Piazzolla, and Mario Tamburrini. "Phase noise in semiconductor lasers: A theoretical approach." *IEEE Journal of Quantum Electronics* 19.7 (1983): 1195-1199.
27. Ahmed, Moustafa, Minoru Yamada, and Masayuki Saito. "Numerical modeling of intensity and phase noise in semiconductor lasers." *IEEE journal of quantum electronics* 37.12 (2001): 1600-1610.
28. SAKAI, Yoshihisa, Shigeki AISAWA, and Ken-ichi HAYASHI. "A Study on FM Noise and Line-width of Semiconductor Laser." *IEICE TRANSACTIONS (1976-1990)* 70.4 (1987): 303-305.
29. Daino, B., et al. "Phase Noise and Spectral Line Shape in Semiconductor Lasers." *Quantum Electronics, IEEE Journal of* 19.3 (1983): 266-270.
30. Ohtsu, Motoichi, and Shinichi Kotajima. "Derivation of the Spectral Width of a 0.8 μm AlGaAs Laser Considering 1/f Noise." *Japanese Journal of Applied Physics* 23.6R (1984): 760.
31. Kikuchi, K., and T. Okoshi. "Measurement of spectra of and correlation between FM and AM noises in GaAlAs Lasers." *Electronics Letters* 19.20 (1983): 812-813.
32. Takakura, Toshihiko, Kenichi Iga, and Toshiharu Tako. "Linewidth Measurement of a Single Longitudinal Mode AlGaAs Laser with a Fabry-Perot Interferometer." *Japanese Journal of Applied Physics* 19.12 (1980): L725.
33. Ohdaira, Yasuo, and H. O. R. I. Hirokazu. "High resolution optical near-field spectroscopy using intrinsic frequency noise of diode laser." *IEICE Transactions on Electronics* 85.12 (2002): 2097-2103.
34. 堀健夫: 原子スペクトルと原子構造, 丸善 (1964).

35. F. バソロ, R. C. ジョンソン共著；山田祥一郎訳:配位化学:金属錯体の化学, 化学同人 (1987).
36. 保田和雄: 原子吸光分析, 講談社サイエンティフィク (1982).
37. 大津元一: レーザと原子時計, オーム社 (1986-2).
38. T. Sato, H. Sugai, and M. Shimba, Denshi Jyouhou Tsushin Gakkai Raonbunshi C **J69-C** [5], 600 (1986) [in Japanese].
39. A. Yariv, Quantum Electronics (Wiley, New York, 1988) 3rd ed., p. 175.
40. Moro, Tomoko, et al. "Generation of physical random number using the lowest bit of an A - D converter." *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)* 89.6 (2006): 13-21.
41. Yamazaki, Taiki, and Atsushi Uchida. "Performance of random number generators using noise-based superluminescent diode and chaos-based semiconductor lasers." *IEEE Journal of Selected Topics in Quantum Electronics* 19.4 (2013): 0600309-0600309.
42. Takahashi, Rie, et al. "Fast physical random bit generation with photonic integrated circuits with different external cavity lengths for chaos generation." *Optics express* 22.10 (2014): 11727-11740.
43. Yamaguchi, Akihiro, Takaaki Seo, and Keisuke Yoshikawa. "On the pass rate of NIST statistical test suite for randomness." *JSIAM Letters* 2.0 (2010): 123-126.
44. Kaneda, M., H. Okutomi, and K. Nakamura. *A study on discrete Fourier transform test included in NIST randomness test suite*. IEICE Technical Report, ISEC2006-124, 2007.
45. Okada, Hiroki, and Ken Umeno. "Randomness Evaluation with the Discrete Fourier Transform Test Based on Exact Analysis of the Reference Distribution." *arXiv preprint arXiv:1701.01960* (2017).
46. Drever, R. W. P., et al. "Laser phase and frequency stabilization using an optical resonator." *Applied Physics B* 31.2 (1983): 97-105.
47. Nimonji, Toshiya, et al. "New frequency stabilization method of a semiconductor laser using the Faraday effect of the Rb-D2 absorption line." *Japanese journal of applied physics* 43.5R (2004): 2504.
48. Wieman, C., and Th W. Hänsch. "Doppler-free laser polarization spectroscopy." *Physical Review Letters* 36.20 (1976): 1170.
49. Torii, Yoshio, et al. "Laser-phase and frequency stabilization using atomic coherence." *Physical Review A* 86.3 (2012): 033805.
50. Pearman, C. P., et al. "Polarization spectroscopy of a closed atomic transition: applications to laser frequency locking." *Journal of Physics B: Atomic, Molecular and Optical Physics* 35.24 (2002): 5141.
51. 須田信英: PID制御（システム制御情報ライブラリー6），朝倉書店 (1992).

52. http://power.nagaokaut.ac.jp/convenience/pdffiles/5apidcontrol.pdf
53. http://www-pse.cheme.kyoto-u.ac.jp/members/tonomura/LevelControl.pdf
54. 岡村廸夫: 定本 OP アンプ回路の設計, CQ 出版 (1990).
55. https://www.hamamatsu.com/resources/pdf/ssd/03_handbook.pdf
56. レーザー学会: レーザーハンドブック(第 1 版), オーム社 (1982).
57. http://gate.ruru.ne.jp/rfdn/TechNote/BasePllTech.asp
58. D. W. Allan and J. A. Barnes: A MODIFIED "ALLAN VARIANCE" WITH INCREASED OSCILLATOR CHARACTERIZATION ABILITY, Proc. 35th Ann. Freq. Control Symposium, USAERADCOM, Ft. Monmouth, NJ 07703 (1981).
59. D. W. Allan, Chairman, J. A. Barnes, F. Cordara, M. Garvey, W. Hanson, J. Kusters, R. Smythe, F. L. Walls: Precision Oscillators: Dependence of Frequency on Temperature, Humidity and Pressure, IEEE Proceedings of the 1992 IEEE Frequency Control Symposium Report of Working Group 3 of the IEEE SCC27 Committee (1992).
60. Ohtsu, Motoichi, et al. "Estimation of the ultimate frequency stability of semiconductor lasers." *Japanese Journal of Applied Physics* 22.7R (1983): 1157.
61. Kuboki, Katsuhiko, and M. O. T. O. I. C. H. I. Ohtsu. "Frequency offset locking of AlGaAs semiconductor lasers." *IEEE journal of quantum electronics* 23.4 (1987): 388-394.
62. 大津元一, and 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* 58.10 (1989): 1428-1444.