



系统控制漫谈

FFT：跨越百年的传奇

莱永升 北京大学

快速傅里叶变换（Fast Fourier Transform, FFT）是离散傅里叶变换的一种快速算法。在 20 世纪六十年代刚刚被提出的时候，FFT 以其优越的表现一度成为算法界的弄潮儿。然而，FFT 面世之前的一段历史却鲜为人知。

一、十七世纪之前的发展

1807 年，面对法国科学院，振振有辞的拉格朗日想不到他所反对的工作将会成为现代信息学科的基石，更想不到一个更有名的年轻人，早已悄无声息地迈出了卓越的一步。

自古以来，发明权以及随之而来的冠名权之争，随着时代发展一遍又一遍地席卷科学界。倘若翻开科学史的厚重书页，这种争论、攻讦甚至相互倾轧周而复始，层出不穷。好事者倘若用今日的主角傅里叶变换，对发生过的这些事件做一下分析，说不定可以大有收获，找到令学术界动荡的元凶。

当然，现在人们普遍相信，这些动荡的原因是古代通讯能力太差，只能通过书信的方式实现。书信自然需要有人送信，而即便是“科学”的发祥地欧洲的面积也太过广阔——有一个叫马拉松的年轻人甚至为了送个捷报活活累死——也难怪栖居于世界各地的科学家们互不相识。那时，相隔千里之外的科学家们同时做出科学发现的例子比比皆是，更不用说我们时常对某位中国科学家的发明早于另一位欧洲数学大家而引以为傲了。世界文明的发展受限于缓慢的信息传递速度，我们只好将这些历史的尘埃怪罪于电报、电话和电视的发明者出生太晚——顺便一提，这些发明也存在发明权之争，所以我们并不确定到底该怪罪于谁。然而，即便是当今世界，信息已经可以凭借着电信号在导线中以光速传播，科技巨头们也会为了专利权打得头破血流。以至于研究者在有了新的发现之后，第一时间想到的都是赶紧挂 arXiv。如今，国别、语言甚至期刊的影响因子依然是影响一项科学发现的发明权的障碍：一项卓越的工作，只是因为发表的语言或者期刊不被主流科学界注意，而后有人以同样的内容发表了更“好”的文章，就能揽走所有功劳。

今天的主角诞生之前的故事，依然要从那个最著名的发明权之争讲起。微积分起源于无穷级数，其推动者是两位爵爷：牛顿和莱布尼茨——前者的爵位是货真价实的，后者自称自己有爵位，就看你信不信。祸起于年少的莱布尼茨向仰慕已久的牛顿写信，诉说自己的数学想法。牛顿在回信中写了一大段关

于他通过通量求流量的工作，大概是想告诉莱布尼茨这个工作已经被解决了。然而，恃才傲物的牛顿将这一段叙述用密码文书写，并进行了加密，然后他却用明文写了一句“这个问题尚未被解决”。很显然，这是牛顿爵爷在消遣这位可怜的后辈。天真的莱布尼茨将愚弄当成了鼓励，立刻回信告诉牛顿自己的工作，然而后者并没有回信。这两封信后来被称为“前函”和“后函”，成为了二人争锋的呈堂证供。莱布尼茨在之后奋发图强，终于在 1684 年和 1686 年相继发表了关于微分和积分的论文，并将自己的新发明起名“微积分 (Calculus)”。莱布尼茨的第一篇文章题目，翻译过来是《一种求极大极小和切线的新方法，它也适用于分式和无理量，以及这种新方法的奇妙类型的计算》，这冗长的名字，如今被递到哪怕最不起眼的期刊编辑面前都会被拒稿，却也显示出莱布尼茨对自己的伟大创造的骄傲。而事实上，牛顿确实早在 1665 年就已经创立了他略显笨拙的通量方法，并写在了《流数法和无穷级数》中。有人说是害怕批评，有人说是并不在意，总之出于某种原因，牛顿很晚才发表了这部著作。随着莱布尼茨名声大噪，牛顿终于注意到了这个海峡彼岸的挑战者。1687 年，牛顿用《自然哲学的数学原理》以压倒性的优势赢得了他和胡克的斗争，并在这本书的序言部分吹响了新的战斗号角：“十年前，在我和最杰出的几何学家莱布尼茨的通信中，我表明了我已经知道了确定极大值和极小值、作切线以及类似的方法，但我在交换的信件中隐瞒了这方法，……这位最卓越的科学家在回信中写道，他也发现了一种同样的方法，并描述了他的方法，它与我的方法几乎没有什么不同，除了他的措词和符号以外。”震惊而后恍然大悟的莱布尼茨为此和愤怒的牛顿开始了长达几十年的辩论，并在二人分别成为柏林科学院院长和英国皇家学会会长之后愈演愈烈。如日中天的牛顿控诉年轻的对手抄袭，而莱布尼茨的学生和追随者则坚定地为其辩护。直到莱布尼茨居然天真到向英国皇家学会控告牛顿，皇家学会“不偏不倚”的牛顿追随者们于是“公正”地宣布，牛顿是微积分的“第一发明人”。牛顿看似取得了又一次的胜利。然而，如果以今天的角度看，我们用的绝大多数微积分符号都来自于符号学大师莱布尼茨的手笔。

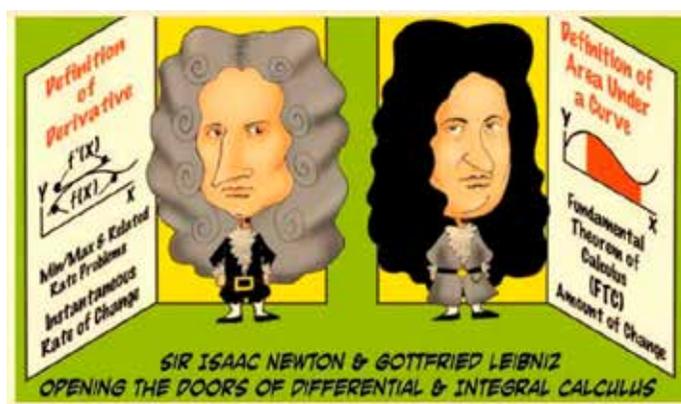


图 1.1 牛顿与莱布尼茨之争。图片来自 CalculusBook.net

“Calculus”这个词来源于词根“calx”，意思是石头（古人用石头计算），因此还有一个意思是结石。两位爵爷也许并不承认对方独立发明了微积分，却必须承认双方都独立地死于结石：莱布尼茨患有肾结石，而牛顿得了膀胱结石。只不过，伟大的牛顿风光光地以国葬安葬，而政治押宝汉诺威公

