中国数学会通讯， 2004, 第 4 期， 13–17.

组合数论中两个局部到整体的结果

孙智伟 (南京大学数学系，南京 210093)

摘要

本文介绍组合数论中两个新型的局部 - 整体性定理。其证明涉及 Vandermonde 行列式，既简明易懂又有启发性。

1. 引言

对于整数 a 与正整数 n，让 $a(n)$ 表示模 n 的剩余类

$$a+n\mathbb{Z}=\{x\in\mathbb{Z}:\ x\equiv a\ (\mathrm{mod}\ n)\}=\{\ldots,\,a-n,\,a,\,a+n,\,\ldots\}.$$

给定有限个剩余类 $a_1(n_1),\ldots,a_k(n_k)$, 如果 $\bigcup_{s=1}^k a_s(n_s)=\mathbb{Z}$ 则称

$$A=\{a_s(n_s)\}_{s=1}^k \tag{1}$$

为一个覆盖系。这一概念由著名数学家 Paul Erdős 在二十世纪三十年代首创；他指出 $\{0(2),0(3),1(4),5(6),7(12)\}$ 就是个不同模覆盖系，并应用覆盖构造出一个全由奇数组成的剩余类使其中每个数都不能表成 2 的幂次加素数的形式。作者最近在 [S3] 中揭示出覆盖系与 Abel 群上的零和问题及域上的子集和问题密切相关。

1962 年 Erdős [E1, E2] 悬赏求证他的下述猜想：如果 (1) 覆盖 1 到 2^k 间每个整数，则它必为覆盖系。注意 $\{1(2),2(2^2),\ldots,2^{k-1}(2^k)\}$ 覆盖除 2^k 倍数之外的所有整数，这表明 Erdős 猜想中 2^k 是最好可能的。1969-1970 年 R. B. Crittenden 与 Vanden Eynden [CV1, CV2] 运用深刻的素数分布规律极为繁琐地证明了 $k>20$ 时 Erdős 猜想成立。作者 ([S1, S2]) 在 1995-1996 年运用 Vandermonde 行列式简洁地证明了下述更强的结果。

局部 - 整体性定理 I. 给定剩余类系 (1) 及分别与模 $n_1,\ldots,n_k$ 互素的整数 $m_1,\ldots,m_k$. 让

$$S=\Big\{\Big\{\sum_{s\in I}\frac{m_s}{n_s}\Big\}:\ I\subseteq\{1,\ldots,k\}\Big\}, \tag{2}$$

其中 $\{\alpha\}$ 表示实数 α 的小数部分。假设 (1) 覆盖连续 $|S|$ ($\leqslant 2^k$) 个整数至少 m 次，则它覆盖每个整数至少 m 次。

这儿是它的一个有趣推论。

推论 1 ([S3]). 设 n 为正整数，整数 $m_1,\ldots,m_{n-1}$ 都与 n 互素。则集合

$$\Big\{\sum_{s\in I}m_s:\ I\subseteq\{1,\ldots,n-1\}\Big\}$$

包含一个模 n 的完全剩余系。

证明： $A=\{1(n),\dots,n-1(n)\}$ 覆盖了 $1,\dots,n-1$ 但不覆盖 n 的倍数。依局部 - 整体性定理 I，集合

$$\left\{\left\{\sum_{s\in I}\frac{m_s}{n}\right\}:\ I\subseteq\{1,\dots,n-1\}\right\}$$

的基数不能不超过 $n-1$. 这就证明了所要结论。 □

剩余类系 (1) 的覆盖函数是如下的 $\mathbb{Z}$ 上周期函数：

$$w_A(x)=\sum_{s=1}^{k}[x\equiv a_s\ (\mathrm{mod}\ n_s)],$$

这儿 $[x\equiv a_s\ (\mathrm{mod}\ n_s)]$ 在 $x\equiv a_s\ (\mathrm{mod}\ n_s)$ 时取值 1, 此外取值 0. 注意 (1) 覆盖整数 x 至少 m 次相当于 $w_A(x)\geqslant m$.

