KZG 承诺的同点批量打开：一个引理及其证明

2026年6月2日 · 更新于 2026年7月15日

目录

> **占位内容。** 这篇笔记是为了测试站点的中文与公式排版而写的样例：定义、引理、定理与证明的自动编号，多行对齐公式，行内公式与中文混排，以及一个用来测试窄屏横向滚动的超长公式。内容是标准结论，可以替换或删除。

多项式承诺让证明者先承诺一个多项式 f，之后再令人信服地打开它在任意一点的取值。KZG 方案[1]的承诺和打开证明都只有一个群元素，这使它成为 PLONK 等证明系统的基础构件。实际系统里，验证者往往需要在**同一个点** z 上同时打开 t 个多项式：逐个验证需要 $2t$ 次配对，而一次随机线性组合可以把它降到 2 次。[2] 这篇笔记把其中用到的引理单独拿出来，完整地证明一遍。

记号

设 $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ 是阶为素数 p 的循环群，生成元分别为 g_1, g_2, g_T；$e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ 是非退化的双线性映射，$\mathbb{F} = \mathbb{F}_p$。对 $a \in \mathbb{F}$，记 $[a]_1 = a \cdot g_1$，$[a]_2 = a \cdot g_2$。

定义 1（KZG 多项式承诺）　令 d 为次数上界。可信设置选取随机的 $\tau \leftarrow \mathbb{F}$，输出

$$\mathsf{srs} = \big([1]_1,\, [\tau]_1,\, [\tau^2]_1,\, \dots,\, [\tau^d]_1;\;\; [1]_2,\, [\tau]_2\big)$$

并销毁 τ。对任意 $f \in \mathbb{F}[X]$，$\deg f \le d$：

- **承诺**：$\mathsf{com}(f) = [f(\tau)]_1$，它可以由 srs 线性地算出；
- **打开**：要证明 $f(z) = v$，令 $q(X) = \dfrac{f(X) - v}{X - z}$，证明为 $\pi = [q(\tau)]_1$；
- **验证**：接受当且仅当 $e\big(C - [v]_1,\, [1]_2\big) = e\big(\pi,\, [\tau]_2 - [z]_2\big)$。

验证等式之所以成立，是因为 q 是多项式当且仅当 $(X - z) \mid f(X) - v$，也就是当且仅当 $f(z) = v$。

同点批量打开

设证明者已经承诺了 $f_1, \dots, f_t$，承诺为 $C_i = \mathsf{com}(f_i)$，并声称对所有 i 都有 $f_i(z) = v_i$。协议如下：

1. 验证者发送随机挑战 $\gamma \leftarrow \mathbb{F}$（非交互的情形下，$\gamma$ 由 Fiat–Shamir 变换得到）；
2. 证明者计算批量商多项式 $h(X) = \sum_{i=1}^{t} \gamma^{i-1} \cdot \dfrac{f_i(X) - v_i}{X - z}$，发送 $\pi = [h(\tau)]_1$；
3. 验证者计算 $C_\gamma = \sum_{i=1}^{t} \gamma^{i-1} C_i$ 与 $v_\gamma = \sum_{i=1}^{t} \gamma^{i-1} v_i$，接受当且仅当

$$e\big(C_\gamma - [v_\gamma]_1,\, [1]_2\big) = e\big(\pi,\, [\tau]_2 - [z]_2\big).$$

记 $F_\gamma(X) = \sum_{i=1}^{t} \gamma^{i-1}\big(f_i(X) - v_i\big)$。诚实的证明者满足 $C_\gamma - [v_\gamma]_1 = [F_\gamma(\tau)]_1$ 以及 $F_\gamma(X) = h(X)\,(X - z)$，于是完备性由双线性直接得到：

$$\begin{aligned} e\big(C_\gamma - [v_\gamma]_1,\, [1]_2\big) &= e\big([F_\gamma(\tau)]_1,\, [1]_2\big) \\ &= e\big([h(\tau)\,(\tau - z)]_1,\, [1]_2\big) \\ &= e\big([h(\tau)]_1,\, [\tau - z]_2\big) = e\big(\pi,\, [\tau]_2 - [z]_2\big). \end{aligned}$$