爵（后来的英国国王乔治一世，汉诺威盛产英国国王）的莱布尼茨，却被汉诺威公爵扔在了老家，贫穷而屈辱地死去^[1]。

至此，牛顿看似赢得了这场战争。然而，与高傲的牛顿不同，莱布尼茨拥有众多学生。其中一位是他与牛顿战争中的急先锋约翰·伯努利。这位最值得称道的，一是发明了因贫穷而卖掉的 L' Hospital 法则，二是他教出了学生欧拉。作为世界上最高产的数学家，欧拉不仅将他师爷的方法和符号学发扬光大，同时也对莱布尼茨的老对头所开拓的领域进行进一步探索，发明了变分法、创立了分析力学。作为 18 世纪最伟大的数学家，劳模欧拉并没有卷入什么官司，我们只能赞叹他是如何以惊人的速度完成浩大的工作的，并顺便以这位“独眼巨人”的事迹告诫自己在工作的同时保护眼睛。正是由欧拉将 FFT 的雏形引入了科学界的视野。



图 1.2 欧拉。图片来自百度

欧拉和其他伟大的数学家继续开拓着对于无穷级数的探索。无穷级数能否表示所有函数？至少幂级数不行：无穷次可微的要求实在太高了。欧拉将目光投向了三角级数。1747 年，欧拉在用插值法计算行星扰动问题时，得到了一个可以用三角级数表示的函数。欧拉证明了，对于整数 x ，存在解析周期函数 $f(x)$ ，满足

$$f(x) = f(x - 1) + X(x)$$

其中

$$X(x) = \frac{df}{dx} - \frac{d^2f}{2! dx^2} + \frac{d^3f}{3! dx^3} - \dots$$

其通解是：

$$f(x) = \int_0^x X(\xi) d\xi + 2 \sum_{n=1}^{\infty} \cos 2n\pi x \int_0^x X(\xi) \cos 2n\pi \xi d\xi \\ + 2 \sum_{n=1}^{\infty} \sin 2n\pi x \int_0^x X(\xi) \sin 2n\pi \xi d\xi$$

欧拉声称这是插值问题的最一般解，果真如此，则意味着任意周期函数都可以用三角级数来表示，但谨慎的欧拉否认了这一点。到了1757年，法国数学家克莱罗 (Clairaut) 在研究太阳引起的摄动时已经宣称，任何函数都可以展开成为：

$$f(x) = A_0 + 2 \sum_{n=1}^{\infty} A_n \cos nx$$

显然这一结论并不正确，但他离真理也仅一步之遥。1777年 Euler 在研究天文问题时，就已经给出了求解连续情况下三角级数系数的方法，这与现代的方法已经完全相同。此时，所谓的傅里叶变换其实已经初具雏形^[2]。尽管如此，当时的科学家们如欧拉，拉格朗日，达朗贝尔等始终认为，并非所有函数都可用三角级数表示。可以想象，数学家们从无尽的宇宙中汲取灵感，可令宇宙也会纳闷的是尽管它已经暗示得这么明显了，为什么这临门一脚还要留给后来的年轻人。

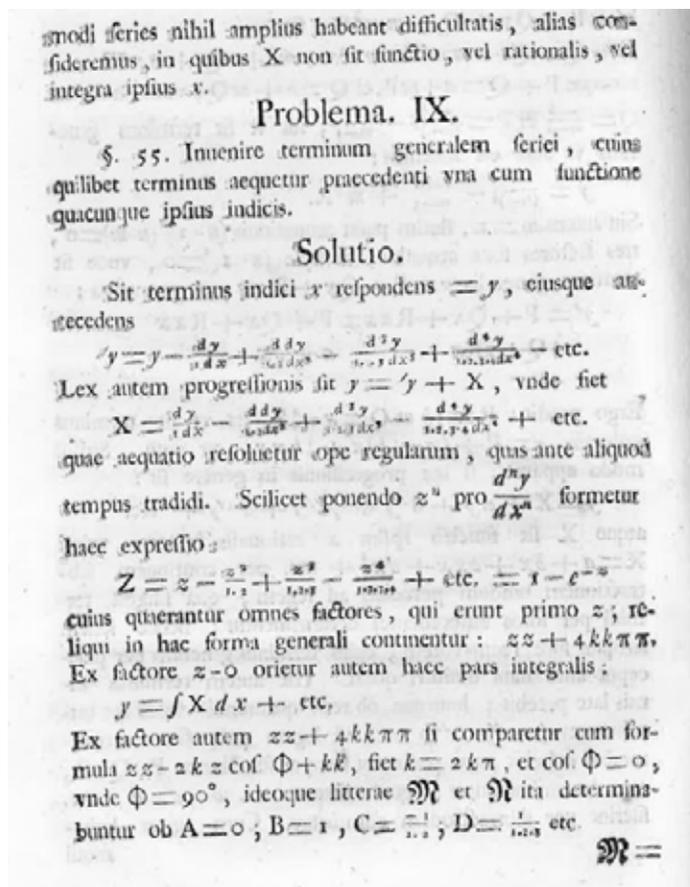


图 1.3 欧拉著作 De serierum determinatione seu nova methodus inveniendi terminos generales serierum 影印版。图片来自 Euler Archive

1807年，傅里叶将论文《热的传播》递交到法国科学院，从此现代信息科学的基石将以他命名。这位拿破仑年轻的追随者和宠儿，从小出身贫寒、父母双亡，在申请进入当时仅有的开设数学科目的陆军学校时惨遭拒绝：“傅里叶出身不高贵，不得加入炮兵，虽然他是第二个牛顿。”多亏法国大革命打破了阶级的壁垒，傅里叶终于获准进入法国科学院阅读数学论文，他在那里认识了拉格朗日和蒙热。1798年，拿破仑进军埃及，带了庞大的科学顾问团，傅里叶就是其中成员之一。他迅速展现出了行政和外交的才能，获得了拿破仑的赏识，成为了法国数学最好的地方行政长官。



图 1.4 傅里叶与拿破仑。图片来自百度

年轻的傅里叶在论文中使用三角级数来探索热传导问题，并提出所有周期函数都可以表示成三角级数的形式。论文的审稿人拉普拉斯，蒙热和拉克鲁瓦都赞成接受这篇论文。然而，法国数学界至高无上的权威拉格朗日并不能接受这个狂妄的想法。拉格朗日的理由是：正弦曲线永远无法组合成一个带有棱角的信号，例如方波。拉格朗日自然是对的，因为三角级数确实无法组合成一个带有棱角的信号，但可以无限逼近——所以傅里叶也是对的。科学大师们功成名就之后总是因为他们的偏见和固有知识而充当了科学发展的反面角色，即使是最伟大的科学家也不例外。法国科学院最后屈服于拉格朗日的权威，论文并未发表。我们的政治新星傅里叶倒也不怎么在乎，继续跟着他的小个子伯乐走南闯北。直到两年后拿破仑称帝，他被授予男爵称号。