除了剩余类的特征函数外， Dirichlet 特征也是常见的周期算术函数。熟知椭圆曲线上的有理点 (连同无穷远点 O) 构成 Abel 群； a 是加法 Abel 群中阶为 n 的挠元素时 $\mathbb{Z}$ 上映射 $\psi(x)=xa$ 具有周期 n. 关于周期算术映射的和函数，作者 ([S4, S5]) 最近获得了下述一般性定理。

局部 - 整体性定理 II. 设 G 为加法 Abel 群， $\psi_1,\dots,\psi_k$ 都是 $\mathbb{Z}$ 到 G 的周期映射且分别有正周期 $n_1,\dots,n_k$. 令

$$T=\bigcup_{s=1}^{k}\left\{\frac{r}{n_s}:\ r=0,1,\dots,n_s-1\right\}. \tag{3}$$

如果和函数 $\psi=\psi_1+\cdots+\psi_k$ 在连续 $|T|$ ($\leqslant\sum_{s=1}^{k}n_s-k+1$) 个整数处都取某个常数值，则 ψ 必为常函数。

此定理有下述推论。

推论 2. 假设剩余类系 (1) 覆盖连续 $|T|$ 个整数恰好 m 次 (其中集合 T 由 (3) 给出)，则它覆盖每个整数恰好 m 次。

证明：这是因为 $\psi_s(x)=[x\equiv a_s\ (\mathrm{mod}\ n_s)]$ 是周期为 n_s 的算术函数。 □

能否在多项式时间内判定给定的剩余类系 (1) 是否为覆盖系等价于著名世界难题 NP=?P (见 [GJ, T]) ，与此相对照局部 - 整体性定理 II 表明我们可在多项式时间内判定给定的剩余类系 (1) 是否具有指定的覆盖函数。

在下一节中我们将证明第一个局部 - 整体性定理及 G 为复数域 $\mathbb{C}$ 时的第二个局部 - 整体性定理。

2. 主要结果的证明

引理 1. 假设 $c_1,\dots,c_k$ 为复数， $z_1,\dots,z_k$ 为非零复数。如果有连续 $|\{z_1,\dots,z_k\}|$ 个整数 x 使得 $\sum_{s=1}^{k}c_sz_s^x=0$, 则对任何整数 x 都有 $\sum_{s=1}^{k}c_sz_s^x=0$.

证明：假设 $\{z_1,\dots,z_k\}$ 由 l 个不同复数 $\rho_1,\dots,\rho_l$ 构成，且对 $n=0,1,\dots,l-1$ 有 $\sum_{s=1}^k c_s z_s^{h+n}=0$，这儿 $h\in\mathbb{Z}$. 令

$$C_t=\sum_{\substack{1\leqslant s\leqslant k\\ z_s=\rho_t}} c_s \quad (t=1,\dots,l),$$

则线性方程组

$$\sum_{t=1}^{l}\rho_t^n x_t=0 \ \ (n=0,1,\dots,l-1) \tag{4}$$

有解 $x_t=C_t\rho_t^h$ $(t=1,\dots,l)$. 而其系数行列式 $|\rho_t^n|_{0\leqslant n<l,1\leqslant t\leqslant l}$ 是个 Vandermonde 行列式，其值为

$$\prod_{1\leqslant s<t\leqslant l}(\rho_t-\rho_s)\neq 0,$$

故依 Cramer 法则方程组 (4) 只有零解。于是 $C_t=\rho_t^{-h}x_t=0$ $(t=1,\dots,l)$, 从而对任何 $x\in\mathbb{Z}$ 都有

$$\sum_{s=1}^{k}c_s z_s^x=\sum_{t=1}^{l}C_t\rho_t^x=0.$$

引理 1 证毕。 □

局部 - 整体性定理 I 的证明: 先假定 $m=1$. 任给整数 x，

$$\begin{aligned}
&x\text{被 (1) 所覆盖}\\
\Longleftrightarrow&\text{有}1\leqslant s\leqslant k\text{使得}n_s\mid m_s(a_s-x)\\
\Longleftrightarrow&\prod_{s=1}^{k}\left(1-e^{2\pi i\frac{m_s}{n_s}(a_s-x)}\right)=0\\
\Longleftrightarrow&\sum_{I\subseteq\{1,\dots,k\}}(-1)^{|I|}e^{2\pi i\sum_{s\in I}a_s m_s/n_s}\left(e^{-2\pi i\sum_{s\in I}m_s/n_s}\right)^x=0.
\end{aligned}$$