把 h 完全展开，就是下面这个很长的式子（它同时用来测试窄屏上的横向滚动）：

$$h(X) = \frac{f_1(X) - v_1}{X - z} + \gamma \cdot \frac{f_2(X) - v_2}{X - z} + \gamma^2 \cdot \frac{f_3(X) - v_3}{X - z} + \gamma^3 \cdot \frac{f_4(X) - v_4}{X - z} + \cdots + \gamma^{t-1} \cdot \frac{f_t(X) - v_t}{X - z} = \frac{1}{X - z} \sum_{i=1}^{t} \gamma^{i-1} \big(f_i(X) - v_i\big).$$

引理与证明

可靠性的核心是：只要有一个声称的取值是错的，做完随机线性组合之后它以压倒性的概率「仍然是错的」。

引理 1（随机线性组合）　设 $f_1, \ldots, f_t \in \mathbb{F}[X]$，$z, v_1, \ldots, v_t \in \mathbb{F}$，$F_\gamma$ 如上定义。若存在 j 使得 $f_j(z) \neq v_j$，则

$$\Pr_{\gamma \leftarrow \mathbb{F}} \Big[(X - z) \mid F_\gamma(X) \Big] \;\leq\; \frac{t - 1}{|\mathbb{F}|}.$$

证明　由余式定理，$(X - z) \mid F_\gamma(X)$ 当且仅当 $F_\gamma(z) = 0$。把 $F_\gamma(z)$ 看成关于 γ 的多项式：

$$P(\gamma) = \sum_{i=1}^{t} \big(f_i(z) - v_i\big)\, \gamma^{i-1} \;\in\; \mathbb{F}[\gamma].$$

它的次数至多为 $t - 1$，并且 γ^{j-1} 的系数 $f_j(z) - v_j \neq 0$，所以 P 不是零多项式。域上非零多项式的根的个数不超过它的次数，因此使 $P(\gamma) = 0$ 的 γ 至多有 $t - 1$ 个；而 γ 在 $\mathbb{F}$ 上均匀分布，故所求概率不超过 $(t - 1)/|\mathbb{F}|$。 ∎

定理 1（批量打开的可靠性，非正式）　假设单个多项式的 KZG 方案满足求值绑定性，并且从敌手输出的每个承诺 C_i 都能提取出对应的多项式 f_i（例如在代数群模型中[3]）。那么对任何多项式时间的敌手，批量验证通过、同时又存在某个 j 使 $f_j(z) \neq v_j$ 的概率至多为 $(t - 1)/|\mathbb{F}| + \mathrm{negl}(\lambda)$。

证明　（概要）设验证通过且某个 $f_j(z) \neq v_j$。由引理 1，除去至多 $(t-1)/|\mathbb{F}|$ 的概率，有 $F_\gamma(z) \neq 0$。此时 $C_\gamma - [v_\gamma]_1$ 是多项式 F_γ 的承诺，而敌手的 π 把它在 z 处打开为 0；归约算法知道所有的 f_i，可以自己诚实地算出把同一个承诺在 z 处打开为 $F_\gamma(z) \neq 0$ 的证明。同一个承诺在同一点有两个取值不同的合法打开，与求值绑定性矛盾。 ∎

代价

	逐个打开	批量打开
证明大小	t 个 $\mathbb{G}_1$ 元素	1 个 $\mathbb{G}_1$ 元素
配对次数	$2t$	2
$\mathbb{G}_1$ 上的标量乘	约 $2t$	约 $t + 1$
额外的可靠性损失	无	$(t-1)/\lvert\mathbb{F}\rvert$

对 $|\mathbb{F}| \approx 2^{255}$ 和实际中出现的 $t \leq 2^{10}$，这个损失完全可以忽略。

---

1. Aniket Kate, Gregory M. Zaverucha, Ian Goldberg, “Constant-Size Commitments to Polynomials and Their Applications”, ASIACRYPT 2010. ↩
2. Ariel Gabizon, Zachary J. Williamson, Oana Ciobotaru, “PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge”, IACR ePrint 2019/953. ↩
3. Georg Fuchsbauer, Eike Kiltz, Julian Loss, “The Algebraic Group Model and its Applications”, CRYPTO 2018. ↩