1814年，拿破仑兵败，傅里叶和拉普拉斯开始效忠路易十八。然而十个月后，拿破仑卷土重来，骑墙派傅里叶迅速倒向旧主。很不幸，百日皇帝拿破仑不久再次被扔到了岛上，暴怒的路易十八将傅里叶视为叛徒，使他一度无家可归。然而，由于傅里叶名声在外，即使在路易十八的反对下，他也成功当选了法国科学院院士，并在1822年当选为法国科学院终身秘书。就在这一年，终于走上学术权力巅峰的傅里叶，发表了他的《热的解析理论》。此时，再也没有人有资格拒绝他的工作了。在这本书中，傅里叶将他热的数学理论与力学理论相提并论，这个被誉为第二个牛顿的科学家终于向世人推出了他一生中最重要的贡献。这本书开启的另一个领域是量纲分析。

前文已经提到，欧拉等人事实上已经提出了傅里叶变换的积分表示。而我们今天的主角，是傅里叶变换的另一种形式：离散傅里叶变换的快速求解方法。离散傅里叶变换在时域和频域上都呈现离散形式，就比如我们前面提到的冠名权之争的诸多历史事件，总是散落在历史长河的些许角落。对于 N 点序列 $\{x[n]\}$ ，它的离散傅里叶变换（Discrete Fourier Transform, DFT）为：

$$\hat{x}[k] = \sum_{j=0}^{N-1} e^{-i\frac{2k\pi}{N}j} x[j]$$

其逆变换为:

$$x[j] = \frac{1}{N} \sum_{k=0}^{N-1} e^{i\frac{2k\pi}{N}j} \hat{x}[k]$$

掰着指数数数就会知道,如果朴素地计算快速傅里叶变换,那么时间成本将是 $O(N^2)$ 的,随着数据规模的增加,运算量将急剧上升。所以当时懒惰的科学家们一般只计算四五阶就放弃了。

二、快速傅里叶变换的发现

快速傅里叶变换是 DFT 的一种快速算法,它的唯一特点就是快,其余方面与离散傅里叶变换别无二致。在那个计算机刚刚兴起的年代,慢一点都可能造成致命的后果。从太空到军备,美苏之间展开了一场史诗级的竞赛,任意一方稍慢一点都可能大难临头。就是在和平年代,国家之间也会在运动会上追求更高、更快、更强。

1957年,苏联以最快的速度成功发射了洲际导弹和人造地球卫星,震惊西方。赫鲁晓夫吹嘘他们制造导弹如此之快,就像制造香肠一样,不断从车间里生产出来。其实,肯尼迪的情报部门早就告诉他,苏联的洲际导弹数目只有区区五十余枚。然而,肯尼迪掩盖了这一事实,并大肆宣扬美苏之间的导弹差距,从而忽悠国会加大投资巩固美国的优势。1961—1962年美苏进行了大量的核试验,尤其是苏联在1961年10月30日进行的历史上最大当量的核试验,据说在1000公里外都能看到爆炸的闪光,恐怖的核乌云给世界的未来蒙上了一层阴影。



图 2.1 古巴导弹危机中的肯尼迪与赫鲁晓夫。图片来自百度

局势在古巴导弹危机时达到了顶峰,人类第一次发现核战争如此迫在眉睫。双方领导人终于认识到,核冲突对两国都没有好处。肯尼迪和赫鲁晓夫终于恢复理智,1963年8月,双方签署了部分禁止核试验条约,禁止在大气层、外层空间和水下进行核试验。美俄之间的战略武器限制谈判一直延续到了今日。

然而，昔日的战略对手并不会立刻取得相互信任。条约签是签了，如何知道对方是否违约？核试验往往都是秘密进行的，另一个国家可能根本无法知晓，也不会被允许访问对方的核设施进行调查。一向以拥有庞大的科学顾问团著名的肯尼迪，最后决定向科学家们求助。来自 IBM 的加温就是其科学顾问之一。作为费米的学生，就像他的老师和同僚们一样，这位首个氢弹的设计者终身都致力于研究核武器控制。加温在亲手将 Teller-Ulam 构型变为现实之后，就加入了 IBM 公司，后者成了他一生中的主要雇主。他很早就和 IBM 达成协议：他三分之一的时间会用于政府工作，IBM 不会问他为五角大楼做了什么，并且报销他的全部费用。然而，这位科学家先后三个大老板肯尼迪、约翰·尼克松都是著名的短命总统。在这之后，离开总统国家科学顾问团的他，也只能做一些大声疾呼的工作了。

在肯尼迪的科学咨询委员会上，加温提出可以通过在苏联周边国家地下埋藏传感器，来检测核武器爆炸所产生的地震波。这些传感器会生成地震的时间序列，通过比对不同传感器的信息，就可以将核武器试验的地点确定在十五公里范围以内。然而，由于传感器数据量极大，分析这些数据需要一种可以快速计算离散傅里叶变换的算法。这时，坐在加温旁边的来自普林斯顿大学的图基搭了腔。他与加温都是年轻有为的科学家，因为资历较低，都坐在桌子的末端，于是他们经常交流各自的研究。



图 2.2 加温 (Garwin) 接受总统自由勋章。图片来自百度

图基是一个半路出家的数学家。他从小是被自己的母亲教大的，因为母亲担心他“进入学校会变得懒惰”，这与现在大多数因为懒惰把孩子扔给学校老师的家长们形成了鲜明的对比。在布朗大学，图基一直学的是化学，并拿到了化学硕士学位。随后，他进入普林斯顿大学并转攻数学，拿到了两个数学学位。和加温一样，这位能坐在总统面前的科学家也是从那个战火纷飞的年代一路走来的，据说他曾经参与过 U-2 间谍飞机的设计。图基一生的贡献有很多，包括发明了“bit”和“software”两个词。要是他现在还活着，搞不好会被比特币的狂热粉丝们奉为神明，毕竟就连马斯克打个喷嚏都能引起市场动荡。

加温的问题正中图基下怀。作为一名统计学家，图基早已关注到了离散傅里叶变换的问题。这其实并不是人们第一次尝试降低 DFT 的计算难度，包括林肯实验室团队在内的一大批科学家都曾探讨过如何将这一复杂的过程简单化。但这些研究都散落在不同的工程领域之中。而从 1960 年开始，图基非常幸运地与这些科学家都有过接触，他意识到即使面对的问题不同，解决的方式却都殊途同归。在图基看来，这都不过是一个关于频率和统计学的问题。于是图基开始搜集文献，思考这一问题。在那次会议上，图基顺势提出了他的快速计算 DFT 的算法。敏锐的加温博士立刻意识到了这种算法的潜力。这种伟大的算

法离成熟仅剩一步之遥：还差一个程序员。于是，加温找到了他在 IBM 的同事库利。与能够“上桌吃饭”的总统顾问图基和加温不同，在 IBM 工作的库利几年前还只是一个程序员——当然不是现在这种成天对着屏幕，一直坐到 35 岁等着被公司优化的程序员，他操纵的是古老的冯诺依曼机。通过加温，图基和库利取得了联系，并告知了他的想法。起初资格不够只能“站着吃饭”的库利并不知道这个算法的真实目的，他被告知这是用来确定 He-3 在晶体中的自旋周期的^[3]。