由于

$$\left|\left\{e^{-2\pi i\sum_{s\in I}m_s/n_s}:\ I\subseteq\{1,\dots,k\}\right\}\right|=|S|,$$

应用引理 1 便知 (1) 覆盖连续 $|S|$ 个整数时它必为覆盖系。

显然 (1) 不可能覆盖某个整数超过 k 次。下设 $1<m\leqslant k$. 易见 (1) 覆盖整数 x 至少 m 次当且仅当对 $\{1,\dots,k\}$ 的任一个 $m-1$ 元子集 J 剩余类系 $\{a_s(n_s)\}_{s\notin J}$ 都覆盖 x. 由此利用已证结果便知， (1) 覆盖连续

$$L(m)=\max_{\substack{J\subseteq\{1,\dots,k\}\\ |J|=m-1}}\left|\left\{\left\{\sum_{s\in I}\frac{m_s}{n_s}\right\}:\ I\subseteq\{1,\dots,k\}\setminus J\right\}\right|\leqslant\min\left\{|S|,2^{k-m+1}\right\}$$

个整数至少 m 次时它覆盖每个整数至少 m 次。 □

局部 - 整体性定理 II 在 G 为复数域时的证明: 由于常数可看作周期为 $n_0=1$ 的 $\mathbb{Z}$ 上常函数，我们只需假定 $\psi(x)=0$ 对连续 $|T|$ 个整数 x 成立来证明 ψ 为零函数。注意

$$\begin{aligned}\psi(x)=&\sum_{s=1}^{k}\sum_{a=0}^{n_s-1}\psi_s(a)[x\equiv a\ (\mathrm{mod}\ n_s)]\\=&\sum_{s=1}^{k}\sum_{a=0}^{n_s-1}\frac{\psi_s(a)}{n_s}\sum_{r=0}^{n_s-1}e^{2\pi i(x-a)r/n_s}\\=&\sum_{s=1}^{k}\sum_{r=0}^{n_s-1}\Big(\sum_{a=0}^{n_s-1}\frac{\psi_s(a)}{n_s}e^{-2\pi iar/n_s}\Big)\left(e^{2\pi ir/n_s}\right)^x,\end{aligned}$$

应用引理 1 立得欲证。 □

对上述证明稍作推广可证 G 是特征不整除 $n_1,\ldots,n_k$ 的域时局部 - 整体性定理 II 成立，详情可见孙智伟的论文 [S4]. 一般形式的局部 - 整体性定理 II 由作者在 [S5] 中首先获得，这时使用 Vandermonde 行列式的办法不再有效，证明需要递归序列与代数数论知识。

References

[CV1] R. B. Crittenden and C. L. Vanden Eynden , *A proof of a conjecture of Erdős*, Bull. Amer. Math. Soc. **75**(1969), 1326–1329.

[CV2] R. B. Crittenden and C. L. Vanden Eynden, *Any n arithmetic progressions covering the first 2^n integers cover all integers*, Proc. Amer. Math. Soc. **24**(1970), 475–481.

[E1] P. Erdős, *Remarks on number theory IV: Extremal problems in number theory I*, Mat. Lapok **13**(1962), 228–255.

[E2] P. Erdős, *Extremal problems in number theory*, Proc. Sympos. Pure Math. **8**(1965), 181–189, Amer. Math. Soc., Providence, R. I..

[GJ] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-completeness*, W.H. Freeman, New York, 1983.

[S1] Z. W. Sun, *Covering the integers by arithmetic sequences*, Acta Arith. **72**(1995), 109–129.

[S2] Z. W. Sun, *Covering the integers by arithmetic sequences* II , Trans. Amer. Math. Soc. **348**(1996), 4279–4320.

[S3] Z. W. Sun, *Unification of zero-sum problems, subset sums and covers of* $\mathbb{Z}$, Electron. Res. Announc. Amer. Math. Soc. **9**(2003), 51–60.

[S4] Z. W. Sun, *Arithmetic properties of periodic maps*, Math. Res. Lett. **11**(2004), 187–196.

[S5] Z. W. Sun, *A local-global thorem on periodic maps*, `arXiv:math.NT/0404137`.

[T] S. P. Tung, *Complexity of sentences over number rings*, SIAM J. Comp. **20**(1991), 126–143.