1965 年，库利和图基联合发表论文[4]，这个伟大的算法就此诞生——或者重生，这是后话。1994 年美国数学家吉尔伯特·斯特朗把 FFT 描述为“我们一生中最重要的数值算法”，它还被 IEEE 科学与工程计算期刊列入 20 世纪十大算法之一。该算法被命名为库利-图基算法。以图基命名的成果还有很多，但这已经是程序员库利一生中最伟大的成就。除了这篇算法论文本身外，他被引最高的论文都是关于这个算法的发明历史的。

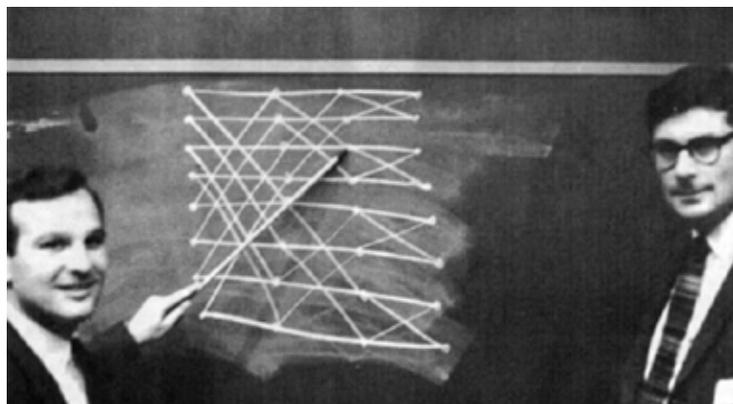


图 2.3 库利和图基。图片来自百度

为了阐明快速傅里叶变换的原理，首先需要引入两个概念：多项式的点值表示法和单位根。首先介绍多项式的点值表示法。我们来想想如何定义一个人？这是数千年来困扰哲学家和生物学家的永恒命题。也许，当我们知道一个人的全部基因组后便可以定义他。然而，如果说基因是一个人的内在的话，我们更熟悉的是从这个人的表征去定义，高矮胖瘦、兴趣爱好、家庭住址等等。倘若有一组足够详尽的特征，我们就可以精准定位到一个人，如“北京市海淀区北京大学附属中学三年级二班的李华”。哲学家们可以争辩这不足以定义一个灵魂，但幸运的是，数学的严谨和逻辑使得它比哲学清晰得多。如果说我们熟悉的多项式系数表示法

$$F(x) = \sum_{i=0}^{n-1} a_i x^i$$

是多项式的灵魂（也就是多项式的基因）的话，那么我们也拥有它的表征定义，即多项式的点值表示法。

将一组互不相同的插值节点 $(x_0, x_1, \dots, x_{n-1})$ 分别代入 $F(x)$ ，得到 n 个取值 $(y_0, y_1, \dots, y_{n-1})$ 。你可以将不同

的插值节点和取值之间的关系类比成一种映射索引，比如城市（北京），中学（北京大学附属中学）。我们有定理： n 个不同点的取值唯一确定一个 $n-1$ 次多项式。于是，我们就可以用这 n 个点来表示这个多项式，这就是多项式的点值表示。它将在之后给我们带来巨大的便利。

那么，我们该取哪些插值节点呢？数学也给我们准备好了材料。单位根是指方程 $x^n = 1$ 的解，它们均匀分布在单位圆上。其中辐角为正且最小的称为 n 次单位向量，记为 ω_n^1 ，其余依次记为 $\omega_n^2, \dots, \omega_n^n$ 。特别地， $\omega_n^n = \omega_n^0 = 1$ 。其中， $\omega_n^k = e^{\frac{2\pi k}{n}i} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$ 。顺便一提，虚数 i 这个符号也是大数学家欧拉的杰作。

关于单位根，我们需要用到它的两个引理。折半引理： $\omega_{2n}^{2k} = \omega_n^k$ ，当将单位圆划分为 $2n$ 份后，它的第偶数个单位根正好是 n 次单位根。消去引理： $\omega_n^{k+\frac{n}{2}} = -\omega_n^k$ ，将单位根沿着单位圆逆时针转动半圈，就正好转到了它的反面。

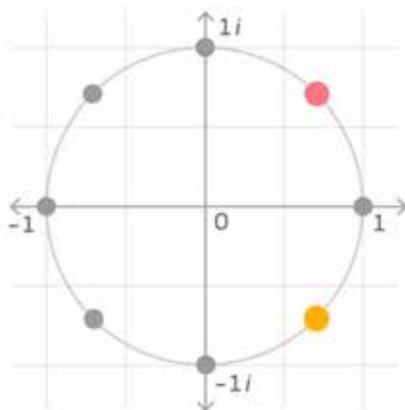


图 2.4 单位根示意图。图片来自网络

有了这两个引理，我们就可以开始介绍快速傅里叶变换的具体原理了。我们将进行傅里叶变换的数列 $x[j]$ 看成是多项式 $F(x)$ 的系数 a_j ，那么如果将 n 次单位根的 $0 \sim n-1$ 次幂分别代入 $F(x)$ ，得到该多项式点值向量 $(F(\omega_n^0), F(\omega_n^1), F(\omega_n^2), \dots, F(\omega_n^{n-1}))$ ，为了下文简便起见，我们将其记为 $(y_0, y_1, \dots, y_{n-1})$ 。这一过程就是离散傅里叶变换。实际上，就是将该多项式的系数表示转化为单位根对应的点值表示。可以想见，如果老实地进行代入计算，那么时间复杂度将是 $O(n^2)$ 。对于高维计算，这将消耗大量的计算资源，在计算能力有限的情况下，降低算法的时间复杂度将使工作效率得到大幅度提升。

我们可以对多项式分而治之。给定一个多项式

$$F(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$$

不妨设 n 为偶数, 如果一个多项式次数不是偶数, 可以令 $a_{n-1}=0$ 来补足位数。对其进行奇偶分组:

$$\begin{aligned} F(x) &= (a_0 + a_2x^2 + a_4x^4 + \cdots + a_{n-2}x^{n-2}) + (a_1x + a_3x^3 + \cdots + a_{n-1}x^{n-1}) \\ &= (a_0 + a_2x^2 + a_4x^4 + \cdots + a_{n-2}x^{n-2}) + x(a_1 + a_3x^2 + \cdots + a_{n-1}x^{n-2}) \end{aligned}$$

然后重新定义两个多项式:

$$\begin{aligned} F_1(x) &= a_0 + a_2x + a_4x^2 + \cdots + a_{n-2}x^{\frac{n-2}{2}} \\ F_2(x) &= a_1 + a_3x + a_5x^2 + \cdots + a_{n-1}x^{\frac{n-2}{2}} \end{aligned}$$

前者具有多项式的偶次系数, 后者具有奇次系数。于是, 聪明的图基就可以将 $F(x)$ 写作 $F_1(x)$ 和 $F_2(x)$ 的组合:

$$F(x) = F_1(x^2) + xF_2(x^2)$$

对于每一个特定的 x_0 , 上述等式都成立。图基提出了这样一个简单的思路: 通过 $F_1(x)$ 与 $F_2(x)$ 的点值表示推算出 $F(x)$ 的点值表示。然而, 我们依然需要 n 个点值。所以我们可以通过分类讨论的方法, 并应用我们之前介绍的两个引理: 对于 $0 \leq k \leq \frac{n}{2} - 1$

$$F(\omega_n^k) = F_1(\omega_n^{2k}) + \omega_n^k F_2(\omega_n^{2k}) = F_1(\omega_{n/2}^k) + \omega_n^k F_2(\omega_{n/2}^k)$$

对于 $\frac{n}{2} \leq k + \frac{n}{2} \leq n - 1$

$$\begin{aligned} F\left(\omega_n^{k+\frac{n}{2}}\right) &= F_1(\omega_n^{2k+n}) + \omega_n^{k+\frac{n}{2}} F_2(\omega_n^{2k+n}) \\ &= F_1(\omega_n^{2k+n}) - \omega_n^k F_2(\omega_n^{2k+n}) \\ &= F_1(\omega_{n/2}^k) - \omega_n^k F_2(\omega_{n/2}^k) \end{aligned}$$

这样, 如果我们知道 $F_1(\omega_{n/2}^k), F_2(\omega_{n/2}^k)$, 我们就能直接求出 $F(\omega_n^k)$ 与 $F\left(\omega_n^{k+\frac{n}{2}}\right)$, 而不需要理会那些烦人的系数了。原问题被转化成了两个规模一半的子问题! 计算难度大大降低了。可是 F_1 和 F_2 的点值表示依然很难计算啊? 我们当然不会止步于此。

同样地, F_1 和 F_2 的点值表示也可以化为更小的两个子问题, 如此不断地分治下去。这样的递归问题的时间复杂度为:

$$T(n) = 2T\left(\frac{n}{2}\right) + O(n) = O(n \log n)$$

库利和图基联合发表论文二十多年后, 将多项式分为奇部和偶部的技巧还将被用来破解哈里托诺夫(Kharitonov)的密码。这还是一个和多项式有关的故事。控制学家们关心一个多项式的稳定性问题, 当

它的根全部在负半平面时,我们就称其为稳定的。也许你会说,那不是求出所有根就好了?然而在实际的工程中,我们也许并不知道一个多项式的确切系数,只知道每个系数的大致范围 $a_i \in [a_i^-, a_i^+]$,这样的多项式被称为区间多项式,可以严格写作 $N = \{f(s) = a_0 + a_1s + \dots + a_{n-1}s^{n-1} + a_ns^n \mid a_i \in [a_i^-, a_i^+]\}$ 。这样,不同的系数组合会产生无穷多个多项式,这些多项式是否都稳定?这困扰了数学家和控制学家们很多年。1975年,苏联博士生 Kharitonov 提出了一个关于区间多项式的稳定性定理,这个定理将一个无穷个多项式的稳定性问题,简化成了四个区间端点多项式的稳定问题:区间多项式稳定的充分必要条件是以下四个多项式都稳定,

$$f_1(s) = a_0^+ + a_1^-s + a_2^-s^2 + a_3^+s^3 + a_4^+s^4 + a_5^-s^5 \dots$$

$$f_2(s) = a_0^+ + a_1^+s + a_2^-s^2 + a_3^-s^3 + a_4^+s^4 + a_5^+s^5 \dots$$

$$f_3(s) = a_0^- + a_1^+s + a_2^+s^2 + a_3^-s^3 + a_4^-s^4 + a_5^+s^5 \dots$$

$$f_4(s) = a_0^- + a_1^-s + a_2^+s^2 + a_3^+s^3 + a_4^-s^4 + a_5^-s^5 \dots$$

这四个多项式被称为 Kharitonov 多项式。怎么样,看出规律了吗?三年后,他将这一成果发表在了苏联期刊上。然而因为语言的阻隔,主流科学界并没有注意到这一伟大的理论成就。直到波兰科学家 Olbrot 在瑞士的会议上介绍了这一定理,它才被美国科学家 Barmish 介绍到了英语世界^[5,6]。与俄罗斯有世仇的波兰人,因为历史原因通晓俄语,却也成为了将这一定理引向世界的桥梁。然而, Kharitonov 的原证明极其复杂,加上是用晦涩难懂的俄语写的,对于使用惯了简单语法的美国人来说简直就是折磨。1989年,美国学者 Desoer 指导研究生^[7]巧妙地利用了上面所说的技巧,使得 Kharitonov 定理终于有了简单易懂的证明。

Kharitonov 定理的必要性是显然的,这四个多项式都是区间多项式的元素,当区间多项式稳定时,这四个多项式自然稳定。我们只需要证明其充分性。多项式的根对系数是连续依赖的,当一个多项式从稳定变到不稳定时,它的根一定跨越了复轴。当根在复轴上时,可以写作 $i\omega$ 。因为我们考虑的是实系数多项式,其取值 $f(i\omega)$ 关于实轴对称,所以我们只考虑 $\omega \in (0, +\infty)$ 的情况。每一个多项式 $f(i\omega)$ 的取值在复平面都可以对应一个值点。我们定义 $H_N(\omega) = \{f(i\omega), f \in N\}$,它代表自变量为 $i\omega$ 时,区间多项式在复平面形成的区域。

由于复数乘法的性质,此时多项式

$$\begin{aligned} f(i\omega) &= a_0 + ia_1\omega - a_2\omega^2 - ia_3\omega^3 + a_4\omega^4 + \dots \\ &= (a_0 - a_2\omega^2 + a_4\omega^4 - \dots) + i(a_1\omega - a_3\omega^3 + a_5\omega^5 - \dots) \\ &= U(\omega) + iV(\omega) \end{aligned}$$

多项式 U 的系数是 f 的所有偶数项系数,而 V 的系数是所有奇数项系数,这其实与刚才的 F_1, F_2 如出一辙。对于首一的稳定多项式,其所有系数一定是正的,那么两类多项式的取值分别满足:

$U^-(\omega) \leq U(\omega) \leq U^+(\omega), V^-(\omega) \leq V(\omega) \leq V^+(\omega)$, 其中

$$\begin{aligned} U^-(\omega) &= a_0^- - a_2^+ \omega^2 + a_4^- \omega^4 - \dots, U^+(\omega) = a_0^+ - a_2^- \omega^2 + a_4^+ \omega^4 - \dots \\ V^-(\omega) &= a_1^- \omega - a_3^+ \omega^3 + a_5^- \omega^5 - \dots, V^+(\omega) = a_1^+ \omega - a_3^- \omega^3 + a_5^+ \omega^5 - \dots \end{aligned}$$

在 U, V 的极值中各取一个, 可以组成四个点 $(U^-, V^-), (U^-, V^+), (U^+, V^-), (U^+, V^+)$ 。如图 2.5, 这四个点围成了一个矩形。因为区间多项式的各个系数是独立变化的, 所有区间多项式的值点就都被包含在矩形之中, 并充满整个区域, 这就是 $H_N(\omega)$ 。

为了继续证明, 我们需要用到排零原理: 设一个多项式族 F 的取值区域为 $H_F(\omega) = \{f(i\omega), f \in F\}$, 则该多项式族是稳定的当且仅当:

- 1) F 中至少有一个多项式 f^* 是稳定的;
- 2) $H_F(\omega)$ 不包括原点, 即 $0 \notin H_F(\omega)$, 对任意 $\omega \in (0, +\infty)$ 。

如果四个多项式都稳定, 那么就满足了条件 1), 我们只须证明区间多项式 N 的区域 $H_N(\omega)$ 一定不包括原点。为此, 在之后的证明中还需要用到一个事实: 如果多项式 f 是稳定的, 随着 ω 的增大, 辐角 $\arg(f(i\omega))$ 严格单调递增 (它的值点 $f(i\omega)$ 绕着原点逆时针旋转)。

现在通过反证法进行证明: 因为四个多项式稳定, 它们的系数之一 $a_i^- > 0$, 因此 $0 \notin H(0) = [a_0^-, a_0^+]$ 。假设存在某一个 $\omega_1 \in (0, +\infty)$, 使得 $H_N(\omega_1)$ 包括原点。由于 $H_N(\omega)$ 是随着 ω 连续变化的, 所以一定存在 $\omega_0 \in (0, \omega_1)$ 使得坐标原点在 $H_N(\omega_0)$ 的一条边上。并且由于四个点对应的多项式都是稳定的, 不会有纯虚根, 因此原点只能在矩形边的中间, 而非端点。不妨设原点所在的是下方水平边, 如图 2.5 所示, 已知四个多项式都是稳定的, 那么如果 ω 继续增大, 四个点辐角都会增大。左边的点 (U^-, V^-) 会向右下进入第三象限, 而右边的点 (U^+, V^-) 会向右上进入第一象限, 这条边将不再水平。而这两个点具有相同的虚部, 其连线又必须是水平的, 这就产生了矛盾。如果原点在其他的边上同理可证, 于是充分性的证明就巧妙地完成了。

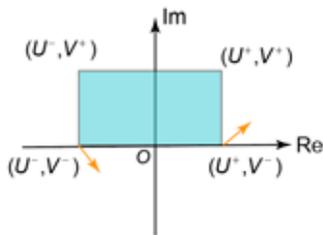


图 2.5 $H_N(\omega)$ 示意图。如果 ω 继续增大, 四个点辐角都会增大 (如箭头所示)。左边的点 (U^-, V^-) 会向右下进入第三象限, 而右边的点 (U^+, V^-) 会向右上进入第一象限, 二者连线将不再水平。

苏联解体之后, Kharitonov 在西方已经小有名气, 在墨西哥一所学校谋了职位, 过着悠闲的日子。从墨西哥退休以后, 他又重返圣彼得堡, 和母亲住在了一起, 过着低调的生活。2021 年, 国际自动控制

联合会 (International Federation of Automatic Control, IFAC) 授予了他终身成就奖 (Lifetime Achievement Award)。一位国际控制大牛评价他: “It would of course be impossible to miss his early result known as the Kharitonov theorem, which is truly a trailblazing contribution and a rare gem, for its extraordinary conceptual importance and mathematical beauty that I think rivals the best known results of our field.” 因为疫情的原因, 颁奖仪式改为线上举行。就在大家翘首以待主角隔着屏幕向大家挥手致意时, 就像每一个在线上课逃课的学生一样, Kharitonov 却说 he 家里网络不好, 没有出席颁奖仪式, 只是说把奖状寄给他就好了。

我们继续说回到快速傅里叶变换。多项式的点值表示对于计算机来说方便了许多, 但是对于人类而言, 我们还是更喜欢系数表达式, 那么如何将多项式的点值表示变回去呢? 下面我们来介绍快速傅里叶逆变换。上面的过程其实可以写作:

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & (\omega_n^1)^1 & (\omega_n^1)^2 & \cdots & (\omega_n^1)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (\omega_n^{n-1})^1 & (\omega_n^{n-1})^2 & \cdots & (\omega_n^{n-1})^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix}$$

如果我们要从点值表示 $(y_0, y_1, \dots, y_{n-1})$ 反推回系数表示, 那我们只需要知道上面矩阵的逆矩阵就可以了。设 x 为 n 次单位根, 注意到

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + 1)$$

当 $x = 1$ 时

$$x^{n-1} + x^{n-2} + \cdots + 1 = n$$

否则

$$x^{n-1} + x^{n-2} + \cdots + 1 = 0$$

那我们就可以发现:

$$\begin{bmatrix} 1 & (\omega_n^{n-i})^1 & \cdots & (\omega_n^{n-i})^{n-1} \end{bmatrix} \begin{bmatrix} (\omega_n^j)^1 \\ \vdots \\ (\omega_n^j)^1 \end{bmatrix} = \sum_{k=0}^{n-1} (\omega_n^{n-i})^k (\omega_n^j)^k = \sum_{k=0}^{n-1} (\omega_n^{n-i+j})^k = \begin{cases} n & i = j \\ 0 & i \neq j \end{cases}$$

于是所求逆矩阵就可以写为:

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & (\omega_n^{n-1})^1 & (\omega_n^{n-1})^2 & \cdots & (\omega_n^{n-1})^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (\omega_n^1)^1 & (\omega_n^1)^2 & \cdots & (\omega_n^1)^{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & (\omega_n^1)^1 & (\omega_n^1)^2 & \cdots & (\omega_n^1)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (\omega_n^{n-1})^1 & (\omega_n^{n-1})^2 & \cdots & (\omega_n^{n-1})^{n-1} \end{bmatrix}$$

则以多项式的点值表示 y_k 为系数, 单位根的共轭 $\overline{\omega_n^k}$ 为插值节点, 做一次快速傅里叶变换, 就可以求得多项式的系数 a_k ^[4]。

作为离散傅里叶变换的快速算法, FFT 迅速在前者的相关领域大显身手, 如频谱分析、数据压缩、

图片处理、求解偏微分方程等等。这里重点介绍 FFT 在算法竞赛中应用最多的领域：多项式乘法。

设有 n 次多项式 $A(x)$, m 次多项式 $B(x)$, 求 $C(x) = A(x) \cdot B(x)$ 。 $C(x)$ 的每一项系数

$$c_k = \sum_{i+j=k} a_i b_j$$

可以想象, 如果按照定义计算, 需要将两个多项式系数逐项相乘再累加, 这其实相当于一次线性卷积, 其计算复杂度也是 $O(n^2)$ 的。

多项式的点值表示可以大大加速多项式乘法的计算。取 $n + m$ 个插值节点, 则两个多项式的点值表示为:

$$A(x): (y_{a0}, y_{a1}, \dots, y_{a(n+m)})$$

$$B(x): (y_{b0}, y_{b1}, \dots, y_{b(n+m)})$$

那么二者相乘

$$C(x): (y_{a0} \cdot y_{b0}, y_{a1} \cdot y_{b1}, \dots, y_{a(n+m)} \cdot y_{b(n+m)})$$

上式就是多项式 $C(x)$ 的点值表示。利用离散傅里叶变换的特点, 可以将时域上的卷积运算, 转换为频域上的相乘运算。

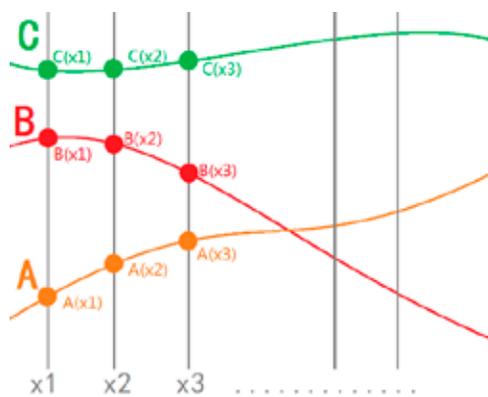


图 2.6 多项式的点值计算。图片来自百度

三、高斯遗珠

“库利-图基算法历史学”著名专家库利先生随后的一项重要工作，就是捍卫他们对这一算法的发明权。平心而论，他们确实独立发明了这个算法。但是随着他们一炮而红，越来越多的科学家和科学史专家发现，这个算法其实在很久以前就诞生过一次。

1795 年和 1798 年，一个来自德国的年轻学生从图书馆借阅了伟大数学家欧拉和拉格朗日关于三角级数的工作。这位学生名叫高斯，他在 1799 年获得了博士学位，虽然此时他早已名声大噪。作为莱布尼茨的后辈、自欧拉之后最伟大的数学家、现代数学的奠基人，高斯此时正处于数学研究的巅峰时期。



图 3.1 高斯。图片来自百度

高斯拓展了前人对于三角级数的研究。回顾离散傅里叶变换：

$$\hat{x}[k] = \sum_{j=0}^{N-1} e^{-i\frac{2k\pi}{N}j} x[j]$$

高斯在需要进行傅里叶变换（此时还并不叫傅里叶变换）的 N 个样本（多项式的系数）时等间隔地取出 N_1 个样本，这样一共可以将原来的集合分成 N_2 个子集（ $N = N_1 N_2$ ）。一开始，他计算出了前两组 N_1 个样本的傅里叶变换，结果却发现它们并不相同，与整个样本所计算的傅里叶系数也不一致。高斯意识到了部分样本的傅里叶变换并不能代表整个样本。基于此，他对每组的傅里叶系数进行了修正，给出了一种新的计算方法：首先，计算出全部 N_2 个规模为 N_1 的集合的离散傅里叶变换，然后再将这 N_2 个值进行组合，计算全部信号的离散傅里叶变换：

$$\hat{x}[k_1 + N_1 k_2] = \sum_{j_2=0}^{N_2-1} \left[\sum_{j_1=0}^{N_1-1} x(N_2 j_1 + j_2) \omega_{N_1}^{j_1 k_1} \omega_N^{j_2 k_1} \right] \omega_{N_2}^{j_2 k_2}$$

其中，对离散傅里叶变换中的系数做出如下变换：

$$\begin{aligned} j &= N_2 j_1 + j_2 \\ k &= N_1 k_2 + k_1 \end{aligned}$$

$j_1, k_1 = 1, \dots, N_1 - 1$, $j_2, k_2 = 1, \dots, N_2 - 1$ 。高斯的方法看起来更加复杂，但根据后世科学家的研究，实际上这是与库利和图基的方法等价的，我们的科技史专家库利也承认了这一点[3.8]。

高斯显然意识到了这一计算方法的便捷性，然而，他并没有估算算法的计算复杂度。更遗憾的是，之后去当天文台长的高斯并没有发表这一成果。在其去世以后，这篇文章也仅仅以新拉丁语发表。晦涩难懂的新拉丁语以及高斯独特的数学符号（例如，高斯用 π, ν, μ 来表示样本数量，而非我们常用的 N ）让后续懒惰的学生们望而却步。也许，如果高斯早点发表这项成果，Cooley-Tukey 算法也就该改名了，科技史专家库利先生也不必为了捍卫他的冠名权而奔走一生。但故事不止于此。

Dating of Gauss' Work on the FFT <i>Theoria interpolationis methodo nova tractata</i> Volume III, Werke	
April 30, 1777	GAUSS is born in Brunswick.
September 1795	GAUSS arrives at Göttingen. Throughout his stay there, he checked out many books from the university library. In particular, he continually read <i>Miscellanea Taurinensia</i> , the proceedings of the academy located in Turin. When these proceedings were being published, LAGRANGE was there and this journal served as his exclusive outlet. In Volumes I and III, LAGRANGE's DFT (sine only) appears.
November 25, 1796	Date given for diary entry 44, ³ which reads <i>Formulae interpolationis elegans</i> . Translated, this entry means "Elegant formula for interpolation". The editor of the diary connected this with the LAGRANGE interpolation formula. No specific library books can be readily connected to this entry.
December 1796	Date given for diary entry 46, which reads <i>Formulae trigonometricae per series expressae</i> . Translated, this entry means "Trigonometric formulas expressed with series". The editor of the diary made no comment about this entry.
September 28, 1798	GAUSS returns home to Brunswick after finishing his studies at Göttingen.
December, 1804–1805	Correspondence between GAUSS and BESSEL indicates their concern with the interpolation problem. No mention is made, however, of the trigonometric interpolation problem. ⁴
March 25, 1805	GAUSS, in a letter to the astronomer OLBERS, ⁵ provides his latest elements for the orbit of the asteroid Juno, among which is the value of the eccentricity 0.254236. ⁶ This number is used by GAUSS in an example in his FFT writings. Thus the treatise must have been completed after this date. These elements were published later in <i>Monatliche Correspondenz</i> , a collection of unreviewed notes containing astronomical observations and information, in May, 1805.
November, 1805	Diary entry 124, which reads <i>Theoriae interpolationis ulterris exsoluitis</i> . Translated, this entry means "We have worked out further a theory of interpolation". The editor takes this entry to mean that his treatise on interpolation could not have been written before November, 1805. He refers to a notebook of GAUSS consisting of short mathematical notes (<i>Mathematische Brouillons</i>), which was begun in October, 1805. Volume 18 of the notebook contains an opening note on interpolation. The editor takes this note to be a first draft of the treatise. However, the collected work of GAUSS does not contain this paper.
January, 1806	In correspondence to OLBERS, GAUSS mentions his work on interpolation, which he says was done "earlier". He stressed the novelty of the second half of the work. He enclosed a copy of it with the letter, asking OLBERS for criticism. In reply, OLBERS encouraged publication, but admitted not being able to follow the second half.
July 30, 1806	Date attached to a letter sent from GAUSS to BOSE, in which the value of the eccentricity for Juno of 0.2549441 is given. Presumably, this means that the FFT treatise must have been written prior to this date. This letter appeared in <i>Monatliche Correspondenz</i> later in 1806. ⁷
November 8, 1808	A letter from SCHUMACHER, a former student of GAUSS, to GAUSS mentions that SCHUMACHER's mother has a handwritten copy of his work on interpolation. ⁸ It is unclear whether this letter is referring to <i>Mathematische Brouillons</i> or the <i>Theoria interpolationis</i> .
June 8, 1816	SCHUMACHER writes GAUSS that he has a handwritten version of GAUSS' work on interpolation, which he hopes GAUSS will publish soon. ⁹ Thus, GAUSS did not keep this work secret, but presumably was not interested in publishing it.

图 3.2 高斯研究 FFT 的大致时间。图片来自[2]

研究者推断，高斯大概是在 1805 年 10 月至 11 月完成的这项工作，这要比 1807 年傅里叶向法国科学院提交论文还早两年！而他最早的手稿可能写于 1804 年。或许，离散傅里叶变换应该改名叫做高斯变换，也确实有人这么做了^[2]。碍于时代和语言的障碍，高斯的工作被历史尘封，可能连他自己也没有意识到这个不起眼的工作的重要性。历史也并没有记载过，他对傅里叶变换的命名有什么不满。拥有一百一

十多项数学成果冠名的数学王子，可能对此也并不在乎。

前面提到，傅里叶变换的连续形式其实已经被欧拉提出，而离散的形式又可以叫做高斯变换。如此看来，傅里叶变换就没傅里叶什么事了。其实不然，尽管前人和同时代的高斯做了很多工作，但敢于越过雷池，第一次提出任何周期函数都可以分解为三角级数这一深刻思想，并给出正确形式的依然是傅里叶。如果没有傅里叶，人类也许只能等待某个新拉丁语专家，从卷帙浩繁的高斯手稿中翻出后世信息学的基石，也不知道信息科学会因此迟滞多少年。

高斯也不是唯一一个在库利和图基之前提出类似方法的人^[9]，龙格是其中最为著名的一位。在 1903、1905 年发表的两篇论文以及与柯尼希合著的书中，都提到了一种通过计算两个 N 点的傅里叶变换来计算 $2N$ 点傅里叶变换的方法。但这一方法在适用的数列长度上有局限性。包括开尔文爵士在内的一系列科学家都曾试图推广龙格的方法。然而，龙格并没有想过用这个方法计算 4 阶以上的傅里叶变换，因为囿于十九世纪的科技发展，4 阶傅里叶级数在当时已经够用了。

Researcher(s)	Date	Lengths of Sequence	Number of DFT Values	Application
C. F. GAUSS [10]	1805	Any composite integer	All	Interpolation of orbits of celestial bodies
F. CARLINI [28]	1828	12	7	Harmonic analysis of barometric pressure variations
A. SMITH [25]	1846	4, 8, 16, 32	5 or 9	Correcting deviations in compasses on ships
J. D. EVERETT [23]	1860	12	5	Modeling underground temperature deviations
C. RUNGE [7]	1903	2^*K	All	Harmonic analysis of functions
K. STUMPF [16]	1939	$2^*K, 3^*K$	All	Harmonic analysis of functions
DANIELSON & LANCZOS [5]	1942	2^*	All	X-ray diffraction in crystals
L. H. THOMAS [13]	1948	Any integer with relatively prime factors	All	Harmonic analysis of functions
I. J. GOOD [3]	1958	Any integer with relatively prime factors	All	Harmonic analysis of functions
COOLEY & TUKEY [1]	1965	Any composite integer	All	Harmonic analysis of functions
S. WINOGRAD [14]	1976	Any integer with relatively prime factors	All	Use of complexity theory for harmonic analysis

图 3.3 FFT 类似算法发明者一览。图片来自[2]

这也难怪，最后将这一算法带到世界面前的，是曾经与冯诺依曼合作设计早期计算机、发明了“bit”一词的图基。1925 年，龙格从哥廷根大学退休，而年轻的冯诺依曼距离从布达佩斯大学毕业却还有一年时间。科学的发展总是与时代相辅相成，现代计算机的发明使得人类的计算能力得到了迅猛发展，技术进步（尤其是信息技术和智能技术的飞速发展）也使得人类面临的问题变得越来越复杂。如果没有这些新的问题的推动，也就不可能催生出后续的工程技术。如果让高斯来对一张北京大学的照片做一个傅里



叶变换，高斯或许会认为这是马可波罗从东方神秘大国带来的巫术。与大多数冠名权之争不同，这次小小的争端不过是历史滚滚向前的车轮扬起的一片尘埃罢了。有诗云：

高斯遗珠沉沧海，百年求索炳春秋。
尔曹身与名俱灭，不废江河万古流。

参考文献

- [1] Hellman H. Great feuds in science: Ten of the liveliest disputes ever. New York: Wiley, 1998.
- [2] Heideman M, Johnson D & Burrus C. Gauss and the history of the fast Fourier transform. IEEE ASSP Magazine, 1984, 1(4): 14 – 21.
- [3] Cooley, J W. The re-discovery of the fast Fourier transform algorithm. Microchimica Acta, 1987, 93(1): 33 – 45.
- [4] Cooley J W & Tukey J W. An algorithm for the machine calculation of complex Fourier series. Mathematics of Computation, 1965, 19(90): 297 – 301.
- [5] Barmish B R. New tools for robustness analysis. Proceedings of the 27th Conference on Decision and Control, IEEE, Austin, TX, 1988.
- [6] Egorov A. Vladimir Kharitonov: Achievements in research. International Journal of Robust and Nonlinear Control, 2022, 32(6): 3101 – 3125.
- [7] Minnichelli R J, Anagnost J J & Desoer C A. An elementary proof of Kharitonov's stability theorem with extensions. IEEE Transactions on Automatic Control, 1989, 34(9): 995 – 998.
- [8] Cochran W T, Cooley J W, Favin D L, Helms H D, Kaenel R A, Lang W W, ... & Welch P D. What is the fast Fourier transform?. Proceedings of the IEEE, 1967, 55(10): 1664 – 1674.
- [9] Cooley J W, Lewis P A & Welch P D. Historical notes on the fast Fourier transform. Proceedings of the IEEE, 1967, 55(10): 1675 – 1677.